36531 Uitvoering van verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (Uitvoeringswet digitaledienstenverordening)

NOTA NAAR AANLEIDING VAN VERSLAG

Met belangstelling heb ik kennisgenomen van de vragen en opmerkingen van de leden van de fracties van de PVV, GroenLinks-PvdA, VVD, NSC, D66 en CDA. Graag beantwoord ik, mede namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de vragen die door de verschillende fracties zijn gesteld. In deze nota zijn de vragen en opmerkingen uit het verslag integraal opgenomen in cursieve tekst en de beantwoording daarvan in niet-cursieve tekst. De vragen zijn genummerd, waarnaar in voorkomende gevallen naar andere antwoorden is verwezen. Gelijkluidende of in elkaars verlengde liggende vragen zijn gezamenlijk beantwoord.

1. Inleiding

1) *De leden van de CDA-fractie merken op dat Nederland vijftien maanden de tijd had om de wet aan te passen aan de Europese regels die volgen uit de verordening, maar dat deze termijn niet is gehaald. Hierdoor kan de toezichthouder, de Autoriteit Consument en Markt (ACM), op dit moment niet handhaven wanneer meldingen binnenkomen. Deze leden vragen aan de regering wat de reden is dat de termijn is overschreden en of er sinds de inwerkingtreding van de DSA al veel meldingen binnen zijn gekomen bij de ACM die dus geen opvolging hebben kunnen krijgen en zo ja, hoeveel.*

Antwoord
In de beantwoording van de recente vragen van de leden Kathmann en Koekoek is toegelicht waarom de uitvoeringstermijn van 15 maanden is overschreden.[1] Het zorgvuldig opstellen van het wetsvoorstel en bijbehorende memorie van toelichting in afstemming met alle betrokken partijen en het doorlopen van alle stappen van het wetgevingsproces, waaronder verplichte raadplegingen en toetsen, hebben ervoor gezorgd dat het niet mogelijk was om de uitvoeringswetgeving binnen de termijn die de DSA voorschrijft (15 maanden) tot stand te doen komen.[2] In dit verband zij opgemerkt dat een uitvoeringstermijn van 15 maanden erg kort is als de uitvoering op het niveau van een formele wet dient plaats te vinden, zoals bij de DSA het geval is. Om die reden heeft de Nederlandse regering tijdens de onderhandelingen gepleit voor een langere uitvoeringstermijn van ten minste 18, maar liever 24 maanden.

Nederland is overigens niet de enige lidstaat die de uitvoeringstermijn heeft overschreden. De Europese Commissie houdt een website bij met daarop een overzicht van de aangewezen digitaledienstencoördinatoren. Uit dit overzicht blijkt bijvoorbeeld dat België, Estland, Frankrijk, Duitsland, Letland, Litouwen, Polen en Slowakije, anders dan Nederland, nog geen digitaledienstencoördinator hebben aangewezen.[3]

Een goede uitvoering van een verordening zoals de DSA vraagt om diverse werkzaamheden naast het tot stand brengen van de uitvoeringswet. Zo wordt er sinds het aannemen van de DSA met onder meer de ACM en AP als beoogd toezichthouders samengewerkt, bijvoorbeeld om informatie over de DSA onder de aandacht te brengen van de bedrijven die er straks aan moeten voldoen en van de gebruikers en belanghebbenden die door de DSA nieuwe rechten krijgen. De ACM is bijvoorbeeld in contact gebracht met partijen die geïnteresseerd zijn in het verwerven van de status van ‘betrouwbare flagger’ of ‘erkend onderzoeker’. Verder heeft de minister van Economische Zaken en Klimaat in 2023 reeds middelen voor beide toezichthouders beschikbaar gesteld zodat zij

[1] Aanhangsel II 2023/24, nr. 1241.

[2] In dit geval moesten de volgende toetsen/adviezen worden verricht: uitvoerbaarheids- en handhaafbaarheidstoetsen van de Autoriteit Consument & Markt en de Autoriteit persoonsgegevens als beoogd toezichthouders, raadpleging van het Adviescollege toetsing regeldruk, wetgevingstoets door het Ministerie van Justitie en Veiligheid, advies van de Raad voor de Rechtspraak, een wetgevingstoets door de Autoriteit persoonsgegevens, een advies van het Openbaar Ministerie, en het advies van de Afdeling Advisering van de Raad van State.

[3] https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs.

zich op dat moment al konden voorbereiden op de uitvoering van de DSA. Ook voor 2024 en verder zijn er inmiddels (structurele) middelen beschikbaar gesteld aan de toezichthouders. Verder heeft de minister van Economische Zaken en Klimaat, vooruitlopend op de uitvoeringswet, het Besluit voorlopige aanwijzing ACM als bevoegde autoriteit en digitaledienstencoördinator digitaledienstenverordening genomen.[4] Het belang van deze voorlopige aanwijzing is dat de ACM, vooruitlopend op de totstandkoming van de uitvoeringswet, kan starten met een deel van de uitvoering van de verordening en dat zij op Europees niveau Nederland kan vertegenwoordigen in de digitaledienstenraad.

Sinds de inwerkingtreding van de DSA zijn er bij de ACM 80 meldingen binnengekomen die mogelijk verband houden met een overtreding van de DSA (stand per 2 mei 2024). Van deze meldingen zijn er 59 reeds volledig beoordeeld. 30 meldingen zijn bestemd voor digitaledienstencoördinatoren in andere lidstaten. Een deel daarvan is reeds doorgestuurd via het Europees Informatie-uitwisselingssysteem, AGORA (artikel 85 van de verordening). AGORA is nog volop in ontwikkeling en niet alle functionaliteiten zijn al beschikbaar of volledig operationeel. De overige meldingen worden op termijn doorgestuurd zodra het Europese systeem dit toelaat.

De andere reeds beoordeelde 29 meldingen zullen onder het toezicht van de ACM gaan vallen en worden bewaard totdat de ACM bevoegd is en zij de meldingen kan betrekken bij haar toezicht op de naleving van de verordening. Per 2 mei 2024 wachten nog 21 meldingen op nadere informatie, advisering of beoordeling.

2) *Zij vragen welke activiteiten de ACM tot nu toe heeft ondernomen op basis van het Besluit voorlopige aanwijzing ACM als bevoegde autoriteit en digitaledienstencoördinator digitaledienstenverordening. De leden van de CDA-fractie steunen een spoedige behandeling van het wetsvoorstel in de Eerste en de Tweede Kamer.*

Antwoord
De ACM neemt als digitaledienstencoördinator deel aan de digitaledienstenraad. Dit is het samenwerkingsverband van alle digitaledienstencoördinatoren onder de verordening en wordt voorgezeten door de Europese Commissie. De digitaledienstenraad komt momenteel maandelijks wisselend fysiek of online bij elkaar. Ook heeft de ACM contact met andere digitaledienstencoördinatoren om te zorgen voor een consistente wijze waarop de taken van de digitaledienstencoördinatoren wordt uitgevoerd in de EU. Daarnaast neemt de ACM deel aan de (nu nog) enige werkgroep van de digitaledienstenraad over verkiezingen. In de toekomst kan de ACM deelnemen aan meerdere werkgroepen over verschillende onderwerpen, wanneer deze worden opgestart.

De ACM neemt momenteel meldingen over vermeende inbreuken op de DSA in ontvangst en stuurt deze, waar nodig en voor zover dit kan, door naar de bevoegde digitaledienstencoördinator in een andere lidstaat. Zie hierover ook de beantwoording van vraag 1.

Als beoogd toezichthouder vindt de ACM het belangrijk dat partijen die onder de DSA vallen zich goed voor kunnen bereiden op de nieuwe Europese regels. Daarom heeft de ACM begin dit jaar een conceptleidraad opgesteld en geconsulteerd, die partijen helpt bij deze voorbereiding.[5] Op basis van de ontvangen input tijdens de consultatie, zal de ACM in de loop van dit jaar een volgende versie van de leidraad publiceren. Daarnaast geeft de ACM op haar website aandacht aan de DSA.[6]

Gegeven het brede bereik van de DSA en de coördinerende rol van de digitaledienstencoördinator heeft het Samenwerkingsplatform Digitale Toezichthouders (SDT) een DSA-kamer opgericht.[7] Bij deze kamer zijn ook andere toezichthouders betrokken dan de leden van het SDT, dat in oktober 2021 werd opgericht door de Autoriteit Consument & Markt (ACM), de Autoriteit Financiële Markten

[4] Stcrt. 2024, 3993.
[5] https://www.acm.nl/nl/publicaties/acm-consulteert-leidraad-dsa-voor-aanbieders-online-diensten.
[6] https://www.acm.nl/nl/publicaties/acm-roept-online-bedrijven-op-goed-te-controleren-aan-welke-nieuwe-dsa-regels-zij-moeten-voldoen.
[7] https://www.acm.nl/nl/publicaties/toezichthouders-van-sdt-breiden-samenwerking-digitaal-toezicht-uit.

(AFM), de Autoriteit Persoonsgegevens (AP) en het Commissariaat voor de Media (CvdM). Het doel is om een goede samenwerking te waarborgen en kennis en ervaringen uit te wisselen.

De ACM werkt met andere toezichthouders en overheidsorganisaties aan afspraken over het doorsturen van bevelen in de zin van artikel 9 en 10 van de verordening aan de ACM. Om een goed beeld te krijgen van wat er speelt en waar partijen tegenaan lopen, voert de ACM gesprekken met een brede groep belanghebbenden. Zoals onder meer aanbieders van online tussenhandeldiensten, beoogde betrouwbare flaggers, onderzoekers en maatschappelijke organisaties en relevante overheidsorganisaties.

2. Doel, reikwijdte en belangrijkste begrippen

2.1 Doel en achtergrond van de verordening

3) *De leden van de D66-fractie hebben kennisgenomen van de memorie van toelichting. De onderbouwing over wat wél en niet classificeert als 'dienst van de informatiemaatschappij' zorgt nog voor enige verwarring. Klopt het dat een platform zoals Airbnb níet classificeert als zodanig, maar Uber bijvoorbeeld wél, zo vragen deze leden.*

Antwoord
De digitaledienstenverordening heeft betrekking op tussenhandeldiensten. Tussenhandeldiensten zijn diensten van de informatiemaatschappij, zo volgt uit artikel 3, onderdeel g, van de verordening. Het Hof van Justitie van de Europese Unie heeft zich in verschillende arresten uitgesproken over de vraag of een online dienst, zoals een online platform, dat bemiddelt tussen aanbieders en gebruikers van offline diensten, wel of niet moet worden beschouwd als 'dienst van de informatiemaatschappij'. In het Uber-arrest[8] betrof dat taxivervoersdiensten en in het Airbnb-arrest[9] de verhuur van toeristische woonruimte.

Het HvJEU heeft in beide zaken op grond van de feiten in de zaak beoordeeld of de online bemiddelingsdienst in kwestie los gezien kan worden van de offlinedienst waarin wordt bemiddeld, of dat zij onlosmakelijk verbonden zijn. In het Uber-arrest oordeelde het HvJEU dat de taxivervoersdienst onlosmakelijk verbonden is met de bemiddelingsdienst en dat het geheel van die diensten moet worden beschouwd als taxivervoersdienst en niet als een 'dienst van de informatiemaatschappij'. In het Airbnb-arrest oordeelde het HvJEU dat de verhuur van toeristische woonruimte los gezien kan worden van de online bemiddelingsdienst en dat die online bemiddelingsdienst daarom moet worden beschouwd als 'dienst van de informatiemaatschappij'.

4) *De leden van de D66-fractie constateren dat er geen definitie van desinformatie wordt gegeven in de verordening, maar wel in de memorie van toelichting van het kabinet. Wat zijn de gevolgen hiervan voor de uitwerking van de verordening?*

Antwoord
De verordening heeft mede tot doel de maatschappelijke risico's van de verspreiding van schadelijke inhoud aan te pakken, waaronder ook inhoud die valt onder de definitie van 'desinformatie' zoals die wordt gebruikt in beleidsdocumenten van de Europese Commissie en het kabinet. Het begrip 'desinformatie' als zodanig wordt echter niet gebruikt in de verordening zelf en daarom ook niet gedefinieerd. In paragraaf 2.4.2 van de memorie van toelichting bij het wetsvoorstel is ter verduidelijking toegelicht welke invulling het kabinet en de Europese Commissie in hun beleid geven aan het begrip 'desinformatie' en hoe dat zich verhoudt tot de verschillende zorgvuldigheidsverplichtingen uit de verordening. De belangrijkste zorgvuldigheidsverplichtingen ten aanzien van het tegengaan van schadelijke inhoud zijn gericht aan de zeer grote online platforms en zoekmachines en de Europese Commissie is exclusief bevoegd voor toezicht en handhaving van die verplichtingen. Het is dus aan de Europese Commissie om in de praktijk deze onderdelen nader uit te werken in hun toezichtsbeleid.

[8] HvJ EU 20 december 2017, zaak C-434/15, ECLI:EU:C:2017:981 (Elite Taxi/Uber Spain) en HvJ EU 10 april 2018, zaak C-320/16, ECLI:EU:C:2018:221 (Uber France).
[9] HvJ EU 19 december 2019, zaak C-390/18, ECLI:EU:C:2019:1112 (Airbnb Ireland).

5 en 6) *Verder worden voorbeelden aangehaald waar in beginsel geen sprake is van illegale inhoud, zoals complottheorieën en foutieve medische informatie. In hoeverre klopt de veronderstelling van deze leden dat deze verordening deze uitingen dus niet kan aanpakken? Welke mogelijkheden zijn er om op nationale schaal hier maatregelen tegen te nemen?*

Antwoord
De verspreiding van schadelijke inhoud kan leiden tot maatschappelijke problemen. Desinformatie kan zowel de vorm aannemen van illegale inhoud als schadelijke inhoud. De regels onder de verordening voor schadelijke inhoud zijn echter wezenlijk anders dan die voor illegale inhoud, hetgeen van belang is voor de mogelijke aanpak daarvan.

Een aantal bepalingen uit de verordening heeft immers enkel betrekking op 'illegale inhoud', en niet op desinformatie of andere schadelijke inhoud die niet tevens kwalificeert als illegale inhoud, zoals de kennisgevings- en actiemechanismen en de bepalingen over bevelen om op te treden tegen illegale inhoud. De aanpak van schadelijke, maar niet-illegale, desinformatie door de verordening gebeurt op andere manieren. Zo bevat de verordening verschillende bepalingen over inhoudsmoderatie door aanbieders van tussenhandeldiensten. Volgens de definitie van het begrip 'inhoudsmoderatie' (artikel 3, onderdeel t, van de verordening) gaat het dan om zowel illegale inhoud als om informatie die in strijd is met de algemene voorwaarden die de aanbieder toepast, bijvoorbeeld omdat hij deze onwenselijk of schadelijk acht. Desinformatie en andere schadelijke inhoud kunnen onder contractuele beperkingen vallen die in de algemene voorwaarden opgenomen zijn. Op grond van artikel 14 van de verordening zijn aanbieders van tussenhandeldiensten verplicht om in hun voorwaarden duidelijk en gebruiksvriendelijk hun beleid ten aanzien van inhoudsmoderatie op te nemen en bij het formuleren en toepassen van die voorwaarden gepaste aandacht hebben voor de legitieme belangen en fundamentele rechten van alle betrokkenen.

Daarnaast kan de verspreiding van schadelijke inhoud en met name desinformatie, ook een zogenaamd 'systeemrisico' vormen. Artikel 34 van de verordening beschrijft een aantal typen schadelijke inhoud die een zogenaamd 'systeemrisico' kunnen vormen, zoals inhoud die een negatief effect heeft of kan hebben op de burgerdialoog, de verkiezingsprocessen, de bescherming van minderjarigen of de volksgezondheid. Hieronder valt ook informatie die niet illegaal is, maar wel bijdraagt tot de in deze verordening genoemde systeemrisico's. Aanbieders van zeer grote online platforms en zeer grote online zoekmachines moeten daarom, bij de beoordeling van systeemrisico's, bijzondere aandacht besteden aan de manier waarop hun diensten (kunnen) worden gebruikt om misleidende of bedrieglijke inhoud, met inbegrip van desinformatie en gecoördineerde desinformatiecampagnes, te verspreiden of versterken. Daarbij moeten ze met name rekening houden met de vraag of en hoe het ontwerp van hun aanbevelingssystemen en andere relevante algoritmische systemen, hun inhoudsmoderatiesystemen, de toepasselijke algemene voorwaarden en de handhaving ervan, systemen voor de selectie en weergave van reclame en data-gerelateerde praktijken van de aanbieder van invloed zijn op deze systeemrisico's.

Indien dergelijke systeemrisico's aanwezig zijn, moeten aanbieders van zeer grote online platforms en zeer grote online zoekmachines maatregelen treffen om deze te beperken. Dergelijke maatregelen kunnen de aanpassing van hun diensten, online-interfaces, algemene voorwaarden inhoudsmoderatieprocedures, algoritmische systemen of aanbevelingssystemen omvatten. Ook kunnen de aanbieders bewustmakingsmaatregelen nemen om de gebruikers van de dienst meer informatie te verschaffen. Ook wordt de maatregel genoemd om gegenereerd of gemanipuleerd beeld-, audio- of videomateriaal dat een merkbare gelijkenis vertoont met bestaande personen, voorwerpen, plaatsen of andere entiteiten of gebeurtenissen, en door een persoon ten onrechte voor authentiek of waarheidsgetrouw wordt aangezien, opvallend te markeren.

Niet-illegale, maar wel schadelijke desinformatie valt dus onder het bereik van de regels gericht op het voorkomen van systeemrisico's door zeer grote online platforms en zeer grote online zoekmachines. De Commissie is exclusief bevoegd voor het toezicht op en de handhaving van deze verplichtingen. De Commissie is recent twee formele procedures gestart om te onderzoeken of Meta en X deze verplichtingen om burgers te beschermen tegen de verspreiding van desinformatie

hebben overtreden.[10] De lidstaten – en dus de op nationaal niveau aangewezen bevoegde autoriteiten – hebben geen bevoegdheid tot toezicht en handhaving ten aanzien van deze verplichtingen.

De verordening voorziet in volledige harmonisatie van de zorgvuldigheidsverplichtingen voor tussenhandeldiensten. Dat betekent dat de verordening het niet toestaat om in het nationale recht aanvullende zorgvuldigheidsverplichtingen op te nemen voor aanbieders van tussenhandeldiensten die dezelfde doelstelling hebben als de verordening. De verordening laat wel ruimte om zorgvuldigheidsverplichtingen op te leggen die een ander doel dienen dan de verordening, uiteraard met inachtneming van de regels inzake het vrije verkeer van diensten van de informatiemaatschappij (artikelen 3 en 4 van de richtlijn elektronische handel). De verordening laat het verder mede aan ander Unierecht en het nationale recht van de lidstaten om te bepalen wat illegale inhoud is.

Wat betreft schadelijke online content ziet het kabinet verder een rol voor de overheid om de weerbaarheid van burgers tegen deze content te versterken. Daarom werkt het kabinet aan verschillende acties in het kader van de rijksbrede strategie desinformatie, waaronder acties om de weerbaarheid van burgers te versterken.[11] Op 17 juni is uw Kamer over de voortgang hiervan geïnformeerd, waarbij ook nieuwe maatregelen zijn aangekondigd om de aanpak van desinformatie te verstevigen.[12]

7) *De leden van de CDA-fractie lezen dat volgens de regering het probleem van illegale online-inhoud en illegale online-activiteiten niet uitsluitend kan worden aangepakt door te richten op de aanbieders, maar juist ook moeten worden bestreden bij de bron. Deze leden vragen hoe de regering dit wil bewerkstelligen, nu veel mensen zich anoniem op het internet bewegen en vaak niet achterhaald kan worden wie achter een anoniem account zit. Is de regering het met deze leden eens dat het effectiever zou zijn als het niet meer mogelijk wordt gemaakt om een anoniem account aan te maken op sociale media? Zo nee, waarom niet?*

Antwoord
Anonimiteit, ook op sociale media, heeft niet enkel nadelen maar ook belangrijke voordelen: het beschermt tegen lastigvallen en intimidatie, tegen politieke vervolging, en beschermt de privésfeer van mensen die misschien thuis of in hun land zichzelf niet kunnen zijn. Het biedt mensen de mogelijkheid om informatie op te zoeken waar niet iedereen in hun omgeving achter staat. Of het nu gaat om informatie over soa’s of informatie over politiek afwijkende standpunten. Ook klokkenluiders kunnen anonimiteit nodig hebben om zichzelf tegen vervolging te beschermen. Anonimiteit is dus een belangrijk middel om de vrijheid van meningsuiting en de toegang tot informatie te beschermen, en het is een belangrijk onderdeel van de bescherming van privacy. Dit wordt ondersteund door het eindrapport van de Adviescommissie Versterken Weerbaarheid Democratische Rechtsorde dat in november 2023 uitkwam. Overigens staat het partijen vrij om binnen de grenzen van de wet en met inachtneming van het grondrecht op privacy zelf keuzes te maken over de mate van anonimiteit die mogelijk is op een platformen of dienst.

Voor de mogelijkheden om strafbaar gedrag online te vervolgen is het afschaffen van anonimiteit niet nodig. Gebruikers van online diensten genieten over het algemeen slechts een beperkte vorm van anonimiteit. De aanbieders van online diensten beschikken veelal over gebruikersgegevens zoals IP-adressen en e-mailadressen. Een opsporingsambtenaar heeft in het geval van een misdrijf de mogelijkheid om die gegevens te vorderen en daarmee gebruikers te identificeren (artikel 126na Wetboek van Strafvordering). Voor civielrechtelijke zaken zijn de mogelijkheden om informatie over gebruikers te verkrijgen beschreven in paragraaf 4.2.2 van de memorie van toelichting.

In 2023 heeft de Tweede Kamer een motie van het voormalige Kamerlid Gündogan aangenomen.[13] Daarin is de regering verzocht om onderzoek te verrichten naar de aspecten van sociale media die

[10] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

[11] Kamerstukken II 2022/23, 30 821, nr. 173.

[12] Kamerstukken II 2023/24, 30 821, nr. 230.

[13] Kamerstukken II 2022/23, 30 821, nr. 192.

bijdragen aan risico's voor onze democratie, en de rol van anonimiteit daarbij te betrekken. De motie verzoekt ook om te onderzoeken welke technische mogelijkheden een oplossing zouden kunnen bieden met behoud van publieke waarden als privacy en recht op zelfbeschikking. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties werkt momenteel aan de uitvoering van deze motie.

8) *De leden van de CDA-fractie vragen aan de regering of het dankzij onderhavige Uitvoeringswet en de DSA makkelijker wordt om bijvoorbeeld makers en verspreiders van deepfake-pornobeelden te achterhalen en op te sporen, en zo ja, op welke manier dit wordt verbeterd en of hier daadwerkelijk actief op wordt gehandhaafd.*

Antwoord
De verordening beoogt onder meer om de verspreiding van illegale inhoud aan te pakken. Dat moet ook bijdragen aan een betere bestrijding van deepfake-pornobeelden, omdat die veelal illegaal zijn.[14] Zo verduidelijkt de verordening bijvoorbeeld in artikel 16, derde lid, dat een melding van illegale inhoud conform de vereisten van dat artikel leidt tot zogenaamde "*daadwerkelijke kennis of bekendheid*" van die illegale inhoud bij een hostingbedrijf of online platform. Zodra dat het geval is moeten zij prompt handelen om die illegale inhoud te verwijderen of de toegang daartoe onmogelijk te maken. Doen ze dat niet dan kunnen ze geen beroep doen op de vrijwaring van aansprakelijkheid uit artikel 6 van de verordening en zelfstandig aansprakelijk worden gesteld voor die illegale inhoud.

De verordening bevat geen bepalingen die specifiek zien op het achterhalen of opsporen van de makers van dit materiaal. De civielrechtelijke mogelijkheden daartoe zijn beschreven in paragraaf 4.2.2 van de memorie van toelichting. In het kader van een strafrechtelijke procedure kan informatie worden gevorderd over de makers of verspreiders van strafbare deepfake-pornobeelden bij een communicatiedienst. Als het noodzakelijk is ter beëindiging van het strafbare feit kan de officier van justitie – ook voordat een verdachte voor het strafbare feit is veroordeeld - in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Wetboek van Strafvordering, met een machtiging van de rechter-commissaris aan een aanbieder van een communicatiedienst bevelen om gegevens ontoegankelijk te maken (artikel 125p Sv).

2.2 Volledige harmonisatie en ruimte voor aanvullende nationale regels

9) *De leden van de GroenLinks-PvdA-fractie begrijpen volledig de gedachte achter de behoefte voor volledige harmonisatie die de DSA beoogt en bereikt. Ook zien deze leden in dat de lidstaten geen aanvullende nationale eisen mogen stellen of in stand houden die binnen het toepassingsgebied van de verordening vallen. Dientengevolge vragen zij of er aanvullende eisen zijn die de regering graag in de verordening had gezien, die er nu niet in zijn opgenomen. Kan de regering aangeven welke eisen dat zijn?*

Antwoord
Het kabinet heeft gedurende de onderhandelingen gepleit voor een sterkere regeling voor het tegengaan van misbruik van diensten van online tussenpersonen voor criminaliteit. In het bijzonder *bad hosting*. Het kabinet heeft in het kader daarvan gepleit voor een (beperkte) zorgplicht of een samenstel van maatregelen dat eenzelfde effect heeft. Het kabinet zag daarin een goede aanvulling om aanbieders van hostingdiensten en online platformen te stimuleren om hun inspanningen te blijven verbeteren naar gelang technologische middelen en industriepraktijken zich in de loop van de tijd gaan ontwikkelen.[15] Hier was binnen de Raad echter onvoldoende draagvlak voor.

Daarnaast had het kabinet graag een meer realistische uitvoeringstermijn gezien. Waar het oorspronkelijke voorstel een termijn van 3 maanden voorschreef, heeft het kabinet gepleit voor een termijn van tenminste 18 maar bij voorkeur 24 maanden. Zoals nader toegelicht in de beantwoording van de Kamervragen van Kathmann en Koekoek, en vraag 1 in dit verslag, is de

[14] Zie de brief van de minister voor Rechtsbescherming en de minister van Justitie en Veiligheid over de regulering van deepfakes en immersieve technologieën (Kamerstukken II, 2022/23, 26643, nr. 1041).

[15] Kamerstukken II, 2021/22, 21 501-30, nr. 533, p. 3, 13–15, Kamerstukken II, 2021/22, 21 501-30, nr. 542, p.3, en Kamerstukken II, 2023/34, 29 574, nr. 708.

uiteindelijk in de verordening opgenomen termijn van 15 maanden voor Nederland te kort. Dit geldt voor meer lidstaten.[16]

Sinds de onderhandelingen heeft het kabinet zich op Europees niveau ingespannen om de bescherming van minderjarigen online te versterken, zoals het aanpakken van verslavend ontwerp van online diensten en applicaties. De verordening draagt bij aan het aanpakken van deze problematiek. Bijvoorbeeld door middel van het verbod op het gebruik van manipulatieve online interfaces van online platforms en de verplichting voor aanbieders van online platforms om maatregelen te nemen om minderjarigen te beschermen (de artikelen 25 en 28 van de verordening). De verordening heeft echter alleen betrekking op tussenhandeldiensten, terwijl de problematiek van bijvoorbeeld verslavend ontwerp ook speelt bij online diensten en applicaties die niet zijn aan te merken als tussenhandeldienst. Er wordt daarom aanvullend naar deze problematiek gekeken in het kader van de lopende '*fitness check on digital fairness*' van het consumentrecht. De inzet van het kabinet is om aan de Commissie te vragen om de reikwijdte en de definities van de huidige wetgeving te verduidelijken. Als dit onvoldoende blijkt om problemen aan te pakken, dan is het aan de Europese Commissie om met een voorstel te komen voor aanvullende wetgeving of andere beleidsmaatregelen.

10) *Kan de regering aangeven of zij bij de Europese Commissie gaat aandringen op een evaluatie van de DSA om eventueel deze eisen in een later stadium alsnog op te nemen in de DSA? Met welke andere lidstaten trekt de regering hierin gezamenlijk op?*

Antwoord
De verordening voorziet in artikel 91 reeds in een tweetal evaluaties; per 17 november 2025 en 17 november 2027. Er is zodoende geen noodzaak om aan te dringen op een extra of eerdere evaluatie. In de aanloop naar de evaluatie die de Europese Commissie op uiterlijk 17 november 2027 moet hebben verricht kan een volgend kabinet zich beraden op de vraag of het nodig en wenselijk is om opnieuw te pleiten voor een (beperkte) zorgplicht of een samenstel van maatregelen dat eenzelfde effect heeft voor het tegengaan van misbruik van diensten van online tussenpersonen voor criminaliteit en *bad hosting* in het bijzonder.

Dat wil niet zeggen dat het kabinet zal wachten tot de evaluatie voordat het stappen onderneemt. Om het leveren van hostingdiensten voor criminele doeleinden tegen te gaan zijn al enkele initiatieven gestart. Vorig jaar is de Kamer geïnformeerd over de resultaten van de zogenaamde *reseller* actie van de politie.[17] Hierbij is een door de politie verzamelde lijst van verdachte hostingdiensten verstrekt aan de brancheverenigingen Dutch Cloud Community zodat zij hun netwerk op de hoogte konden stellen van potentieel criminele activiteiten die via hun diensten verlopen. Er zijn meer activiteiten die de sector ondersteunen met informatie over criminele handelingen zodat deze beter kunnen worden tegengegaan. De Stichting Nationale Beheersorganisatie Internet Providers werkt, ondersteund door het ministerie van Justitie en Veiligheid en Europese financiering, aan het project Cleannetworks. Dit project beoogt het opzetten van een systeem om hostingproviders structureel te informeren over actuele criminele handelingen en kwetsbaarheden. Daarnaast wordt gestimuleerd dat hostingdiensten de Gedragscode Abusebestrijding onderschrijven. Doel van deze gedragscode is dat partijen zich inspannen om het gebruik van hun faciliteiten voor onrechtmatige activiteiten tegen te gaan.

11 en 12) *De leden van de VVD-fractie lezen dat lidstaten geen aanvullende nationale eisen mogen stellen of in stand houden die binnen het toepassingsgebied van de verordening vallen, tenzij daarin uitdrukkelijk is voorzien in de verordening. Hoewel de leden van de VVD-fractie begrijpen dat harmonisatie van groot belang is en dat er voldoende ruimte gecreëerd wordt voor nationale regels, vragen deze leden hoe de huidige nationale aanvullende regels zich verhouden tot de verordening. Wordt er voldoende rekening gehouden met de Europese regels? Wordt het mkb hierin voldoende ondersteund?*

[16] Aanhangsel Handelingen II 2023/24, nr. 1241.

[17] Kamerstukken II, 2022/23, 29 911, nr. 392.

Antwoord
De verhouding tussen nationale regels en de verordening is onderzocht. Waar nodig stelt het wetsvoorstel in hoofdstuk 5 aanpassingen van het nationale recht voor.

De verordening voorziet in uitzonderingen voor het micro- en kleinbedrijf. Dat zijn ondernemingen waar minder dan 50 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 10 miljoen EUR niet overschrijdt.[18] Deze ondernemingen hoeven niet te voldoen aan de aanvullende verplichtingen die gelden voor aanbieders van onlineplatforms (hoofdstuk III, afdeling 3, van de verordening) en die gelden voor aanbieders van onlinemarktplaatsen (hoofdstuk III, afdeling 4), van de verordening)

Ter ondersteuning van onder meer het MKB is er informatie over de verordening beschikbaar gemaakt op Ondernemersplein en werkt de ACM aan een leidraad waarin zij aanbieders handvatten geeft over de DSA. De ACM heeft die leidraad gepubliceerd op haar website. In 2024 zal een volgende doorontwikkelde versie worden gepubliceerd, op basis van ontvangen input en ervaringen.[19]

2.3. Het begrip «tussenhandeldienst»

13) *De leden van de VVD-fractie lezen dat de verordening niet van toepassing is op diensten die worden verleend via tussenhandeldiensten, als die diensten op zichzelf niet voldoen aan de definitie van tussenhandeldienst. Hoe wordt hier in praktijk onderscheid tussen gemaakt? Hoe komen platformen te weten of zij worden beschouwd als een tussenhandeldienst of niet?*

Antwoord
De digitaledienstenverordening heeft betrekking op tussenhandeldiensten. Blijkens artikel 2, tweede lid, van de verordening is de verordening niet van toepassing op diensten die worden verleend via tussenhandeldiensten, als die diensten op zichzelf niet voldoen aan de definitie van tussenhandeldienst. In de memorie van toelichting bij het wetsvoorstel wordt in dit verband het voorbeeld genoemd van een offline dienst, een schoonmaakdienst, die wordt aangeboden via een online platform. Als dat online platform kwalificeert als ‘tussenhandeldienst’, dan betekent dat niet automatisch dat de diensten die via dat online platform worden aangeboden ook kwalificeren als ‘tussenhandeldienst’ en dat aanbieders van die dienst zich uit dien hoofde aan de verplichtingen van de verordening moeten houden. De desbetreffende dienst moet op zichzelf beoordeeld worden aan de hand van de criteria die volgen uit de definitie van ‘tussenhandeldienst’. Het aanbieden van een offline dienst als een schoonmaakdienst voldoet daar niet aan.

Het kan echter ook zijn dat tussenhandeldiensten worden gebruikt voor het aanbieden van online diensten, zoals in het geval dat een online platform voor zijn website gebruik maakt van een hostingdienst van een hostingprovider. Ook in dat geval moet de online platform-dienst afzonderlijk beoordeeld worden voor de vraag of de dienst kwalificeert als tussenhandeldienst. Het is in eerste instantie aan de aanbieders van dergelijke diensten zelf om die beoordeling te maken. Op nationaal niveau kan de ACM, in haar rol als digitaledienstencoördinator, daarbij helpen in de vorm van voorlichting. In dat kader kan bijvoorbeeld gewezen worden op de in het antwoord op vraag 12 genoemde leidraad die de ACM heeft opgesteld en geconsulteerd. Op Europees niveau hebben de Europese Commissie en de digitaledienstenraad ook een rol in het geven van voorlichting over de verordening. Uiteindelijk is het aan de rechter om, indien er in een individueel geval een geschil over bestaat, tot een oordeel te komen.

2.4. Het begrip «desinformatie of andere inhoud»

14) *De leden van de PVV-fractie lezen in de memorie van toelichting dat desinformatie beschouwd dient te worden als het (onafhankelijk van het onderwerp, de producent/verspreider of wijze van verspreiding) doelbewust, veelal heimelijk, verspreiden van misleidende informatie, met het doel*

[18] Zie artikel 2, tweede en derde lid, van Aanbeveling 2003/361/EG.

[19] https://www.acm.nl/nl/publicaties/acm-consulteert-leidraad-over-digital-services-act-dsa-voor-aanbieder-van-online-diensten.

om schade toe te brengen aan het publieke debat, democratische processen, de openkenniseconomie of de volksgezondheid. Tevens lezen deze leden dat de Commissie desinformatie definieert als "onjuiste of misleidende inhoud die wordt verspreid met de bedoeling te bedriegen of economisch of politiek gewin te verkrijgen en die publieke schade kan berokkenen".

De leden van de PVV-fractie merken op dat dergelijke indicaties vrijelijk interpretabel zijn. In hoeverre wordt er gekeken naar de 'bron' of 'de zender' die de informatie gepost heeft?

Antwoord
Zoals in paragraaf 2.4.2 van de memorie van toelichting is aangegeven, is de kwalificatie van desinformatie onafhankelijk van de producent of verspreider. De identiteit van de bron of afzender en diens (politieke) opvattingen zijn dus bijvoorbeeld niet relevant voor de kwalificatie van informatie als desinformatie. Bepalend is of er sprake is van het doelbewust, veelal heimelijk, verspreiden van misleidende informatie, met het doel om schade toe te brengen aan het publieke debat, democratische processen, de openkenniseconomie of de volksgezondheid.

De identiteit van de bron of afzender van desinformatie speelt dus geen rol om te bepalen of er sprake is van desinformatie. Het kan wel relevant zijn voor het duiden van het soort desinformatie en het bepalen van een reactie. Zoals bijvoorbeeld in het geval dat de desinformatie afkomstig is van een statelijke actor. In dat geval is er sprake van *Foreign Information Manipulation and Interference* ('FIMI'). Dat rechtvaardigt een ander soort inzet of reactie dan wanneer de desinformatie afkomstig is van bijvoorbeeld één of meerdere individuen, zoals ook beschreven in eerdere kamerbrieven van het kabinet over de Rijksbrede strategie voor de effectieve aanpak van desinformatie.[20]

15) *Welke indicatoren worden in relatie tot de bron gehanteerd om te bepalen of de toegelichte interpretatie van toepassing is?*

Antwoord
Zoals in het antwoord op de voorgaande vraag is beschreven is de identiteit van de bron of afzender niet relevant voor de kwalificatie van informatie als desinformatie.

16) *Hoe wordt geborgd dat een individuele al dan niet ongelukkig geformuleerde mening niet als desinformatie geclassificeerd wordt?*

Antwoord
Dergelijke ongelukkig geformuleerde meningen vallen niet onder de definitie van desinformatie die het kabinet hanteert. Er is namelijk pas sprake van desinformatie wanneer misleidende informatie doelbewust en veelal heimelijk wordt verspreid met het doel om schade toe te brengen aan het publieke debat, democratische processen, de open kenniseconomie of de volksgezondheid. Als die intenties ontbreken dan is er geen sprake van desinformatie. De DSA geeft burgers daarbovenop het recht om klachten over content-moderatiebesluiten van platformen in te dienen bij een gratis te gebruiken intern klachtenafhandelingssysteem van het desbetreffende platform.

17, 18 en 19) *De leden van de GroenLinks-PvdA-fractie zijn verheugd te lezen dat de verordening ook poogt om minderjarigen te beschermen. In het kader van de harmonisatie die de verordening poogt te bewerkstelligen zijn de leden benieuwd wat er onder minderjarig wordt verstaan. Is dit voor het gehele Uniegebied hetzelfde, e.g. onder de 18 jaar? Of zijn er verschillen tussen verschillende landen? Indien er verschillen zijn, hoe pakken die verschillen uit ten aanzien van het toezicht dat de digitaledienstencoördinator moet uitvoeren? Voorziet de regering hier problemen en zo ja, hoe kunnen die problemen aangepakt worden?*

[20] Zie onder meer Kamerstukken II 2022/23, 30 821, nr. 173.

Antwoord
'Minderjarige' in de zin van de verordening is een autonoom Unierechtelijk begrip en dus niet afhankelijk van het recht van de lidstaten. De Europese Commissie heeft verduidelijkt dat minderjaren personen jonger dan 18 jaar zijn.[21]

20) *Het stemt de leden van de VVD-fractie tevreden dat niet-illegale, maar wel schadelijke inhoud, waaronder desinformatie, wel onder het bereik van de regels gericht op het voorkomen van systeemrisico's door zeer grote online platforms en zeer grote online zoekmachines valt. Deze leden vragen hoe hierop toezicht gehouden zal worden, aangezien de op nationaal niveau aangewezen bevoegde autoriteiten hier geen bevoegdheid tot hebben en de Commissie exclusief hiervoor verantwoordelijk is.*

Antwoord
Zoals de vragenstellers correct vaststellen is de Europese Commissie op grond van artikel 56, tweede lid, van de verordening, exclusief bevoegd om toezicht te houden op de verplichtingen voor zeer grote platformen en zoekmachines zoals neergelegd in afdeling 5 van hoofdstuk III van de verordening. Daaronder vallen ook de verplichtingen met betrekking tot de bestrijding van systeemrisico's. Daarbij zijn haar bevoegdheden en mogelijkheden ingekaderd door de verordening, met name in afdeling 4 van hoofdstuk 4 van de verordening. Zo kan de Europese Commissie bijvoorbeeld samen met de digitaledienstencoördinatoren kennis opbouwen en nationale experts detacheren (artikel 64 van de verordening), al dan niet in samenwerking met de digitaledienstencoördinatoren van de lidstaten inspecties uitvoeren (artikel 69 van de verordening) en een boete of last onder dwangsom opleggen (de artikelen 74 en 76 van de verordening). Ten behoeve van de rechtsbescherming moet de Europese Commissie voorafgaand aan een niet-nalevingsbesluit zeer grote platformen en zoekmachines in de gelegenheid stellen om te worden gehoord (artikel 79 van de verordening). De Commissie is recent twee formele procedures gestart om te onderzoeken of Meta en X deze verplichtingen om burgers te beschermen tegen de verspreiding van desinformatie hebben overtreden.[22] Hoe de Europese Commissie dat toezicht in de praktijk vorm zal geven, moet de komende tijd verder blijken.

21) *Deze leden vragen verder hoe gecontroleerd wordt of aanbieders van online platforms hun online interfaces, waarmee zij informatie van hun afnemers verspreiden, op een misleidende of manipulerende manier ontwerpen, organiseren of beheren (artikel 25 van de verordening). Worden algoritmen die extreme content voorrang geven hierin ook meegenomen? Dit ook met het oog op de motie van de leden Rajkowski en Dekker-Abdulaziz (Kamerstuk 30821-193[23]).*

Antwoord
Het begrip 'online-interface' wordt in artikel 3, onder m, van de verordening, gedefinieerd als "*alle software, met inbegrip van een website of onderdeel ervan, en apps, met inbegrip van mobiele apps*". Aanbevelingssystemen worden in artikel 3, onderdeel s, van de verordening gedefinieerd als "*een volledig of gedeeltelijk geautomatiseerd systeem dat door een onlineplatform wordt gebruikt om in zijn online-interface aan afnemers van de dienst specifieke informatie voor te stellen of prioritair weer te geven, onder meer als gevolg van een door de afnemer van de dienst geïnitieerde zoekopdracht, of dat anderszins de relatieve volgorde of het belang van de weergegeven informatie bepaalt*". In de (overwegingen van de) verordening wordt verder veelal gesproken over "*(...) op de online-interface*". Hieruit blijkt dat de online-interface de vormgeving of het ontwerp van een dienst betreft, en niet de onderliggende systemen zoals aanbevelingssystemen, APIs of cookies. Algoritmen die extreme content voorrang geven vallen dus niet onder het bereik van artikel 25 van de verordening. Voor dergelijke algoritmes of aanbevelingssystemen kent de verordening andere zelfstandige verplichtingen, zoals over transparantie van aanbevelingssystemen (artikel 27), de aanpassing van algoritimische en aanbevelingssystemen van zeer grote online platforms om systeemrisico's aan te pakken (artikelen 34 en 35) en de mogelijkheid om bij het gebruik van een

[21] Zie ook in dit document van de Europese Commissie waarin specifiek wordt ingegaan op de bescherming van minderjarigen onder de DSA: https://op.europa.eu/en/publication-detail/-/publication/f3556a65-88ea-11ee-99ba-01aa75ed71a1/language-en/format-PDF/source-296978213.

[22] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

[23] Motie van de leden Rajkowski en Dekker-Abdulaziz over zich op Europees niveau committeren aan het verbieden van ontwrichtende aanbevelingsalgoritmes.

zeer groot online platform te kiezen voor een aanbevelingssysteem dat niet gebaseerd is op profilering (artikel 38).

22) *De leden van de VVD-fractie vragen hoe het verwijderen van illegale content er precies uit gaat zien. Kan de regering het proces schetsen van plaatsen van illegale content tot verwijdering en eventuele opsporing en vervolging?*

Antwoord
Het proces van het verwijderen van door een gebruiker geplaatste illegale inhoud kan op twee manieren plaatsvinden: 1) op bevel van de overheid, zoals door de rechter in een civiele procedure, door een officier van justitie ter beëindiging van een strafbaar feit of door een bestuursorgaan; of 2) op basis van de algemene voorwaarden van een aanbieder, na eigen onderzoek van de aanbieder of een melding van een derde. De digitaledienstenverordening bevat bepalingen die bedoeld zijn om beide processen duidelijker, effectiever en gebruiksvriendelijker te maken. Wat betreft de bevelen van de overheid tot het verwijderen van illegale inhoud, bevat de verordening enkele aanvullende minimumeisen waar deze bevelen aan moeten voldoen en hoe aanbieders daarop moeten reageren. Wat betreft het verwijderen van illegale inhoud op basis van de algemene voorwaarden van aanbieders bevat de verordening een reeks aan zorgvuldigheidsverplichtingen, zoals de verplichting om de algemene voorwaarden zorgvuldig te formuleren en toe te passen (artikel 14), een gemakkelijk toegankelijk en gebruiksvriendelijk kennisgevings- en actiemechanisme in te richten (artikel 16), besluiten tot het verwijderen van informatie goed te motiveren (artikel 17), een klachtensysteem in te richten (artikel 20) en buitengerechtelijke geschillenbeslechting mogelijk te maken (artikel 21). Deze bepalingen bieden waarborgen voor zowel gebruikers wier inhoud wordt verwijderd als derden wier rechten door die inhoud worden geschonden.

3. Aansprakelijkheid van aanbieders van tussenhandeldiensten

23) *De leden van de D66-fractie constateren dat hosting partijen maatregelen moeten nemen om te voorkomen dat er illegale content wordt gehost. Kan de regering nogmaals verduidelijken hoe een actieve rol in deze precies wordt gedefinieerd en welke maatregelen daaronder vallen?*

Antwoord
Het begrip ‘actieve rol’ speelt een rol bij de beoordeling of een aanbieder van een hostingdienst een beroep kan doen op de aansprakelijkheidsvrijstelling voor de informatie van gebruikers die hij opslaat en doorgeeft. Het HvJEU heeft in zijn jurisprudentie namelijk bepaald dat aanbieders alleen een beroep kunnen doen op de vrijstelling als zij geen ‘actieve rol’ hebben ten aanzien van die informatie. Dat is het geval als de aanbieder kennis van of controle heeft over de gegevens in plaats van zich te beperken tot een neutrale levering van die dienst met behulp van een louter technische en automatische verwerking van de gegevens die hem door zijn klanten zijn verstrekt.[24] Als voorbeelden van– mogelijk – actieve bemoeienis noemt het HvJ EU in zijn rechtspraak het verlenen van hulp door de tussenpersoon bij het schrijven van advertenties of bij het vaststellen of selecteren van trefwoorden.[25] Hetzelfde geldt voor het promoten van specifieke verkoopaanbiedingen of de aanbiedingen van een specifieke verkoper door de tussenpersoon.[26] Dit zijn immers handelingen die kunnen leiden tot kennis van en/of controle over specifieke inhoud die de tussenpersoon op verzoek van zijn gebruikers opslaat.

Het niet vervullen van een ‘actieve rol’ van een aanbieder ten aanzien van de door hem opgeslagen en doorgegeven inhoud van zijn gebruikers, is een voorwaarde om een beroep te kunnen doen op de aansprakelijkheidsvrijstelling die voor deze aanbieders geldt. Hieruit volgt dus, anders dan in de vraag wordt gesteld, geen verplichting om maatregelen te nemen om te voorkomen dat er illegale content wordt gehost. Het opleggen van een dergelijke verplichting wordt beperkt door het verbod op een algemene verplichting tot monitoring of actief feitenonderzoek (artikel 8 van de verordening). Het HvJ EU heeft echter bevestigd dat het verbod op algemeen toezicht niet geldt

[24] Zie onder meer HvJ EU 23 maart 2010, zaak C-236/08, ECLI:EU:C:2010:159 (Google France), r.o. 120.

[25] HvJ EU 23 maart 2010, zaak C-236/08, ECLI:EU:C:2010:159 (Google France), r.o. 117–118.

[26] HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L’Oréal/eBay), r.o. 116.

voor toezichtverplichtingen in ‘speciale gevallen’. Een dergelijk speciaal geval kan zijn informatie die door een hostingprovider is opgeslagen op verzoek van een bepaalde gebruiker en waarvan de inhoud is onderzocht en beoordeeld door een bevoegde rechterlijke instantie, die deze informatie onwettig heeft verklaard. In zo’n situatie kan aan de hostingprovider een bevel worden opgelegd om opgeslagen informatie die inhoudelijk identiek is aan informatie die eerder onwettig is verklaard, te verwijderen om te voorkomen dat de betrokken belangen verder worden geschaad.[27]

24) *De verordening stelt regels over het geven van bevelen die nationale gerechtelijke of bestuursrechtelijke autoriteiten aan aanbieders van tussenhandeldiensten kunnen richten ten aanzien van het bestrijden van illegale inhoud, maar creëert echter geen wettelijke grondslag voor het geven van deze bevelen. Hoe kijkt de regering naar het ontbreken van deze grondslagen, zo vragen de leden van de D66-fractie.*

Antwoord
Het begrip ‘illegale inhoud’ is zeer breed en omvat ingevolge artikel 3, onderdeel h, van de verordening alle informatie die op zichzelf of in verband met een activiteit, waaronder de verkoop van producten of het aanbieden van diensten, indruist tegen het Unierecht of het recht van een lidstaat. De verordening harmoniseert dus niet welke inhoud illegaal is. De vraag of informatie illegaal is, valt daarmee buiten de reikwijdte van de verordening. De beoordeling van die vraag dient te geschieden op basis van het toepasselijke Unierecht of het toepasselijke recht van de lidstaten. Dat toepasselijke Unierecht of lidstatelijk recht dient ook te voorzien in passende mogelijkheden voor toezicht en handhaving, waaronder de bevoegdheid voor een gerechtelijke of bestuursrechtelijke autoriteit om bevelen te geven om illegale online inhoud te bestrijden.

Het kabinet vindt het in het licht van deze brede definitie van ‘illegale inhoud’ logisch dat de verordening niet voorziet in een grondslag voor de toezichthouder op de naleving van de verordening om bevelen te geven om illegale inhoud te bestrijden. Het is volgens het kabinet wenselijk dat een dergelijke bevelbevoegdheid zijn grondslag vindt in de wetgeving die ook de materiële normen bevat op grond waarvan de online informatie illegaal is. Het is aan de wetgever in kwestie om te bepalen welke gerechtelijke of bestuursrechtelijke autoriteit die bevoegdheid het beste kan uitoefenen en welke voorwaarden voor de uitoefening van die bevoegdheid moeten gelden.

25) *De leden van de D66-fractie constateren dat het Europese Hof van Justitie heeft geoordeeld dat van een verlener van de online dienst niet kan worden verlangd het actief surveilleren van alle gegevens van al zijn klanten om elke toekomstige inbreuk op intellectuele-eigendomsrechten te voorkomen. Geldt er daardoor een recht op encryptie, zo vragen deze leden?*

Antwoord
Het verbod om algemene monitoringsverplichtingen op te leggen aan aanbieders (artikel 8 van de verordening) is gericht aan de Europese en nationale overheid. Het vormt een beperking op de mogelijkheden die zij hebben om tussenhandeldiensten te verplichten tot monitoring van informatie, en de bevoegdheid die nationale rechters hebben om te verplichten tot monitoring. Uit artikel 4, derde lid, artikel 5, tweede lid, en artikel 6, vierde lid van de verordening volgt namelijk dat nationale rechters wel een bevoegdheid hebben om de beëindiging van een inbreuk te beëindigen of voorkomen. Het (opnieuw) voorkomen van een inbreuk kan monitoring noodzakelijk maken. De jurisprudentie van het HvJEU waar de vragenstellers naar verwijzen, verduidelijkt dat nationale rechters niet de bevoegdheid hebben om te verplichten tot het soort algemene monitoring dat in die zaken werd verzocht. Uit het verbod om algemene monitoringsverplichtingen op te leggen aan aanbieders en de jurisprudentie van het HvJEU daarover kan echter niet worden afgeleid dat klanten of gebruikers van tussenhandeldiensten een recht op encryptie hebben.

3.1. Het kader voor aansprakelijkheid van tussenhandeldiensten voor door afnemers verstrekte informatie

[27] HvJ EU 3 oktober 2019, zaak C-18/18, ECLI:EU:C:2019:821 (Glawischnig-Piesczek).

26 en 27) *De leden van de VVD-fractie lezen dat er verschillende aansprakelijkheidsvrijstellingen zijn waar tussenhandeldiensten een beroep op kunnen doen. Deze leden vragen hierbij of het voldoende afgebakend is wanneer een dienst hier recht op heeft. Tegelijkertijd zijn deze leden benieuwd naar de mogelijkheid om misbruik te maken van deze regelingen. Hoe wordt er gezorgd dat alleen zij die recht hebben op vrijstelling, hier ook gebruik van kunnen maken?*

Antwoord
De voorwaardelijke aansprakelijkheidsvrijstellingen voor aanbieders van tussenhandeldiensten in de digitaledienstenverordening zijn een voortzetting van de vrijstellingen die voorheen golden op grond van de richtlijn elektronische handel. Er is veel jurisprudentie van het HvJEU en van de nationale rechter die nadere invulling geven van de voorwaarden die gelden voor de aansprakelijkheidsvrijstellingen. Uit de overwegingen bij de verordening volgt dat aanbieders, die opzettelijk samenwerken met een afnemer om illegale activiteiten te ontplooien, geen beroep kunnen doen op de aansprakelijkheidsvrijstellingen. Deze beperking is relevant voor de Nederlandse handhavingspraktijk. Zo blijkt uit onderzoeken dat de Nederlandse hostingsector veelvuldig wordt gebruikt door criminelen voor het plegen van strafbare feiten. Criminaliteit wordt bewust gefaciliteerd door malafide hostingbedrijven (*bullet proof* hosting) dan wel onwetende hostingbedrijven die zeer weinig maatregelen nemen (*bad* hosting).[28] Van malafide hostingbedrijven is duidelijk dat zij opzettelijk samenwerken met een afnemer om illegale activiteiten te ontplooien en uit dien hoofde geen beroep kunnen doen op de vrijstelling van aansprakelijkheid. Bij de groep onwetende hostingbedrijven die zeer weinig maatregelen nemen hangt het van de omstandigheden van het geval af of gesteld kan worden dat zij opzettelijk samenwerken met een afnemer om illegale activiteiten te ontplooien en uit dien hoofde geen beroep kunnen doen op de vrijstelling van aansprakelijkheid. Het uiteindelijke oordeel daarover is aan de rechter.

3.2. Eisen aan bevelen om op te treden tegen illegale inhoud of om informatie te verstrekken

28) *De leden van de VVD-fractie vragen, gezien er verschillende eisen zijn die gelden als het gaat om het optreden tegen illegale inhoud of om informatie te verstrekken, in welk tijdsbestek er opgetreden kan worden tegen illegale inhoud. In de digitale wereld is elke seconde dat er illegale inhoud online staat, één seconde teveel. Daarom denken de leden dat het noodzakelijk is om snel te handelen in deze situaties. In hoeverre laat de verordening dit toe?*

Antwoord
Zoals is uiteengezet in het antwoord op vraag 22, geschiedt het optreden tegen door een gebruiker geplaatste illegale inhoud op twee manieren: 1) op bevel van de overheid, zoals door de rechter in een civiele procedure, door een officier van justitie ter beëindiging van een strafbaar feit of door een bestuursorgaan; of 2) op basis van de algemene voorwaarden van een aanbieder, na eigen onderzoek van de aanbieder of een melding van een derde.

Als er sprake is van een bevel van de overheid, dan laat de verordening het aan het toepasselijke nationale of EU-recht om te bepalen binnen welke termijn de aanbieder actie moet ondernemen. Bij wijze van voorbeeld kan worden gewezen op de verordening terroristische online-inhoud, waarin is bepaald dat een verwijderbevel met betrekking tot terroristische inhoud binnen één uur moet worden uitgevoerd (artikel 3, derde lid). De DSA regelt wel dat de aanbieder het betreffende overheidsorgaan onverwijld op de hoogte moet stellen van welke actie hij naar aanleiding van het bevel heeft ondernomen (artikel 9, eerste lid).

Als sprake is van meldingen van gebruikers of van derden, dan schrijft de verordening voor dat er “tijdig” moet worden besloten over meldingen van illegale inhoud (artikel 16, zesde lid). Wat tijdig betekent, hangt blijkens overweging 52 bij de verordening af van het type illegale inhoud en de urgentie om actie te ondernemen. Als algemeen horizontaal kader is de verordening immers van toepassing op alle soorten illegale inhoud. Zo dienen aanbieders van hostingdiensten onverwijld te handelen als het strafbare feiten betreft die een bedreiging vormt voor het leven of de veiligheid van personen. Voor dat soort strafbare feiten geldt er ook een plicht om die te melden bij de

[28] Zie onder meer Kamerstukken II, 2019/20, 26 643, nr. 696, blz. 5.

bevoegde rechtshandhavingsinstanties, in Nederland is dat de politie (artikel 18 van de verordening).

Meldingen die afkomstig zijn van een betrouwbare flagger moeten tot slot “prioritair en onverwijld” worden verwerkt en afgehandeld (artikel 22). Dit betekent dat hun meldingen in de praktijk (veelal) voorrang krijgen op andere meldingen, hetgeen de prioritering bij het afhandelen van meldingen beïnvloedt. Om goed uitvoering te kunnen geven aan de verplichting om tijdig een beslissing te nemen moet het mogelijk zijn voor aanbieders van hostingdiensten en online platformen, waaronder zeer grote online platformen en zoekmachines, om te prioriteren bij de afhandelingen van meldingen.[29]

De verordening voorziet aldus in een gebalanceerd kader dat rekening houdt met het feit dat het van toepassing is op verschillende soorten van illegale inhoud en de beperking qua automatische middelen en menselijke beoordeling en dat oververwijdering van informatie beoogt te voorkomen. De verordening laat bovendien ruimte voor het stellen van nadere termijnen voor specifieke vormen van illegale inhoud indien de nationale of EU-wetgever dat nodig acht.

4. Zorgvuldigheidsverplichtingen voor aanbieders van tussenhandeldiensten

29 en 30) *In hoeverre hebben overheidsorganisaties nu de status van ‘betrouwbare flaggers’ toegediend gekregen en in hoeverre behouden zij deze status? In hoeverre is dit wenselijk volgens de regering, zo vragen de leden van de D66-fractie?*

Antwoord
Het is positief dat er verschillende aanbieders van hostingdiensten en online platformen zijn die op dit moment op basis van vrijwilligheid goed samenwerken met overheidsorganisaties die illegale inhoud tegengaan, zoals de NVWA of het openbaar ministerie.[30] De verordening verzet zich niet tegen deze vrijwillige samenwerking. Uiteraard is het daarbij van belang dat voor de geadresseerden helder is welk juridisch kader van toepassing is als een overheidsorganisatie contact opneemt: gaat het om een melding in de hoedanigheid van ‘trusted flagger’ onder de verordening of in het kader van de Gedragscode Notice and Takedown (NTD) of gaat het om een formeel bevel van een officier van justitie op grond van het Wetboek van Strafvordering of van een bestuursorgaan.

Voor de goede orde wordt opgemerkt dat er in Nederland nog geen organisaties zijn, en dus ook geen overheidsorganisaties, die over de status van ‘betrouwbare flagger’ in de zin van de verordening beschikken. Die status moet op grond van de verordening toegekend worden door de digitaledienstencoördinatoren in de lidstaten (artikel 22). Hoewel de ACM voorlopig is aangewezen[31] als digitaledienstencoördinator voor Nederland, heeft zij die bevoegdheid tot het toekennen van deze status pas zodra onderhavige uitvoeringswet in werking is getreden.

Op grond van artikel 22 van de verordening kunnen ‘entiteiten’, die aan een aantal criteria voldoen, de status van ‘betrouwbare flagger’ krijgen. Het begrip ‘entiteit’ is een breed begrip, dat zowel publieke als private organisaties omvat. Wel beschouwt het kabinet de status van ‘betrouwbare flagger’ als iets dat met name geschikt is voor private handhaving door private organisaties. Het aanvragen van de status van betrouwbare flagger onder de verordening door overheidsorganisaties en toezichthouders lijkt weinig toegevoegde waarde te hebben. De praktijk laat immers zien dat overheidsorganisaties en toezichthouders veelal vrijwillige afspraken hebben of maken met online platforms en tussenhandeldiensten op basis waarvan illegale inhoud gemeld en verwijderd kan

[29] In dit kader wordt gewezen op de DSA Transparancy Database die de Europese Commissie heeft ingericht ter uitvoering van artikel 24, vijfde lid, van de verordening (https://transparency.dsa.ec.europa.eu/). In die openbaar toegankelijke database worden besluiten over meldingen van illegale inhoud bij aanbieders van online platformen opgenomen. Aanbieders van zeer grote online platformen en zoekmachines zijn daar sinds 25 augustus 2023 op aangesloten, en andere online platformen zijn daar sinds 17 februari 2023 mee begonnen. Uit de database blijkt dat er sinds 25 augustus 2023 meer dan 17 miljard besluiten over meldingen van illegale inhoud zijn genomen, waarvan 69% volledig geautomatiseerd. De enorme omvang van het aantal besluiten dat aanbieders van online platformen moeten nemen illustreert de druk die de beoordeling van meldingen oplevert voor de organisatie en middelen van die aanbieders en dientengevolge de noodzaak om enige flexibiliteit te hebben bij de beoordeling daarvan.

[30] Zie ook de memorie van toelichting bij de Wet Computercriminaliteit III (Kamerstukken II 2015/16, 34372, nr. 3).

[31] Besluit voorlopige aanwijzing ACM als bevoegde autoriteit en digitaledienstencoördinator digitaledienstenverordening (Stcrt. 2024, nr. 3993).

worden. Bovendien beschikken overheidsorganisaties en toezichthouders vaak over wettelijke bevoegdheden om bevelen uit te vaardigen teneinde illegale inhoud onverwijld verwijderd te krijgen. Gelet op deze praktijk, lijkt het niet veel toe te voegen als overheidsorganisaties en toezichthouders een formele status als 'betrouwbare flagger' bij de digitaledienstencoördinator zouden aanvragen. Op die manier wordt ook bijgedragen aan het in overweging 61 genoemde streven tot het beperkt houden van het aantal personen en organisaties aan wie de status van 'betrouwbare flagger' wordt toegekend, hetgeen de werkbaarheid van het systeem van artikel 22 van de verordening ten goede komt.

31) *De leden van de D66-fractie zien bij de maatregelen voor minderjarigen nog weinig terug over het versterken van de leeftijdsverificatie voor platforms met leeftijdsvereisten. In hoeverre zijn er verplichtingen die voortvloeien vanuit de verordening op dit gebied, zo vragen deze leden?*

Antwoord
De verordening verplicht niet tot het gebruik van leeftijdsverificatie. Wel bevat de verordening een aantal verplichtingen die de bescherming van minderjarigen moet verbeteren, zoals de verplichting om passende en evenredige beschermingsmaatregelen te nemen (artikel 28). Ook is de bescherming van minderjarigen aangewezen als systeemrisico, die door zeer grote online platforms moet worden geïdentificeerd en aangepakt (artikel 34, eerste lid, onder b en d en artikel 35, eerste lid, onder j), van de verordening. Leeftijdsverificatie is een van de maatregelen die aanbieders van onlinediensten kunnen treffen om de bescherming van minderjarigen binnen hun dienst te verbeteren. De verplichtingen voor online dienstenaanbieders om maatregelen te nemen om minderjarigen te beschermen uit zowel de DSA als de richtlijn audiovisuele mediadiensten (2018/1808/EU) kunnen online platformen stimuleren om de leeftijd van gebruikers te gaan verifiëren. De Europese Commissie heeft mede ten behoeve daarvan een aantal maanden geleden een '*Task Force on Age Verification*' ingesteld.[32] Daar worden de initiatieven die inmiddels in diverse lidstaten zijn gestart bij elkaar gebracht om zo effectief invulling te kunnen geven aan de verplichtingen uit de DSA en de Audiovisuele Mediadienstenrichtlijn. De ambitie van de Europese Commissie is om uiteindelijk tot een geharmoniseerd kader te komen van standaarden waar leeftijdsverificatiesystemen aan moeten voldoen. Dat kan vervolgens als leidraad dienen voor de (door-)ontwikkeling van technische middelen voor leeftijdsverificatie. Het kabinet draagt daar actief aan bij. Op 9 april jl. heeft de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties een afwegingskader leeftijdsverificatie met uw Kamer gedeeld. Het afwegingskader heeft als doel om ontwikkelaars te helpen om een passende vorm van leeftijdsverificatie voor hun online product of dienst te ontwikkelen en biedt een routekaart voor de afweging van de verschillende belangen die daarbij zijn gemoeid.[33] Dat kader is inmiddels ook met de Europese Commissie gedeeld.

4.1. Verplichtingen die gelden voor alle aanbieders van tussenhandeldiensten

32) *De leden van de GroenLinks-PvdA-fractie lezen dat uit overweging 51 bij de verordening volgt dat elke inhoudsmoderatie strikt gericht moet zijn op de specifieke onderdelen die als illegale inhoud of in strijd met de algemene voorwaarden worden beschouwd, zonder de vrijheid van meningsuiting en van informatie van afnemers van de dienst onnodig aan te tasten. De leden vragen of de regering kan reflecteren op de situatie wanneer de algemene voorwaarden verder gaan dan de maatschappelijke moraal, zowel wanneer het hostingdiensten als zeer grote online platforms betreft. Het specifieke voorbeeld waar de leden van de GroenLinks-PvdA-fractie op doelen betreft het tonen van mannelijke en vrouwelijke tepels. Sommige hostingdiensten en zeer grote online platforms verbieden het tonen van vrouwelijke, maar niet het tonen van mannelijke tepels, vanuit een maatschappelijk puriteins moraal uit het land van oorsprong dat anders ligt dan de Nederlandse en/of Europese moraal. En er zijn meer voorbeelden te bedenken waarin de moraal van het hostingdienst of zeer grote online platform verschilt van de maatschappelijke moraal in Nederland. Kan de regering hierop reflecteren?*

Antwoord

[32] https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0.

[33] Kamerstukken II 2023/24, 26 643, nr. 1149.

Aanbieders van tussenhandeldiensten hebben een contractuele verhouding met de afnemers van hun diensten. De inhoud daarvan ligt vast in de algemene voorwaarden die de aanbieders hanteren. In deze algemene voorwaarden hebben aanbieders van tussenhandeldiensten vaak opgenomen dat het hun gebruikers niet is toegestaan om bepaalde inhoud te plaatsen, als die informatie illegaal is of omdat de aanbieder die informatie anderszins onwenselijk vindt. Ook staat in de algemene voorwaarden vermeld wat de gevolgen zijn als er wel illegale inhoud wordt geplaatst, zoals verwijdering van de informatie. Dit wordt ook wel inhoudsmoderatie genoemd.

Voor dergelijke contractuele verhoudingen geldt het beginsel van contractvrijheid: het staat partijen binnen de grenzen van het recht vrij om contracten te sluiten en de inhoud en vorm van het contract te bepalen. Dit raakt ook aan de vrijheid van ondernemerschap van de aanbieder. Hieruit volgt dat het in beginsel aan de aanbieder van de tussenhandeldienst is om te bepalen welke inhoud hij wel of niet wenselijk vindt op zijn dienst, ook als dat verder gaat dan er wordt voorgeschreven door wet- of regelgeving. Dat zal onvermijdelijk soms botsen met de moraal van sommige mensen en overeenkomen met de moraal van anderen, zeker als de aanbieder in veel verschillende landen actief is. Het is vervolgens aan de gebruiker of hij wel of niet gebruik wenst te maken van de dienst, of om een geschil over een concreet inhoudsmoderatiebesluit aan de rechter voor te leggen als hij het oneens is met het besluit, bijvoorbeeld omdat zijn recht op vrijheid van meningsuiting wordt geschonden. Het is belangrijk dat de overheid zich hier terughoudend opstelt en ruimte aan burgers en bedrijven laat om zelf keuzes te maken.

De contractvrijheid kan om redenen van algemeen belang worden ingeperkt. De digitaledienstenverordening bevat daarom regels over de algemene voorwaarden inzake inhoudsmoderatie van deze aanbieders, in het belang van de transparantie, de bescherming van afnemers en het voorkomen van oneerlijke of willekeurige resultaten. Het is kort gezegd verplicht voor aanbieders om in hun algemene voorwaarden duidelijk en begrijpelijk te formuleren wat hun beleid is ten aanzien van inhoudsmoderatie. Verder moeten aanbieders bij het ontwerpen, toepassen en handhaven van dat beleid op een niet-willekeurige en niet-discriminerende wijze te werk gaan. Ook moeten zij gepaste aandacht hebben voor de rechten en legitieme belangen van alle betrokkenen, waaronder de vrijheid van meningsuiting, de vrijheid van informatie en de pluriformiteit van de media. Deze grondrechten zijn op Europees niveau vastgelegd in het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag voor de Rechten van de Mens. Ook vergemakkelijkt de verordening het voor gebruikers om op te komen tegen inhoudsmoderatiebesluiten van aanbieders, bijvoorbeeld door de verplichting om dergelijke besluiten duidelijk en nauwkeurig te motiveren en de verplichting voor aanbieders van onlineplatforms om een intern klachtenafhandelingssysteem in te richten en door buitengerechtelijke geschilbeslechting mogelijk te maken.

33) *Acht de regering het wenselijk dat private bedrijven een moraal die anders is dan onze waarden op kunnen dringen? Kan de regering hierin een onderscheid maken tussen hostingdiensten en zeer grote online platforms?*

Antwoord
Het is belangrijk dat burgers en bedrijven de keuze hebben uit verschillende hostingdiensten en online platforms, zodat ze zich niet gedwongen voelen om te handelen naar de regels en de daarin besloten moraal van een specifieke aanbieder. Daarom is het belangrijk dat er voldoende concurrentie is, en dat toetredingsdrempels laag worden gehouden zodat bestaande ondernemingen uitgedaagd kunnen worden. Dit wordt onder meer bereikt door de ruime uitzonderingen in de verordening voor het micro- en kleinbedrijf.

Voor zover een onderscheid tussen hostingdiensten en zeer grote online platforms relevant is, is dat gelegen in de mogelijkheden die zij hebben om inhoud te verwijderen of ontoegankelijk te maken. Een pure hostingdienst kan veelal niet ingrijpen op het niveau van specifieke inhoud, maar wel op het niveau van een hele website. Bijvoorbeeld door die ontoegankelijk te maken. Als de betreffende website ook legale informatie bevat dan leidt dit tot oververwijdering en mogelijk een disproportionele beperking van de vrijheid van meningsuiting. Online platforms hebben veelal wel de mogelijkheid om specifieke inhoud te verwijderen. Daarmee heeft optreden door online platforms over het algemeen een minder verstrekkende invloed dan door hostingbedrijven.

34) *Welke mogelijkheden biedt de DSA om op te treden tegen dit soort onwenselijke algemene voorwaarden?*

Antwoord
Zoals in het antwoord op vraag 32 is uiteengezet, volgt uit de verordening dat aanbieders van tussenhandeldiensten in hun algemene voorwaarden op duidelijke en begrijpelijke wijze hun inhoudsmoderatiebesluit moeten formuleren. Bij het formuleren van dat beleid moeten zij op een niet-willekeurige en niet-discriminerende wijze te werk gaan, met gepaste aandacht voor de legitieme belangen en fundamentele rechten van alle betrokkenen. Hiermee bevestigt de verordening dat grondrechten (indirecte) horizontale werking hebben in dit soort private verhoudingen. Hoewel de contractvrijheid van de aanbieder van een tussenhandeldienst het uitgangspunt is en blijft, is deze vrijheid dus niet onbegrensd. Hiermee wordt bijgedragen aan de doeltreffende bescherming van de in het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag voor de Rechten van de Mens gewaarborgde grondrechten.

Bij de inhoudsmoderatie door aanbieders van tussenhandeldiensten zijn verschillende grondrechten in het geding. Er is geen rangorde tussen deze verschillende grondrechten. De grondrechten zijn gelijkwaardig aan elkaar. Wanneer meerdere grondrechten in een bepaalde situatie botsen, moet een juist evenwicht worden verzekerd tussen de botsende rechten door deze tegen elkaar af te wegen. De rechtspraak van het HvJ EU maakt duidelijk dat van een ‘juist evenwicht’ geen sprake is als één of meer grondrechten in de «kern» worden geraakt.[34] Dit sluit aan bij de beperkingsclausule neergelegd in artikel 52, eerste lid, van het Handvest, die voorschrijft dat beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden onder meer de ‘wezenlijke inhoud’ van die rechten en vrijheden moeten eerbiedigen. Een maatregel die leidt tot een ernstige aantasting van een in het Handvest beschermd recht voldoet niet aan het vereiste dat een juist evenwicht wordt verzekerd tussen de met elkaar in overeenstemming te brengen grondrechten.

Gebruikers of derden kunnen, in het kader van de interne klachtenprocedures, buitengerechtelijke geschillenbeslechting of bij de civiele rechter, opkomen tegen inhoudsmoderatiebesluiten van aanbieders. Dit kan bijvoorbeeld ook als de algemene voorwaarden zelf aan de eisen van de verordening voldoen, maar in de praktijk door de aanbieder op onzorgvuldige wijze worden toegepast. De genoemde instanties kunnen ook doeltreffende remedies opleggen, zoals bevelen dat de inhoud wordt verwijderd of juist wordt teruggeplaatst, of in het geval van de civiele rechter, het vaststellen van een schadevergoeding.

Gebruikers en derden kunnen voorts op grond van artikel 53 van de verordening een klacht indienen bij de digitaledienstencoördinator, in Nederland de ACM, als zij menen dat een aanbieder een inbreuk op deze onderdelen van de verordening heeft begaan. Het toezicht op deze bepaling zal zich primair richten op de vraag of een aanbieder daadwerkelijk in zijn algemene voorwaarden een duidelijk en begrijpelijk inhoudsmoderatiebeleid heeft opgenomen. Het is primair aan de aanbieder zelf om dat beleid in te vullen en daarbij de aan de orde zijnde belangen en rechten af te wegen. Dit volgt uit de in het antwoord op vraag 32 genoemde contractvrijheid en de vrijheid van ondernemerschap. Wel volgt uit de verordening dat het beleid niet-willekeurig en niet-discriminerend moet zijn en dat er gepaste aandacht moet zijn voor de legitieme belangen en fundamentele rechten van alle betrokkenen. Het is aan de ACM om daar in een concreet geval een oordeel over te vormen en eventueel tot handhaving over te gaan.

35) *Wordt optreden tegen dit soort onwenselijke algemene voorwaarden bemoeilijkt wanneer het hoofdkantoor of de wettelijk vertegenwoordiger van een hostingdienst of zeer groot online platform zich in een Unieland bevindt waarin de moraal eveneens verschilt van de Nederlandse? Deze leden zijn zeer benieuwd naar een uitgebreide reflectie van de regering.*

Antwoord
Zoals is uiteengezet in het antwoord op vraag 34, zijn aanbieders van tussenhandeldiensten op grond van de verordening gehouden om bij het vormgeven en toepassen van hun

[34] Zie onder meer HvJ EU 24 november 2011, zaak C-70/10, ECLI:EU:C:2011:771 (Scarlet/SABAM), r.o. 48 en 49, HvJ EU 16 februari 2012, zaak C-360/10, ECLI:EU:C:2012:85 (SABAM/Netlog), r.o. 46 en 47.

inhoudsmoderatiebesluit een juist evenwicht te verzekeren tussen door de Unie beschermde grondrechten en niet om rekening te houden met de moraal van de lidstaat waar zij gevestigd zijn of waar zij hun diensten aanbieden. De toezichthouders op de naleving van deze bepalingen van de verordening en de bevoegde rechters in de lidstaten maken dus gebruik van hetzelfde normenkader bij het beoordelen van dit beleid, namelijk het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag voor de Rechten van de Mens. De samenwerking van de digitaledienstencoördinatoren met elkaar en met de Europese Commissie draagt verder bij aan een uniforme uitleg en toepassing van deze regels. Een uniforme uitleg is tevens geborgd omdat het HvJEU in laatste instantie bevoegd is om uitleg te geven aan deze regels.

4.2. Aanvullende verplichtingen voor online platforms

36) *De leden van de GroenLinks-PvdA-fractie zijn blij te lezen dat de schorsing van gebruikers dankzij de verordening aan regels wordt gebonden. De aanbieder zal pas tot schorsing kunnen overgaan, als hij in meerdere afzonderlijke gevallen heeft vastgesteld dat door een gebruiker verstrekte informatie illegaal is of een door een klager ingediende klacht ongegrond is. Wat betreft de mogelijkheid van bevelen van een administratieve of gerechtelijke autoriteit: artikel 23 van de verordening komt pas in beeld als bepaalde misbruik zich frequent heeft voorgedaan. Kan de regering aangeven wat het verstaat onder ¨frequent¨ misbruik? Is het aan de ACM om hier zelf richtlijnen voor op te stellen?*

Antwoord
Het begrip ‘frequent’ zoals gebruikt in artikel 23, eerste lid, van de verordening is een autonoom Unierechtelijk begrip en de verordening geeft geen definitie of nadere invulling daarvan. Van het frequent verstrekken van illegale inhoud of het frequent doen van ongegronde meldingen of klachten is bijvoorbeeld sprake als een gebruiker, persoon of entiteit meerdere keren dezelfde illegale inhoud verstrekt of dezelfde ongegronde melding of klacht doet, ook nadat is vastgesteld dat de betreffende inhoud illegaal is of de melding of klacht ongegrond.

Artikel 23 van de verordening biedt de ruimte aan aanbieders van online platforms om zelf hun beleid ten aanzien van dit soort misbruik te bepalen. Zij zijn op grond van het vierde lid wel verplicht om dat beleid duidelijk en gedetailleerd in hun algemene voorwaarden op te nemen en daarbij voorbeelden te geven van de feiten en omstandigheden waar zij rekening mee houden bij het vaststellen van misbruik en bij het bepalen van een redelijke schorsingstermijn. Aanbieders moeten bij besluiten over schorsingen rekening houden met alle relevante feiten en omstandigheden van het geval, waaronder het aantal keer dat een afnemer de fout in is gegaan, de ernst en de gevolgen daarvan en de intenties van de afnemer, melder of klager (artikel 23, derde lid, van de verordening).

De ACM is op grond het wetsvoorstel belast met het toezicht op de naleving van deze bepaling en zal daarbij tot een eigen interpretatie van het begrip ‘frequent’ dienen te komen Ook de digitaledienstenraad kan nadere uitleg geven en zo uitvoering geven aan haar opdracht om bij te dragen aan de consistente toepassing van de verordening (artikel 61, tweede lid, onder a, van de verordening), bijvoorbeeld door het uitbrengen van een aanbeveling (artikel 63, eerste lid, onder b, van de verordening). De uitleg van de verordening is tot slot uiteindelijk aan het Hof van Justitie van de Europese Unie.

37) *Kan de regering reflecteren op mogelijke verschillen tussen de zienswijze van de ACM en de algemene voorwaarden van aanbieders van online platforms ten aanzien van frequent misbruik? Is de visie van de ACM of zijn de algemene voorwaarden leidend?*

Antwoord
Het begrip ‘frequent’ in artikel 23 van de verordening is een autonoom Unierechtelijk begrip. De uitleg daarvan is uiteindelijk aan het Hof van Justitie, en niet de uitleg van de bevoegde autoriteiten, of die van een tussenhandeldienst zoals een online platform. In de tussentijd is het in Nederland aan de ACM om te beoordelen wat ‘frequent’ in de praktijk inhoudt en daar desnoods op te handhaven. Daarbij moet wel worden opgemerkt dat de algemene voorwaarden onderdeel van een privaatrechtelijke overeenkomst zijn waar in principe contractvrijheid voor bestaat en niet alle

online platformen en soorten illegale inhoud eenzelfde behandeling vragen. Het is dan ook mogelijk dat het wenselijk en nodig is om enige flexibiliteit te behouden bij het uitleggen van ‘frequent’ in de zin van artikel 23 van de verordening.

38 en 39) *Ook lezen de leden van de GroenLinks-PvdA-fractie dat zogenoemde ¨dark patterns¨ verboden worden. Ten aanzien van zaken als cookieconsent pop-ups zijn deze op basis van de AVG reeds verboden. Toch zien deze leden dat er veelvuldig gebruik wordt gemaakt van dark patterns in de vormgeving van deze cookieconsent pop-ups. Kan de regering aangeven of zij denkt dat de Autoriteit Persoonsgegevens (AP) en ACM genoeg capaciteit hebben om hier goed en gericht toezicht op te houden? Denkt de regering dat de DSA tot een wezenlijke verandering en verbetering voor afnemers gaat leiden als de toezichtcapaciteit tekortschiet en zo ja, waarom denkt de regering dat dat het geval is als het naar aanleiding van de AVG nog niet tot het gewenste resultaat heeft geleid ten aanzien van cookieconsent pop-ups?*

Antwoord
De door de vragenstellers beschreven regels inzake ‘dark patterns’ zijn vastgelegd in artikel 25 van de verordening. Artikel 25 van de verordening stelt regels aan de ‘online-interface’ van online platforms. Daaronder wordt ‘alle software, met inbegrip van een website of onderdeel ervan, en apps, met inbegrip van mobiele apps’ verstaan (artikel 3, onderdeel m, van de verordening). Cookie-consent pop-ups kunnen dus een onderdeel van de online-interface zijn.

Uit het tweede lid van artikel 25 van de verordening volgt dat het verbod op ‘dark patterns’ niet geldt voor praktijken die vallen onder de reikwijdte van de richtlijn oneerlijke handelspraktijken[35] en de algemene verordening gegevensbescherming.[36] Die richtlijn en verordening bieden voor die praktijken voldoende bescherming tegen misleidende of manipulerende technieken.

Op het gebruik van cookieconsent pop-ups is artikel 11.7a van de Telecommunicatiewet van toepassing, ter implementatie van artikel 5, derde lid, van de richtlijn privacy en elektronische communicatie.[37] Als bij het toepassen van cookies persoonsgegevens worden verwerkt, dan is ook de algemene verordening gegevensbescherming van toepassing. In artikel 11.7a, vierde lid, van de Telecommunicatiewet is aanvullend bepaald dat het gebruik van zogenoemde tracking cookies wordt vermoed een verwerking van persoonsgegevens te zijn.

Uit het voorgaande volgt dat als het gebruik van cookies de verwerking van persoonsgegevens inhoudt, dat dan de algemene verordening gegevensbescherming van toepassing is en niet artikel 25 van de digitaledienstenverordening. Als het gebruik van cookies geen verwerking van persoonsgegevens inhoudt, dan is artikel 25 van de digitaledienstenverordening wel van toepassing.

Over welke toezichthouder in een concreet geval bevoegd is, de AP in het kader van de algemene verordening gegevensbescherming of de ACM in het kader van de digitaledienstenverordening, zal in de praktijk afstemming moeten plaatsvinden tussen beide toezichthouders. Het uitvoeringswetsvoorstel bevat regels over deze samenwerking en in de praktijk kan er worden aangesloten bij de samenwerking die over dit onderwerp al plaatsvindt tussen AP en ACM waar het gaat om de afstemming van het toezicht op artikel 11.7a van de Telecommunicatiewet, waar de ACM toezichthouder op is, en de algemene verordening gegevensbescherming, waar zoals gezegd AP toezichthouder op is. Het kabinet denkt dat met deze samenwerking en de middelen die aan de ACM zijn toegekend voor de uitvoering van haar taken, er effectief toezicht kan worden gehouden op artikel 25 van de digitaledienstenverordening. Bovendien heeft, voor wat betreft het toezicht op (tracking)cookies, de regering extra budget toegekend aan AP. Verwezen zij in dit verband naar de

[35] Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad (Richtlijn oneerlijke handelspraktijken) (PbEU 2005, L 149).

[36] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

[37] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PbEG 2002, L 201).

brief van de Staatssecretaris van Binnenlandse Zaken en Koninkrijkrelaties van 28 september 2023[38] waarin is aangegeven dat AP voor het toezicht op cookies in de jaren 2024 tot en met 2026 € 500.000 per jaar en vanaf 2027 structureel €350.000 per jaar heeft gekregen.

40) *Is de regering bereid om druk te blijven uitoefenen op verdere regulering van dark patterns en het initiatiefrapport over dit onderwerp van het Europees Parlement[39] volledig te omarmen?*

Antwoord
Het initiatiefrapport van het Europees parlement gaat over het verslavend ontwerp van digitale diensten, zoals sociale media. Het kabinet is voorstander van een verdere Europese aanpak van verslavend ontwerp en zet zich hier in Europees verband ook actief voor in. Het is echter aan de Europese Commissie om met een formele reactie te komen op het initiatiefrapport.

In het kader van de 'fitness check'[40] waarin de Europese Commissie onderzoekt of de huidige regels consumenten ook online voldoende beschermen is aandacht gevraagd voor de aanpak van dark patterns. Dark patterns zijn manipulatieve of misleidende technieken die consumenten ertoe aan kunnen zetten om keuzes te maken die niet in hun belang zijn. Dark patterns kunnen op grond van de Richtlijn Oneerlijke Handelspraktijken[41] nu al worden aangepakt. Bij een overtreding van de Richtlijn Oneerlijke Handelspraktijken kan de ACM handhavend optreden. De verwachting is dat de Europese Commissie haar uitkomsten van de fitness check in het tweede kwartaal van 2024 publiceert.

41 en 42) *Ten slotte zijn de leden van de GroenLinks-PvdA-fractie blij te lezen dat de DSA extra aandacht heeft voor de bescherming van minderjarigen. Deze leden zijn het ermee eens dat minderjarigen een hoog niveau van privacy, veiligheid en bescherming verdienen. Zij zijn voorts van mening dat óók volwassenen een hoog niveau van privacy, veiligheid en bescherming verdienen. Is de regering het daarmee eens? Zo ja, gaat de regering pogingen ondernemen om bij de Europese Commissie aan te dringen op hogere standaarden voor volwassenen?*

Antwoord
Volwassenen verdienen het ook dat hun privacy en veiligheid online op een hoog niveau worden beschermd. Deze en andere verordeningen zoals de algemene verordening gegevensbescherming voorzien daarin. Daarnaast is de in het antwoord op vraag 40 genoemde fitness check van de Europese Commissie gericht op de online veiligheid van alle consumenten. De bescherming van minderjarigen verdient echter bijzondere aandacht omdat zij kwetsbaarder zijn dan volwassenen.

4.3. Aanvullende verplichtingen voor zeer grote online platforms en zeer grote online zoekmachines

43) *De leden van de GroenLinks-PvdA-fractie zijn blij dat de verordening zich niet alleen richt op het bestrijden van illegale inhoud, maar ook op informatie die weliswaar legaal is, maar niettemin negatieve effecten kan hebben, zoals desinformatie. Tegelijk is al jaren bekend dat de algoritmes van zeer grote online platforms met name content bevoordelen die veel interactie oplevert, en dat content die veel interactie oplevert vaak 'ophef' content is. Deze leden zijn ervan op de hoogte dat de verordening van zeer grote online platforms vereist dat zij een niet-algoritmisch alternatief moeten bieden, zoals een chronologische of alfabetische tijdlijn. De algoritmische tijdlijn blijft echter ook een mogelijkheid en wordt niet verboden. Kan de regering aangeven of het naar haar mening wenselijk en/of mogelijk is dat toezichthouders zeer grote online platforms kunnen dwingen om hun algoritmes aan te passen, om zodoende minder desinformatie te verspreiden? Wat zijn mogelijke drempels en bezwaren?*

Antwoord

[38] Kamerstukken II, 2023/24, 26 643, nr. 1071.

[39] Europarl, New EU rules needed to address digital addiction, 12-12-2023.

[40] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

[41] Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad (PbEY 2005, L 149).

Op grond van artikel 34 van de verordening moeten zeer grote online platforms jaarlijks onderzoeken of hun dienst vatbaar is voor bepaalde systeemrisico's. De verspreiding van sommige vormen van desinformatie kan zo'n systeemrisico zijn. Bijvoorbeeld desinformatie die een negatief effect heeft op verkiezingsprocessen (zie ook het antwoord op vraag 5 en 6). Indien er dergelijke systeemrisico's zijn dan moeten zeer grote online platformen maatregelen nemen om ze te mitigeren. In artikel 35 van de verordening worden voorbeelden gegeven van mogelijke maatregelen. Waaronder het aanpassen van algoritmische systemen en aanbevelingssystemen.

Het toezicht op de naleving van deze verplichtingen ligt op grond van artikel 56, tweede lid, van de verordening exclusief bij de Europese Commissie. In geval van een overtreding kan zij een niet-nalevingsbesluit vaststellen (artikel 73 van de verordening). Daarin moet de Europese Commissie haar bevindingen over de gestelde niet-naleving beschrijven en toelichten welke maatregelen een zeer groot online platform volgens haar moet nemen om dat te remediëren. Het is vervolgens aan het betreffende zeer grote online platform om daarop te reageren door een actieplan op te stellen, een onafhankelijke controle te laten verrichten, en de noodzakelijke maatregelen te treffen (artikel 75, tweede lid, van de verordening). Daarbij is het zeer grote online platform niet verplicht om de suggesties van de Europese Commissie op te volgen. Als het zeer grote online platform andere mogelijkheden ziet om de gestelde niet-naleving op te lossen dan is dat ook toegestaan.

De Europese Commissie heeft dus de mogelijkheid om de rol en invloed van aanbevelingssystemen te betrekken bij haar toezicht en handhaving en aanpassingen aan die aanbevelingssystemen voor te stellen.

44) *Ook lezen de leden van de GroenLinks-PvdA-fractie dat als aanbieders van zeer grote online platforms en zeer grote online zoekmachines vaststellen dat hun diensten systeemrisico's in zich hebben, dat ze dan op grond van artikel 35 van de verordening redelijke, evenredige en doeltreffende risicobeperkende maatregelen moeten treffen om de geïdentificeerde systeemrisico's te adresseren. Deze leden zijn hier tevreden mee. Wel vragen zij waarom de verantwoordelijkheid bij het identificeren van dergelijke systeemrisico's bij de aanbieders zelf ligt. Kan de regering aangeven of toezichthouders of de Europese Commissie hier ook een rol in (kunnen) spelen?*

Antwoord
De verantwoordelijkheid voor een analyse van systeemrisico's ligt in de eerste plaats inderdaad bij de aanbieders zelf. Daarnaast zijn zij op grond van artikel 37 van de verordening verplicht om ten minste één keer per jaar een onafhankelijke controle te laten verrichten om de naleving van onder meer de verplichting omtrent systeemrisico's te laten beoordelen. Indien uit die onafhankelijke controle blijkt dat er niet of onvoldoende is voldaan dan kunnen de auditors die de controle hebben verricht aanbevelingen doen om alsnog naleving te bereiken. In dat geval moeten zeer grote onlineplatforms en zoekmachines de nodige maatregelen treffen om de aanbevelingen uit te voeren. Doen zij dat niet dan zijn ze verplicht om dat te motiveren en een overzicht te geven van eventueel alternatieve maatregelen die zij hebben genomen. Het eigen rapport en dat van de onafhankelijke controle dient (grotendeels) openbaar te worden (artikel 42, vierde lid, van de verordening). Zo kunnen bijvoorbeeld toezichthouders, media, het maatschappelijk middenveld, burgers, politici en overheden er kennis van nemen en het gebruiken in het kader van hun toezicht, verslaggeving, of toekomstige beleidsvorming.

De verordening maakt het verder mogelijk voor erkende onderzoekers om toegang te krijgen tot data van zeer grote online platforms en zoekmachines voor onderzoek dat bijdraagt aan het opsporen, vaststellen en begrijpen van systeemrisico's (artikel 40, vierde lid, van de verordening). Hoewel dergelijk onderzoek niet tot doel heeft om de naleving van de verordening te controleren draagt het wel bij aan het begrip van systeemrisico's, de oorzaken daarvan, en mogelijke mitigerende maatregelen.

De Europese Commissie houdt toezicht op de naleving van zowel de verplichtingen omtrent systeemrisico's als de onafhankelijk controle. De bevoegdheden die zij daarvoor heeft zijn beschreven in afdeling 4 van hoofdstuk 4 van de verordening, zoals ook toegelicht in het antwoord op vraag 20.

45 en 46) *De leden van de CDA-fractie lezen dat de verordening in artikel 40, lid 1 tot en met 3, aanbieders van zeer grote online platforms verplicht om de digitaledienstencoördinator en de Commissie toegang te geven tot de gegevens die nodig zijn om de naleving van de verordening te monitoren en te beoordelen. Deze leden vragen aan de regering hoe wordt gehandeld wanneer een online platform niet voldoet aan deze eisen, door bijvoorbeeld niet te reageren op verzoeken tot inzage in bepaalde gegevens. Op welke manier kunnen deze grote bedrijven alsnog tot verantwoording geroepen worden, ook wanneer een groot online platform niet ingaat op verzoeken vanuit het Openbaar Ministerie (OM)?*

Antwoord
Artikel 40, eerste tot en met derde lid, van de verordening verplichten de aanbieders van zeer grote onlineplatforms of zeer grote onlinezoekmachines om toegang te geven tot gegevens aan de digitaledienstencoördinator of de Europese Commissie. Deze gegevens dienen te worden gebruikt in het kader van het toezicht op de naleving van de verordening. Vorderingen om inzage in gegevens door het openbaar ministerie (hierna: OM) vallen dus niet binnen de reikwijdte van deze bepaling. Het OM heeft in het kader van het strafrecht eigen bevoegdheden waar het gaat om strafvorderlijke onderzoeken waar dit soort aanbieders bij betrokken is.

Op grond van de verordening kan de Europese Commissie tot handhaving overgaan als deze aanbieders een verzoek als bedoeld in artikel 40 van de verordening weigeren. In het nationale recht is het op grond van artikel 5:20 van de Algemene wet bestuursrecht verplicht om medewerking te verlenen aan toezichthouder bij de uitoefening van diens bevoegdheden, waaronder een vordering tot inzage van zakelijke gegevens en bescheiden. Overtreding van deze medewerkingsplicht kan zowel strafrechtelijk als bestuursrechtelijk worden gehandhaafd, bijvoorbeeld door het opleggen van een bestuurlijke boete.

5. Uitvoering, samenwerking, toezicht en handhaving

47) *In de uitvoeringswet van de verordening staat opgenomen dat de toezichthouder, de ACM, tijdig moeten handelen bij klachten die door individuele derden zijn geuit. Waarom wordt ervoor gekozen hier geen maximale termijn aan te verbinden, zo vragen de leden van de D66-fractie.*

Antwoord
Op grond van artikel 53 van de verordening hebben afnemers van een tussenhandeldienst of hun gemachtigden het recht om een klacht in te dienen wegens vermeende inbreuk op de verordening door de dienstaanbieder bij de digitaledienstencoördinator van de lidstaat waar de afnemer van de dienst zich bevindt of gevestigd is. De digitaledienstencoördinator beoordeelt de klacht en stuurt deze, waar passend, door naar de digitaledienstencoördinator van de plaats van vestiging of naar een andere bevoegde autoriteit uit de eigen lidstaat.

Uit artikel 53 van de verordening zelf volgt niet dat de digitaledienstencoördinator tijdig moet handelen bij de beoordeling van een klacht. Wel is in de verordening bepaald dat de bevoegde autoriteiten voor de uitvoering en de handhaving van de verordening, waaronder de digitaledienstencoördinator, hun taken op een onpartijdige, transparante en tijdige wijze uitvoeren. Wat een tijdige uitvoering is, verschilt per taak en hangt af van de omstandigheden van het geval. In onderhavig wetsvoorstel ter uitvoering van de verordening is dan ook niet voorgeschreven dat de ACM tijdig moeten handelen bij klachten die door individuele derden zijn geuit. Dat is ook niet nodig gezien de rechtstreeks werkende bepalingen van de verordening.

Het recht om een klacht over de naleving van de verordening in te dienen bij de digitaledienstencoördinator (artikel 53 van de verordening) moet overigens onderscheiden worden van het recht voor gebruikers en derden om een klacht over een inhoudsmoderatiebesluit in te dienen bij het interne klachtenafhandelingssysteem van de aanbieder van een onlineplatform (artikel 20 van de verordening). Ten aanzien van dat laatste type klacht bepaalt de verordening wel expliciet dat klachten tijdig, op niet-discriminerende, zorgvuldige en niet-willekeurige wijze worden afgehandeld. Wat tijdig in dit verband betekent zal in eerste instantie door de aanbieder zelf moeten worden bepaald. De ACM houdt toezicht op de naleving van deze bepaling. Uiteindelijk is het aan de rechter om zich uit te spreken over wat tijdig in dit verband betekent.

48) *Kan de regering verduidelijken wat het in de praktijk betekent dat er niet wordt voldaan aan het verzoek van de ACM om de Boetebeleidsregel ACM 2014 aan te passen naar aanleiding van dit voorstel, zo vragen de leden van de D66-fractie.*

Antwoord
De bevoegde autoriteiten voor de uitvoering en de handhaving van de verordening moeten op grond van de verordening volledig onafhankelijk kunnen handelen. Dit vereiste beperkt de mogelijkheden om overheidstoezicht te houden op deze autoriteiten, zo volgt uit de jurisprudentie van het HvJ EU. Beleidsregels betreffen regels over hoe de toezichthoudende autoriteit bij het gebruik van een bevoegdheid belangen dient af te wegen, feiten vaststelt of wettelijke voorschriften uitlegt. De verantwoordelijke Minister zou op deze wijze, direct of indirect, invloed kunnen hebben op de beslissingen van de toezichthouder, hetgeen niet in lijn zou zijn met de uitleg van het HvJ EU van het vereiste van ‘volledige onafhankelijkheid’. Om die reden is in artikel 2.1, derde lid, van het wetsvoorstel bepaald dat deze bevoegdheid om beleidsregels op te stellen op grond van de Kaderwet ZBO’s niet geldt voor de uitvoering van de digitaledienstenverordening.

Het gevolg daarvan is dat de Boetebeleidsregel ACM 2014, vastgesteld door de minister van EZK, niet van toepassing kan worden verklaard op de uitvoering van deze uitvoeringswet. De gevolgen daarvan zijn beperkt, omdat de ACM de bevoegdheid behoudt om zelf beleidsregels over dit onderwerp vast te stellen. Het is aan de beoordeling van de ACM of ze daarbij inhoudelijk wenst aan te sluiten bij de keuzes die in de Boetebeleidsregel ACM 2014 zijn gemaakt.

5.1. Uitvoering in Nederland

49 en 50) *De leden van de VVD-fractie lezen dat de ACM en de AP aangewezen zijn als toezichthouder. Hoe wordt ervoor gezorgd dat deze toezichthouders voldoende uitgerust zijn voor deze rol, dit ook met oog op de andere gebieden waar deze partijen toezicht op houden. Kunnen de toezichthouders direct van start zodra deze wet is aangenomen?*

Antwoord
Om de beide toezichthouders in staat te stellen om zich voor te bereiden op hun toezichtstaken heeft de regering reeds in 2023 incidentele middelen beschikbaar gesteld. Daarna zijn er ook structureel middelen beschikbaar gemaakt vanaf 2024. De ACM heeft een structureel budget van € 6,5 miljoen gekregen. Daarmee kan ze 49 fte bekostigen. Voor de AP is er reeds € 517.000,– structureel beschikbaar gemaakt voor de financiering van 3,2 fte.

De doelstellingen van de verordening en de aard van de daarin neergelegde verplichtingen sluiten aan bij de bestaande taken en specifieke deskundigheid van de ACM. De aanbieders van tussenhandeldiensten, de normadressaten van de verordening, zijn ondernemingen die al onderworpen zijn aan toezicht van de ACM op grond van andere wetgeving. Bijvoorbeeld op grond van de Mededingingswet, het consumentenrecht, de bepalingen in het BW ter implementatie van de richtlijn elektronische handel, en, indien het wetsvoorstel[42] daartoe wordt aangenomen, de P2B-verordening. De keuze voor de Autoriteit Persoonsgegevens als toezichthouder op artikel 26, derde lid, en artikel 28, tweede lid, van de verordening, is mede ingegeven door het feit dat het normen zijn die een verbijzondering van de AVG vormen. Daarmee is bij uitstek geborgd dat haar toezichthoudende taken aansluiten op het toezicht op de AVG waar zij reeds mee belast is.[43]

51) *De leden van de NSC-fractie lezen dat de Raad van State waarschuwt dat de ministeriële verantwoordelijkheid in het wetsvoorstel beperkt wordt door op enkele punten af te wijken van de Kaderwet zelfstandig bestuursorganen. Deze leden vragen daarom aan de regering of zij meerdere concrete situaties kan schetsen waarbij het wenselijk is dat de ministeriële verantwoordelijkheid wordt beperkt.*

[42] Kamerstukken II, 2022/23, 36285, nr. 2.

[43] Zie voor een meer uitgebreide toelichting de paragrafen 5.2.2.2 en 5.2.2.3 van de Memorie van Toelichting bij het wetsvoorstel.

Antwoord
De ACM en de AP worden in het wetsvoorstel aangewezen als bevoegde autoriteiten. Zowel de ACM als de AP zijn zelfstandige bestuursorganen, hetgeen de ministeriële verantwoordelijkheid ten aanzien van de uitvoering van hun taken inperkt. In de artikelen 2.1, derde en vierde lid, en 3.1, tweede en derde lid, van het wetsvoorstel is bepaald dat enkele bevoegdheden uit de Kaderwet zbo's niet van toepassing zijn op de uitvoering van taken door de ACM en de AP op grond van dit wetsvoorstel. Dit zijn de bevoegdheid van de minister van EZK om besluiten van de ACM en de AP te vernietigen, om beleidsregels te stellen over de uitoefening van bevoegdheden door de ACM en de AP en om in te grijpen bij taakverwaarlozing van inhoudelijke aard door de ACM en de AP. De Afdeling advisering van de Raad van State merkt in haar advies op dat met deze afwijking van de Kaderwet zbo's de ministeriële verantwoordelijkheid van de minister van EZK verder wordt beperkt. Aan het advies van de Afdeling om in de memorie van toelichting een dragende motivering voor deze afwijking op te nemen, is gehoor gegeven.

De afwijkingen van de Kaderwet zbo's zijn ingegeven door de eis uit de verordening dat de ACM en de AP volledig onafhankelijk moeten kunnen handelen en dat zij geen instructies van enige andere overheidsinstantie mogen vragen of aanvaarden. De Algemene verordening gegevensbescherming bevat een gelijkluidende eis en in de Uitvoeringswet AVG is dezelfde keuze gemaakt ten aanzien van het uitsluiten van deze bevoegdheden uit de Kaderwet ZBO's. In dit verband is van belang wat het HvJEU in zijn jurisprudentie heeft bepaald over de waarborg van volledige onafhankelijkheid van de nationale toezichthoudende autoriteiten. Volgens het HvJEU heeft deze waarborg tot doel een grotere bescherming te bieden aan de personen en organen die door hun beslissingen worden getroffen. Bij de uitoefening van hun taken moeten deze toezichthoudende autoriteiten objectief en onpartijdig handelen. Daartoe moeten zij vrij zijn van beïnvloeding van buitenaf, daaronder begrepen de – rechtstreekse of indirecte – beïnvloeding door de staat. Volgens het HvJEU is het niet van doorslaggevende betekenis wat het doel van het eventuele overheidstoezicht is. Wel van doorslaggevende betekenis is dat de staat een belang kan hebben bij de toezichtsbesluiten van de autoriteiten en dat de instanties die belast zijn met het overheidstoezicht, een politieke invloed kunnen uitoefenen op de beslissingen van de toezichthoudende autoriteiten en zo de onafhankelijke vervulling van de taken van deze autoriteiten kunnen hinderen. Het HvJ EU noemt dit 'geanticipeerde gehoorzaamheid'.

Uit het voorgaande volgt dat het niet zo zeer gaat om de wenselijkheid om de genoemde bevoegdheden uit de Kaderwet ZBO's in bepaalde situaties wel of niet te kunnen inzetten. Het HvJEU erkent dat het doel van het overheidstoezicht legitiem kan zijn, bijvoorbeeld om te waarborgen dat onafhankelijke toezichthouders voldoen aan het toepasselijke nationale en Europese recht. Desondanks moet voorkomen worden dat er een politieke invloed uitgeoefend zou kunnen worden op de beslissingen van de toezichthoudende autoriteiten. In het kader van de digitaledienstenverordening zou het dan bijvoorbeeld kunnen gaan om via dit overheidstoezicht invloed uit te oefenen op het al dan niet actie ondernemen door aanbieders van tussenhandeldiensten tegen bepaalde vormen van illegale of anderszins onwenselijke online inhoud. De enkele mogelijkheid dat via het overheidstoezicht op de toezichthouders een dergelijke invloed zou kunnen worden uitgeoefend op het toezichtbeleid van de toezichthouders is onwenselijk en zou kunnen leiden tot wat het HvJEU 'geanticipeerde gehoorzaamheid' noemt.

5.2. Toezicht en handhaving

52) *De leden van de GroenLinks-PvdA-fractie hebben begrip voor de manier waarop de afbakening met andere lidstaten en de Commissie is ingericht. Wel hebben deze leden vragen over verzoeken die de ACM kan doen aan toezichthouders van andere lidstaten en andersom. Kan de regering reflecteren op mogelijke gebreken aan capaciteit, budget of bereidwilligheid van toezichthouders van andere lidstaten ten aanzien van de verzoeken die de ACM bij hen doet, en mogelijke gebreken aan capaciteit, budget of bereidwilligheid van de ACM ten aanzien van verzoeken die het ontvangt van andere toezichthouders?*

Antwoord

De ACM heeft een structureel extra budget van € 6,5 miljoen gekregen. Daarmee kan ze 49 fte extra bekostigen. Daarmee krijgt de ACM meer middelen dan bijvoorbeeld de digitaledienstencoördinatoren in Denemarken (4,6 fte) en Finland (6,5 fte) en in verhouding met wat Duitsland beschikbaar stelt (70,6 fte). Daarbij moet worden opgemerkt dat onbekend is in hoeverre die digitaledienstencoördinatoren hun bestaande capaciteit in kunnen zetten voor DSA-taken. Het kabinet verwacht dat de ACM met de extra toegekende middelen voldoende middelen heeft om haar toezichthoudende taken en de samenwerking met andere digitaledienstencoördinatoren en de Europese Commissie uit te voeren.

Artikel 50, eerste lid, van de verordening, verplicht de lidstaten om de digitaledienstencoördinatoren van "*alle nodige middelen*" te voorzien die zij nodig hebben om hun taken uit te voeren. Zoals technische, financiële en personele middelen. Hoewel er verschillen zijn in de extra middelen die lidstaten tot nog toe beschikbaar hebben gesteld, moet er van worden uitgegaan dat het voldoende is om te voldoen aan de deze verplichting.

Verschillen in de beschikbaar gestelde middelen kunnen overigens worden verklaard door verschillen in de omvang van lidstaten, de mate waarin hun digitale economie is ontwikkeld, in hoeverre digitaledienstencoördinatoren hun reeds bestaande capaciteit in kunnen zetten voor DSA-taken en het aantal zeer grote online platformen en zoekmachines dat er in een lidstaat is gevestigd. Hoewel het toezicht op die diensten primair bij de Europese Commissie ligt is er een gedeelde verantwoordelijkheid met de digitaledienstencoördinator uit de lidstaat van vestiging. In het kader van haar toezicht zal de Europese Commissie soms hulp behoeven en daarbij een beroep doen op die digitaledienstencoördinator (artikel 57 van de verordening). Na Ierland is Nederland de lidstaat waar momenteel de meeste zeer grote online platformen en zoekmachines zijn gevestigd of een wettelijk vertegenwoordiger aangesteld hebben. Namelijk AliExpress, Booking.com en Snap.[44]

Vooralsnog is er geen reden om aan te nemen dat de digitaledienstencoördinatoren onvoldoende middelen hebben gekregen om hun taken te kunnen verrichten. De verordening voorziet verder in mogelijkheden voor de digitaledienstencoördinatoren en de Europese Commissie om samen te werken en zo optimaal gebruik te maken van de beschikbare middelen.

53) *Voorziet de regering mogelijke problemen wanneer andere toezichthouders niet bij machte zijn om handhavend op te treden wanneer de ACM overtredingen in Nederland constateert maar de wettelijke vertegenwoordiger van de overtreder zich in een ander Europese Unieland bevindt?*

Antwoord
Nee. De verordening voorziet in de artikelen 50 tot en met 52 in de onafhankelijkheid van de digitaledienstencoördinatoren en andere bevoegde autoriteiten en de verplichting om hen van de bevoegdheden en middelen te voorzien die ze in staat stellen om de verordening effectief te handhaven. Het is daardoor niet voorstelbaar dat toezichthouders niet bij machte zijn om op te treden tegen overtredingen van de verordening.

Indien er andersoortige belemmeringen zijn waardoor een toezichthouder in een andere lidstaat niet bereid is om te handhaven wanneer de ACM een overtreding door een in die lidstaat gevestigde aanbieder in Nederland heeft vastgesteld, dan voorzien de artikelen 58 en 59 van de verordening in een procedure. Daarmee kan de toezichthouder in de lidstaat van vestiging door de digitaledienstenraad worden aangezet om onderzoek te doen naar een vermeende inbreuk, daarover te besluiten, en verantwoording af te leggen aan de digitaledienstenraad en de digitaledienstencoördinator die de inzet van deze procedure is gestart. Als de digitaledienstenraad het niet eens is met de beoordeling van de digitaledienstencoördinator in de lidstaat van vestiging dan kan zij de zaak naar de Europese Commissie verwijzen. Die moet de zaak vervolgens beoordelen. Afhankelijk van haar bevindingen kan ze de digitaledienstencoördinator in de lidstaat van vestiging opdracht geven om de zaak te herzien. Die digitaledienstencoördinator moet dan de nodige maatregelen nemen om naleving van de verordening te waarborgen. Daarbij moet rekening worden gehouden met het standpunt van de Europese Commissie.

[44] https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

De procedure van artikel 58 en 59 van de verordening zorgt er voor dat digitaledienstencoördinatoren een optie hebben wanneer ze een overtreding van de verordening vaststellen door een aanbieder van een tussenhandeldienst die in een andere lidstaat is gevestigd. De regering heeft zich tijdens de onderhandelingen hard gemaakt voor het opnemen van een dergelijke procedure in de verordening om '*regulator shopping*' te bestrijden.

54) *Voorziet de regering mogelijke overvraging van de ACM door andere toezichthouders en is er een systeem bedacht dat deze overvraging op kan lossen, door bijvoorbeeld automatisch meer budget beschikbaar te stellen voor de ACM?*

Antwoord
Zoals in het antwoord op vraag 52 is aangegeven heeft de regering de ACM een omvangrijk structureel budget toegekend, ook om overvraging te voorkomen.

Er is niet voorzien in een systeem om het budget voor de ACM automatisch te verhogen. In haar uitvoerbaarheid- en handhaafbaarheidstoets heeft de ACM voorgesteld om "*de omvang van de financiering na drie jaar te evalueren*". Van dat aanbod wordt gebruik gemaakt. In de komende jaren zal de ACM bovendien in haar jaarverslag ook aandacht besteden aan haar toezicht op de DSA. Mocht dat al eerder signalen opleveren dat er sprake is van overvraging of een tekort aan middelen dan kan naar aanleiding daarvan in overleg worden getreden.

55) *Ook realiseren de leden van de GroenLinks-PvdA-fractie dat naar aanleiding van het land-van-oorsprongsbeginsel afnemers zich moeten melden bij de toezichthouders van het land waarin de wettelijke vertegenwoordiger van de tussenhandeldienst zich bevindt. Het land-van-oorsprongsbeginsel is vanuit de gedachte van toezicht een logische, maar maakt het melden van klachten niet eenvoudiger. Kan de regering aangeven of het wenselijk is dat Nederlandse afnemers zich te allen tijde bij de ACM en/of AP kunnen melden, die meldingen indien nodig (al dan niet automatisch) door kunnen sturen naar de juiste buitenlandse toezichthouder? Waarom zou dit wel of niet wenselijk kunnen zijn?*

Antwoord
De regering acht het wenselijk dat Nederlandse afnemers zich te allen tijde bij de ACM of de AP (wanneer de klacht ziet op een onderdeel van de DSA waar de AP is aangewezen als toezichthouder) kunnen melden met klachten over een vermeende inbreuk van de verordening door aanbieders van tussenhandeldiensten. Ook als een aanbieder in een andere lidstaat is gevestigd of daar zijn wettelijk vertegenwoordiger heeft aangewezen. De verordening maakt dat in artikel 53 ook mogelijk. De ACM kan dergelijke klachten doorsturen en daar eventueel ook een advies bij voegen.

56) *De leden van de NSC-fractie lezen dat, indien de tussenhandeldienst gevestigd is in een andere lidstaat of daar een wettelijke vertegenwoordiger heeft aangewezen, de ACM en de AP niet bevoegd zijn daar toezicht op te houden. Deze leden vragen daarbij hoe de regering beoogt de Nederlandse consument te beschermen tegen tussenhandeldiensten die gevestigd zijn in andere lidstaten. Hoe kan er toch voor gezorgd worden dat een onderzoek wordt gestart naar dergelijke tussenhandeldiensten?*

Antwoord
Zoals in het antwoord op vraag 52 is beschreven kent de verordening diverse instrumenten op basis waarvan de digitaledienstencoördinatoren en de Europese Commissie kunnen samenwerken om effectief toezicht op de verordening te houden. Zo is er voorzien in een mogelijkheid voor gezamenlijk onderzoek (artikel 60 van de verordening). Verder is er een verplichting tot wederzijdse onderlinge bijstand tussen digitaledienstencoördinatoren en de Europese Commissie (artikel 57 van de verordening). En digitaledienstencoördinatoren kunnen de digitaledienstenraad, en in uiterste gevallen de Europese Commissie, verzoeken om de digitaledienstencoördinator in een lidstaat van vestiging aan te zetten tot onderzoek naar naleving, en zo nodig handhaving van de verordening (artikelen 58 en 59 van de verordening). Ook hebben alle gebruikers in de Unie het recht om een klacht in te dienen bij de digitaledienstencoördinator in de lidstaat waar zij zijn gevestigd of zich bevinden over een vermeende inbreuk door een tussenhandeldienst (artikel 53 van de

verordening). Al deze maatregelen tezamen bieden aan goede basis voor effectief toezicht op de naleving door alle tussenhandeldiensten, ongeacht waar zij gevestigd zijn.

57) *Daarbij vragen deze leden eveneens wat er zou gebeuren indien Nederland het nodig acht dat een dergelijk onderzoek wordt gestart, terwijl de lidstaat waarin de tussenhandeldienst is gevestigd dit niet wil.*

Antwoord
Vooropgesteld is het toezicht op de verordening de exclusieve competentie van onafhankelijk toezichthouders, en niet van de lidstaten. Indien de ACM het nodig acht dat een onderzoek naar een tussenhandeldienst in een andere lidstaat wordt gestart dan kan zij gebruik maken van de procedure uit artikel 58 en 59 van de verordening, die nader is beschreven in de antwoorden op vraag 52 en 53.

58) *De leden van de CDA-fractie constateren dat ook online tussenhandelsdiensten die niet kwalificeren als VLOP grote platformen kunnen zijn die internationaal actief zijn. Deze leden vragen hoe in dit geval samenwerking tussen nationale toezichthouders vorm krijgt, welke rol daar voor de Europese Commissie ligt en hoe de regering effectieve samenwerking bevordert.*

Antwoord
Zoals in de antwoorden op de vragen 52, 53 en 56 is beschreven bevat de verordening een aantal instrumenten voor samenwerking tussen de nationale toezichthouders en de Europese Commissie. De verplichting tot wederzijdse bijstand (artikel 57 van de verordening), gezamenlijke onderzoeken (artikel 60 van de verordening), en de procedure van artikel 58 en 59, zijn ook van toepassing voor tussenhandeldiensten die geen zeer groot online platform zijn. Tot op heden heeft de regering indirect bijgedragen aan samenwerking tussen de toezichthouders door de ACM en AP reeds in 2023 van incidentele financiering te voorzien, en sindsdien van structurele financiering. Daarmee zijn beide toezichthouders in staat gesteld om alvast samen te werken met hun collega-toezichthouders aan de voorbereidingen op het toezicht van de verordening.

5.3. Toezicht en handhaving door de Commissie

59) *Het stemt de leden van de VVD-fractie tevreden dat de ACM als digitaledienstencoördinator genoeg bevoegdheden lijkt te hebben om onderzoeken in te stellen en de verordening te handhaven. De verzoeken voor onderzoek worden door de ACM ontvangen, waarna het verzonden wordt naar de AP. De leden vragen hierbij wat er gebeurt wanneer de ACM tot andere conclusies komt dan de AP. Op welke manier worden dergelijke situaties opgelost en hoe wordt ervoor gezorgd dat het proces niet te lang duurt.*

Antwoord
Op grond van het onderhavige wetsvoorstel worden zowel de ACM als de AP aangewezen als bevoegde autoriteit voor het uitvoeren van het toezicht en de handhaving ten aanzien van de digitaledienstenverordening. Zoals ook voorgeschreven door de verordening, zijn hun taken in het uitvoeringswetsvoorstel duidelijk gedefinieerd en afgebakend: de AP houdt toezicht op twee bepalingen van de verordening die zien op een verbod op profilering met gebruikmaking van persoonsgegevens en de ACM op de overige bepalingen. De bevoegdheden van de ACM en de AP overlappen dus niet en dus kan er ook geen sprake zijn van andere conclusies van de ACM en de AP over de vraag of een bepaling van de verordening is overtreden. Dit geldt ook als sprake is van een verzoek tot onderzoek, afkomstig van de Europese Commissie of de digitaledienstencoördinator van een andere lidstaat.

Om een uniforme uitleg van de begrippen uit de verordening te verzekeren, is bepaald dat de AP de algemene begrippen uit de verordening uitlegt in overeenstemming met de ACM. Tot slot schrijft de verordening voor dat de bevoegde autoriteiten nauw en doeltreffend samenwerken. Dit is in het uitvoeringswetsvoorstel uitgewerkt in een grondslag voor het uitwisselen van gegevens tussen de ACM en de AP en in de verplichting dat zij afspraken maken over hun samenwerking, in de vorm van een samenwerkingsprotocol. Hierin kunnen afspraken worden neergelegd over hoe de afstemming tussen beide autoriteiten effectief en tijdig plaatsvindt.

Er bestaat al een samenwerkingsprotocol tussen de ACM en de AP, en dit protocol wordt vernieuwd mede naar aanleiding van de DSA en onderhavig uitvoeringswetsvoorstel. Dit proces is al in werking gezet, en zal vermoedelijk dit jaar worden afgerond. Dit hangt mede af van de datum van inwerkingtreding van de uitvoeringswet.

Bij het vernieuwen van het samenwerkingsprotocol nemen beide toezichthouders de bestaande en nieuwe wettelijke bevoegdheden van beide partijen in ogenschouw en bezien zij over welke onderwerpen (nadere) afspraken moeten worden gemaakt. Dit wordt verder uitgewerkt in onderlinge werkafspraken. Van het (aangepaste) protocol wordt mededeling gedaan in de Staatscourant (zie artikel 4.4, derde lid, van het wetsvoorstel) en op de websites van beide autoriteiten geplaatst.

60) *Ook vragen deze leden in geval het een situatie betreft waar geen persoonsgegevens in het geding zijn, hoe de rol van de AP er dan uitziet.*

Antwoord
De AP zal op grond van het uitvoeringswetsvoorstel toezicht houden op twee bepalingen van de verordening die zien op een verbod op profilering met gebruikmaking van persoonsgegevens. De AP heeft dus geen rol waar het een situatie betreft waar geen persoonsgegevens in het geding zijn. In dat geval is het altijd aan de ACM om te reageren op een verzoek tot onderzoek, afkomstig van de Europese Commissie of de digitaledienstencoördinator van een andere lidstaat.

5.4. Certificering en toekenning formele statussen

61 en 62) *De leden van de NSC-fractie lezen dat de AP advies uitbrengt aan de ACM over of de aanvrager van een onderzoek of inspectie in staat is om persoonsgegevens te beschermen. Daarbij vragen deze leden wat er zou gebeuren in het scenario dat de AP een negatief oordeel hierover velt, terwijl de ACM of de Europese Commissie het onderzoek desondanks alsnog wil uitvoeren. Daarbij vragen deze leden ook waarom hier niet is gekozen voor een bindend advies vanuit de AP. Het is immers zeer onverantwoord om gevoelige gegevens alsnog te delen terwijl de andere partij deze niet kan beschermen.*

Antwoord
Artikel 40, vierde tot en met twaalfde lid, van de verordening biedt de mogelijkheid voor onderzoekers om de status van ‘erkend onderzoeker’ aan te vragen en aan de digitaledienstencoördinator te verzoeken om hen toegang te verlenen tot gegevens van zeer grote onlineplatforms en zeer grote onlinezoekmachines. Een voorwaarde die geldt voor het verkrijgen van de status van ‘erkend onderzoeker’ en de toegang tot deze gegevens, is dat de onderzoeker in staat is om persoonsgegevens te beschermen. Deze procedure is enkel van toepassing op toegang tot gegevens voor erkende onderzoekers en niet op toegang tot gegevens door de digitaledienstencoördinator of de Europese Commissie. Dat laatste wordt geregeld in artikel 40, eerste tot en met derde lid, van de verordening.

De ACM is, als aangewezen digitaledienstencoördinator op grond van dit wetsvoorstel, bevoegd om te besluiten over aanvragen tot toekenning van de status van ‘erkende onderzoeker’. Vanwege de positie van de AP als toezichthoudende autoriteit onder de AVG en hun expertise met betrekking tot de bescherming van persoonsgegevens, is in het wetsvoorstel voorzien in een verplicht advies van AP over dit aspect van de aanvraag tot toekenning van de status van ‘erkende onderzoeker’. Gezien het belang van de bescherming van persoonsgegevens en de rol en expertise van AP als toezichthoudende autoriteit op grond van de AVG, ligt het in de rede dat de ACM het advies van AP ter zake in de praktijk altijd volgt. In het hypothetische geval dat de ACM zou besluiten af te wijken van een dergelijk advies, dan moeten het advies en de dragende motivering voor afwijking in het (ontwerp)besluit worden opgenomen, zodat de betrokkenen, waaronder de aanbieder van het zeer grote onlineplatform of de zeer grote onlinezoekmachine in kwestie, op dat punt hun zienswijze kunnen geven of bezwaar en beroep kunnen instellen. De AP blijft voorts verder te allen tijde bevoegd om toezicht te houden op naleving van de Algemene verordening persoonsgegevens bij de

uitvoering van het betreffende onderzoek en om tot handhaving over te gaan als zij daarbij overtredingen constateert.

Er is tot slot niet gekozen voor een bindend advies, omdat de verordening voorschrijft dat het besluit over een aanvraag tot toekenning van de status van ‘erkende onderzoeker’ en over de toegang tot gegevens wordt genomen door de digitaledienstencoördinator, op grond van het wetsvoorstel de ACM. Ook voor de goede uitvoering van deze taak is het volgens het kabinet niet nodig om het advies een bindend karakter te geven. Tot slot kan worden genoemd dat de Europese Commissie geen rol heeft in deze procedure en zij dus ook kan niet besluiten dat een onderzoek wel of geen doorgang moet vinden.

6. Gegevensuitwisseling

6.1. Samenwerking tussen de bevoegde autoriteiten en met andere autoriteiten

63) *Wanneer zal het benoemde samenwerkingsprotocol opgesteld worden en hoe wordt ervoor gezorgd dat er geen overlap is op sommige fronten of juist dat er belangrijke informatie wordt gemist, zo vragen de leden van de VVD-fractie.*

Antwoord
Zoals ook aangegeven in het antwoord op vraag 59, bestaat er al een samenwerkingsprotocol tussen de ACM en de AP. Dat protocol wordt mede in het kader van de DSA dit jaar nog vernieuwd.

64) *Hoe wordt ervoor gezorgd dat de samenwerking zorgt voor een verdeling van de verantwoordelijkheid en niet een dubbele verantwoordelijkheid bij beide partijen?*

Antwoord
Op grond van het onderhavige wetsvoorstel worden zowel de ACM als de AP aangewezen als bevoegde autoriteit voor het uitvoeren van het toezicht en de handhaving ten aanzien van de digitaledienstenverordening. Zoals ook voorgeschreven door de verordening, zijn hun taken in het uitvoeringswetsvoorstel duidelijk gedefinieerd en afgebakend: de AP houdt toezicht op twee bepalingen van de verordening die zien op een verbod op profilering met gebruikmaking van persoonsgegevens en de ACM op de overige bepalingen. De bevoegdheden van de ACM en de AP overlappen dus niet en er is geen sprake van een dubbele verantwoordelijkheid. De verordening schrijft voorts voor dat de bevoegde autoriteiten nauw en doeltreffend samenwerken. Dit is in het uitvoeringswetsvoorstel uitgewerkt in een grondslag voor het uitwisselen van gegevens tussen de ACM en de AP en in de verplichting dat zij afspraken maken over hun samenwerking, in de vorm van een samenwerkingsprotocol.

6.2 Gegevensuitwisseling

65 en 66) *De leden van de VVD-fractie vragen hoe ervoor wordt gezorgd dat er voldoende maatregelen zijn genomen om veilig gegevens uit te wisselen tussen beide autoriteiten, doch dat dit ook op een snelle en efficiënte manier gebeurt. Hoe wordt het onderscheid gemaakt tussen welke informatie wel gedeeld moet worden en welke niet? Op welke manier komt er een afbakening die duidelijk maakt wanneer bepaalde processen gestart moeten worden? Kan de ACM ook zonder de AP bepaalde beslissingen nemen en andersom?*

Antwoord
In het kader van uitwisselen van meldingen over de DSA dienen de ACM en de AP in eerste instantie gebruik te maken van het Europees informatie-uitwisselingssysteem, AGORA. Dit systeem is nog in ontwikkeling en daarom zijn de AP en de ACM in gesprek om hierover tijdelijke werkafspraken te maken om meldingen op een veilige manier naar elkaar te kunnen doorsturen. Beide autoriteiten beschikken over *encrypted* software om veilig gegevens met elkaar te kunnen uitwisselen.

Ook de overige processen worden neergelegd in praktische werkafspraken. Bij deze afspraken wordt zoveel mogelijk rekening gehouden met verschillende situaties om te bepalen welk proces

daar het meest passend voor is. Zo ook voor situaties waarin beide toezichthouders bevoegd kunnen zijn. Bij het certificeren van erkende onderzoekers is bijvoorbeeld sprake van een situatie waar de ACM telkens het besluit over het certificeren neemt, terwijl voor de AP een adviesrol is weggelegd. Hierover worden daarom specifieke afspraken gemaakt in het samenwerkingsprotocol.

Daarnaast voorziet het huidige samenwerkingsprotocol, dat ook in antwoord op vraag 63 is benoemd, al in een regeling omtrent het doorsturen van relevante informatie betreffende de toezichtsgebieden van de ACM en de AP.

6.3. Gegevensuitwisseling tussen de ACM, de politie en het OM

67) *De leden van de CDA-fractie lezen dat de verstrekking van politiegegevens door de politie aan de ACM geschiedt op grond van de Wet politiegegevens. De verstrekking van justitiële en strafvorderlijke gegevens door het Openbaar Ministerie zal geschieden op grond van art. 39f, lid 1 onder c Wjsg. Deze leden lezen in dat artikel dat op grond van een zwaarwegend algemeen belang strafvorderlijke gegevens verstrekt kunnen worden met als doeleinde het uitoefenen van toezicht op het naleven van regelgeving. Wanneer is in het licht van de DSA sprake van een zogenoemd zwaarwegend belang? Deze leden vragen hoe zwaar dit criterium wordt geacht te zijn.*

Antwoord
Het criterium van een zwaarwegend algemeen belang in de Wet justitiële en strafvorderlijke gegevens is ontleend op de rechtspraak van het Europees Hof voor de Rechten van de Mens. Aan dit criterium is voldaan indien de verstrekking een legitiem doel dient en de verstrekking noodzakelijk is in een democratische samenleving. In de context van de digitaledienstenverordening bestaat het legitiem belang uit het toezicht op de naleving van die verordening. Het vereiste van noodzakelijkheid in een democratische samenleving strekt tot een evenredigheidsbeoordeling van de verwerkingsverantwoordelijke. Vanwege het College van procureurs-generaal, als verwerkingsverantwoordelijke van het openbaar ministerie, zal per geval worden beoordeeld of de verstrekking niet verder gaat dan geschikt en noodzakelijk is voor het toezicht op de naleving, en de verstrekking in verhouding staat tot dat doel.

68) *De leden van de CDA-fractie lezen dat voor het verstrekken van politiegegevens in het kader van onderhavig wetsvoorstel een grondslag wordt opgenomen in het Besluit politiegegevens. Deze leden vragen wanneer deze grondslag zal worden geïmplementeerd en op welke manier dit wordt vormgegeven.*

Antwoord
In het Besluit politiegegevens zijn de grondslagen neergelegd voor het verstrekken van politiegegevens aan derden. Zo is in artikel 4:3, eerste lid, onderdeel s, van het Besluit politiegegevens neergelegd dat politiegegevens kunnen worden verstrekt aan de ACM voor bepaalde aan haar opgedragen toezichthoudende taken. Het voornemen bestaat de digitaledienstenverordening toe te voegen aan deze bepaling. Aan dit voornemen wordt gevolg gegeven bij de eerstvolgende gelegenheid. Totdat in een structurele verstrekkingsgrondslag is voorzien, kunnen politiegegevens op de voet van artikel 19, onderdeel d, van de Wet politiegegevens aan de ACM worden verstrekt voor het toezicht op de naleving van de digitaledienstenverordening.

7. Gevolgen

7.1 Regeldruk en nalevingslasten van de Uitvoeringswet

69) *In de verordening wordt genoemd dat deze eventuele regeldruk en kosten op kan leveren voor het bedrijfsleven en tussenhandeldiensten. De leden van de VVD-fractie begrijpen dat het toezicht van de ACM en de AP belangrijk is en inderdaad druk en kosten op kan leveren. Echter zijn deze leden benieuwd voor welke partijen deze lasten het zwaarst zullen zijn. Er wordt genoemd dat er geen directe gevolgen zijn voor bedrijfsleven en burgers, maar de leden zijn benieuwd naar hoe deze afweging is gemaakt. Zij verwachten namelijk dat de gevolgen voor ondergenoemde partijen indirect doorspelen naar de burgers. Is de regering het met deze leden eens dat zij het*

bedrijfsleven (het mkb in het bijzonder) en burgers moet ondersteunen in het beter begrijpen van, en in het voldoen aan, deze verordening? Waar blijkt dit uit?

Antwoord
Indien de leden van de VVD-fractie bedoelen te stellen dat de regeldrukeffecten van de verordening indirect kunnen leiden tot een hogere regeldruk of kosten voor gebruikers van tussenhandeldiensten (burgers en bedrijven) dan is dat inderdaad voorstelbaar. Om naleving te verzekeren moeten tussenhandeldiensten mogelijk kosten maken of procedures inrichten. Het kan voorkomen dat die worden doorbelast aan gebruikers of dat gebruikers aanvullende informatie moeten aanleveren. Zoals als gevolg van de verplichtingen uit artikel 30 van de verordening, op grond waarvan aanbieders van onlinemarktplaatsen gehouden zijn om informatie van hun zakelijke gebruikers te registreren, waaronder hun contact- en betaalgegevens, identificatiedocumenten en informatie over hun eventuele inschrijving in het handelsregister.

De regering is het eens met de leden dat het belangrijk is om bedrijven en burgers te ondersteunen in het begrijpen van en het voldoen aan de verordening. Daarbij wordt samengewerkt met de Europese Commissie en de ACM. Zo heeft het kabinet sinds de publicatie van de verordening op verschillende momenten nieuwsberichten uitgebracht waarbij de komst en de doelstellingen van de verordening centraal stonden.[45] Op Ondernemersplein.nl is meer informatie over de verordening geplaatst.[46] De Europese Commissie heeft uitgebreide informatie op haar website geplaatst en via bijvoorbeeld Instagram informatie over de DSA verspreid.[47] De ACM heeft diverse nieuwsberichten over de verordening uitgebracht en werkt aan een leidraad met meer tekst en uitleg over de verordening. Die leidraad is gepubliceerd op haar website. In 2024 wordt een nieuwe versie gepubliceerd, op basis van ontvangen input en ervaringen. De ACM heeft ook recent een rondetafelbijeenkomst georganiseerd over het onderwerp ‘betrouwbare flaggers’, in aanwezigheid van vertegenwoordigers van diverse online platformen en partijen die interesse hebben om trusted flagger te worden.

Het is van belang dat bij de publiekscommunicatie over de verordening de betrokken overheden samenwerken en bewust zijn van de rol die zij vervullen. Het kabinet steunt de ACM hierin door samenwerking met andere toezichthouders te faciliteren en waar nodig informatie te geven over de DSA.[48] Nu de verordening in de uitvoeringsfase is gekomen ligt het primaat om tekst en uitleg te geven over de rechten en verplichtingen van de verordening bij de toezichthouders. Het kabinet wil voorkomen dat zij bij het verspreiden van informatie over de verordening de toezichthouders bij de uitvoering van hun taken onbedoeld in de weg zit.

7.2 Uitvoeringslasten direct voortvloeiend uit de verordening

70) *Het stemt de leden van de VVD-fractie positief te lezen dat de directe kosten voor aanbieders van tussenhandeldiensten volgens de impactanalyse verder in verhouding staan tot de omvang en het bereik van de tussenhandeldienst, evenals de notie dat de uitzonderingen voor het mkb verder voorkomen dat de verordening hoge toetredingsdrempels creëert waardoor de bestaande marktpartijen indirect beschermd zouden worden tegen nieuwe concurrenten. Echter vragen deze leden in hoeverre de regering hierin in acht heeft genomen dat veel mkb’ers vaak intensief samen werken met grotere partijen die lasten en kosten zullen ondervinden van deze verordening. Zal de verordening en de gevolgen hiervan niet indirect ook grote gevolgen hebben voor de uitgesloten partijen zoals het mkb? Waar blijkt dit uit?*

[45] Zie onder meer https://www.rijksoverheid.nl/actueel/nieuws/2024/02/16/dsa-extra-verantwoordelijkheden-gelden-nu-voor-alle-digitale-diensten, https://www.rijksoverheid.nl/actueel/nieuws/2023/08/25/dsa-verplichtingen-voor-en-toezicht-op-allergrootste-online-platforms-ingegaan, https://www.rijksoverheid.nl/actueel/nieuws/2023/02/17/eu-regelgeving-van-start-extra-verantwoordelijkheden-digitale-diensten, en https://www.rijksoverheid.nl/actueel/nieuws/2022/07/05/gebruiker-profiteert-van-nieuwe-regels-voor-digitale-platforms.

[46] https://ondernemersplein.kvk.nl/wet-dsa-online-diensten/ en https://ondernemersplein.kvk.nl/digital-services-act-dsa-komt-met-nieuwe-regels-voor-digitale-dienstverleners/.

[47] Zie https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_nl en onder meer https://www.instagram.com/digitaleu/reels/.

[48] Deze werkzaamheden zien ook op andere nieuwe EU-regelgeving, zoals de Data Governance Act en de Data Act.

Antwoord
De naleving van de verordening kan lasten en kosten veroorzaken voor de aanbieders die er onder vallen. Dat kan onder meer bestaan in de inrichting van procedures zoals een meldingsmechanisme (artikel 16 van de verordening) of het opvragen van informatie van handelaren op online marktplaatsen (artikel 30 van de verordening). Daaraan meewerken of er uitvoering aan geven kan indirect gevolgen hebben voor het mkb dat actief is op online platforms. Daar staat wel tegenover dat mkb-ers die samenwerken met online platforms, bijvoorbeeld door er actief te zijn als handelaar of maker, over het algemeen ook een 'afnemer van de dienst' zijn in de zin van artikel 3, onder b, van de verordening, en daardoor profiteren van de rechten die de verordening creëert voor bijvoorbeeld consumenten.

8. Adviezen en consultatie

8.1 UHT AP

71) *De leden van de GroenLinks-PvdA-fractie zijn verrast te lezen dat de AP een verkeerde inschatting heeft gemaakt ten aanzien van het budget dat zij verwacht nodig te hebben voor de uitvoering van haar taken die volgen naar aanleiding van deze wet. Kan de regering aangeven wat de gevolgen zijn van het te lage budget dat structureel beschikbaar is gemaakt voor de AP? Betekent dit dat de AP niet in staat is om (internationaal) onderzoek te doen? Kan de AP in dat geval nog wel effectief en goed toezicht houden?*

Antwoord
De AP heeft aangegeven dat ze met de vooralsnog beschikbaar gestelde middelen inderdaad niet in staat is om (internationaal) onderzoek te verrichten. Daarvoor stelt zij 2 fte meer nodig te hebben. Dit heeft gevolgen voor het toezicht van de AP. De AP geeft aan dat zij hierdoor zal moeten prioriteren in de taken die zij onder de DSA zal kunnen uitvoeren. Omdat het doen van onderzoek arbeidsintensief is, zal er naar verwachting minder onderzoek plaats kunnen vinden dan de AP nodig acht. De AP gaat hier in haar ambtsbericht naar aanleiding van deze nota nader op in. Er is met de AP afgesproken dat er gedurende 2024 regelmatig wordt gesproken om een zo goed mogelijk beeld te ontwikkelen van de last die het toezicht de AP oplevert en zo te kunnen beoordelen of aanvullende middelen nodig zijn. Indien nodig en mogelijk kan bij Voorjaarsnota 2025 worden besloten om de AP aanvullende middelen te verstrekken vanaf 2025.

72) *Kan de regering aangeven of het verwacht dat het budget van de AP verhoogd kan worden naar het niveau waarvan de AP aangeeft het nodig te hebben om effectief en goed toezicht te kunnen houden en te kunnen handhaven?*

Antwoord
De regering heeft nog geen besluit genomen over het eventueel uitbreiden van de structurele financiering van de AP. Indien nodig en mogelijk kan bij Voorjaarsnota 2025 worden besloten om de AP aanvullende middelen te verstrekken vanaf 2025.

73) *De leden van de D66-fractie constateren dat de AP verwacht 6,6 FTE nodig te hebben, wat resulteert in €977,000 aan extra lasten. Er wordt echter slechts €517,000 structureel beschikbaar gesteld. Kan de regering ingaan op het verhogen van de structurele financiering van de AP voor het houden van toezicht op deze verordening?*

Antwoord
De AP heeft 6,6 fte structureel aangevraagd vanaf 2025, maar 3,2 fte (lees: 517.000 euro) toegezegd gekregen door EZK. Zoals in de antwoorden op vraag 72 en 73 is beschreven is er een afspraak gemaakt met de AP zodat er, indien nodig en mogelijk, bij Voorjaarsnota 2025 kan worden besloten om de AP aanvullende middelen te verstrekken vanaf 2025.

8.2 Advies OM

74) *De leden van de GroenLinks-PvdA-fractie zijn blij te lezen dat ook de Commissie inziet dat een nadere duiding van het begrip "strafbaar feit waarbij het leven of de veiligheid van personen in het*

geding is" wenselijk is en dat zij heeft aangegeven nadere handvatten te willen bieden. Kan de regering aangeven op welke termijn zij verwacht dat de Commissie deze handvatten kan bieden?

Antwoord
Op 2 mei jl. heeft de Europese Commissie de lidstaten verzocht om informatie te leveren die de eerste stap vormt in de uitvoering van artikel 18 van de verordening. De Europese Commissie vraagt de lidstaten daarin onder meer om contactgegevens te verstrekken van de autoriteit(en) waar deze meldingen gedaan moeten worden met het oog om het doen van meldingen door aanbieders van hostingdiensten en online platforms te faciliteren. De Europese Commissie stelt daarin ook voor om de relevante autoriteiten bij elkaar te brengen om dit vraagstuk verder uit te werken. Er is niet bekend op welke termijn dit tot resultaten moet leiden.

75) *Kan de regering tevens aangeven wat haar eigen visie is op dit punt en of zij van plan is om bij de Commissie deze zienswijze kenbaar te maken, zodat de Commissie dit ter overweging kan meenemen? Zo nee, waarom niet?*

Antwoord
Het begrip "strafbaar feit waarbij het leven of veiligheid van een persoon of personen wordt bedreigd" is een autonoom Unierechtelijk begrip. Het is uiteindelijk aan het Hof van Justitie om daar uitleg aan te geven. De regering wil hier geen verdere uitspraken over doen om te voorkomen dat zij een uitleg aan het begrip geeft die mogelijk niet blijkt te stroken met de nadere uitleg waar de Europese Commissie aan werkt. Overweging 56 bij de verordening maakt in ieder geval duidelijk dat het gaat om zeer ernstige strafbare feiten. De overweging noemt als voorbeelden van dergelijke strafbare feiten mensenhandel, seksueel misbruik, seksuele uitbuiting van kinderen, kinderpornografie en terrorisme.

76) *In hoeverre is er nu een uniforme duiding over wat een 'strafbaar feit waarbij het leven of de veiligheid van personen wordt bedreigd', zo vragen de leden van de D66-fractie naar aanleiding van de bijdrage van het Openbaar Ministerie (OM).*

Antwoord
Buiten de voorbeelden die in overweging 56 van de verordening zijn gegeven is er nog geen verdere uniforme duiding over hetgeen een strafbaar feit is waarbij het leven of veiligheid van een persoon of personen wordt bedreigd in de zin van artikel 18 van de verordening.

8.3. Toezicht en grensoverschrijdende bevoegdheid

77) *De leden van de GroenLinks-PvdA-fractie voorzien problemen door het feit dat de AP niet bij andere digitaledienstencoördinatoren verzoeken voor informatie of verzoeken om hun onderzoeksbevoegdheden uit te oefenen kan doen. Kan de regering aangeven of de ACM deze verzoeken namens de AP kan doen bij andere digitaledienstencoördinatoren? Voorziet de regering hier problemen in en wat zijn mogelijke oplossingen?*

Antwoord
De bevoegdheid om een verzoek om informatie te doen of een verzoek om de nodige onderzoeks- en handhavingsmaatregelen te nemen komt inderdaad toe aan de digitaledienstencoördinatoren. Dit sluit aan bij hun verantwoordelijkheid voor de coördinatie op nationaal niveau in verband met kwesties rond het toezicht op de naleving en de handhaving van de verordening en hun samenwerking op Europees niveau. Deze verantwoordelijkheid sluit niet uit dat andere bevoegde nationale autoriteiten, zoals in Nederland de AP, in deze procedures een rol kunnen spelen. Voor onderzoeken in het kader van eventuele inbreuken op de onderdelen van de verordening ten aanzien waarvan de AP toezichthouder is, ligt het in de rede dat de ACM verzoeken om informatie of het nemen van de nodige onderzoeks- en handhavingsmaatregelen aan digitaledienstencoördinatoren doet op verzoek van de AP. De ACM en de AP kunnen hierover afspraken maken in het door het wetsvoorstel voorgeschreven samenwerkingsprotocol. Het kabinet voorziet op dit punt geen problemen.

78) *Betekent dit tevens dat de ACM geen verzoeken kan indienen bij – bijvoorbeeld – de Belgische Gegevensbeschermingsautoriteit indien de Belgische regering heeft besloten om (net als Nederland) een deel van de taken van de digitaledienstencoördinator (bijvoorbeeld de Belgische Mededingingsautoriteit) te delegeren naar de Belgische Gegevensbeschermingsautoriteit?*

Antwoord
De bevoegdheid om een verzoek om informatie te doen of een verzoek om de nodige onderzoeks- en handhavingsmaatregelen te nemen komt inderdaad toe aan de digitaledienstencoördinatoren. Dit sluit aan bij hun verantwoordelijkheid voor de coördinatie op nationaal niveau in verband met kwesties rond het toezicht op de naleving en de handhaving van de verordening en hun samenwerking op Europees niveau. Deze verantwoordelijkheid sluit niet uit dat andere bevoegde nationale autoriteiten, zoals in Nederland de AP, in deze procedures een rol kunnen spelen. Voor onderzoeken in het kader van eventuele inbreuken op de onderdelen van de verordening ten aanzien waarvan de AP toezichthouder is, ligt het in de rede dat de ACM verzoeken om informatie of het nemen van de nodige onderzoeks- en handhavingsmaatregelen aan digitaledienstencoördinatoren doet op verzoek van de AP. De ACM en de AP kunnen hierover afspraken maken in het door het wetsvoorstel voorgeschreven samenwerkingsprotocol. Het kabinet voorziet op dit punt geen problemen.

OVERIG

79) *De leden van de PVV-fractie verzoeken de regering expliciet in te gaan op de term “opruiing”.*

Antwoord
De term ‘opruiing’ wordt niet gebruikt in de digitaledienstenverordening of in het uitvoeringswetsvoorstel. Ook wordt de term niet genoemd in de memorie van toelichting bij het wetsvoorstel. ‘Opruiing’ wordt als term gebruikt in het strafrecht, waarbij het gaat om het in het openbaar, mondeling of bij geschrift of afbeelding, opruien tot een strafbaar feit of tot gewelddadig optreden tegen het openbaar gezag (artikel 131 van het Wetboek van Strafrecht). Naar Nederlands recht vormt opruiing in deze zin dus een strafbaar feit. Tegen online informatie die valt binnen de werkingssfeer van het Nederlandse strafrecht en die voldoet aan de elementen van de strafrechtelijke definitie van ‘opruiing’, kan dus strafvorderlijk worden opgetreden. Ter illustratie kan er verder op gewezen worden dat online materiaal, dat aanzet tot het plegen van een terroristisch misdrijf onder de verordening terroristische inhoud, onder die verordening wordt beschouwd als ‘terroristische inhoud’ waartegen op grond van die verordening kan worden opgetreden. In Nederland gebeurt dat in het kader van de Uitvoeringswet verordening terroristische inhoud. De betreffende online informatie is in deze gevallen ook te beschouwen als ‘illegale inhoud’ in het kader van de digitaledienstenverordening. Aanbieders van tussenhandeldiensten moeten aan de verplichtingen van de verordening voldoen met betrekking tot dit soort illegale inhoud, zoals het instellen van een gemakkelijk toegankelijk en gebruiksvriendelijk kennisgevings- en actiemechanisme.

80) *De leden van de GroenLinks-PvdA-fractie verzoeken de regering om te reflecteren op de invloed van de DSA op twee specifieke casussen. De eerste casus betreft een website die specifiek gericht is op deepfakepornografie. Hierop bevinden zich dan ook talloze pornografische filmpjes, gemaakt met deepfaketechnologie, van bekende Nederlanders en politici. Deze website wordt niet gehost door een bedrijf dat zich bevindt binnen de Europese Unie, heeft geen wettelijk vertegenwoordiger in de EU en reageert niet op e-mailcommunicatie. Welke mogelijkheden biedt de DSA de digitaledienstencoördinator, in dit geval de ACM, om op te treden tegen een dergelijke website die overduidelijk illegale content plaatst en gebruikers aanmoedigt om zo veel mogelijk van dergelijke content te plaatsen? Kan de regering aangeven wat de escalatieladder is van de ACM en of de DSA uiteindelijk mogelijkheden biedt om dit soort websites te laten blokkeren? Welke mogelijkheden en verantwoordelijkheden hebben slachtoffers zelf?*

Antwoord
Als een aanbieder van een tussenhandeldienst buiten de Europese Unie is gevestigd en geen wettelijke vertegenwoordiger heeft aangewezen, dan beschikken alle lidstaten en, indien de aanbieder een zeer groot online platform of zeer grote online zoekmachine is, de Europese

Commissie, over de bevoegdheid tot toezicht en handhaving van de digitaledienstenverordening. Dat betekent dat de ACM, indien geen sprake is van een situatie waarin de Europese Commissie exclusief bevoegd is, ook over deze bevoegdheid beschikt.

Voor de goede orde wordt opgemerkt dat het hierbij gaat om de naleving van de verplichtingen uit de digitaledienstenverordening, zoals het zorgvuldig nemen van besluiten over inhoudsmoderatie en het hebben van een effectief kennisgevings- en actiemechanisme. De verordening biedt dus geen grondslag voor de ACM om op te treden tegen de feiten zoals genoemd in de vraag of om de aanbieder van de onlinedienst in kwestie te sanctioneren voor het opslaan of verspreiden van dergelijk materiaal. In het antwoord op vraag 8 is ingegaan op de mogelijkheden die buiten de digitaledienstenverordening bestaan om op treden tegen de verspreiding van dit type illegale inhoud.

De verplichtingen uit de verordening bieden echter wel aanvullende mogelijkheden om op te treden tegen een website die, zoals in de vraag wordt gesteld, overduidelijk illegale content plaatst en gebruikers aanmoedigt om zo veel mogelijk van dergelijke content te plaatsen.

Indien de ACM constateert dat de aanbieder in kwestie inbreuk maakt op de verplichtingen van de DSA, dan dient zij eerst gebruik te maken van de in artikel 51, eerste en tweede lid, van de verordening genoemde onderzoeks- en handhavingsbevoegdheden, waaronder de bevoegdheid om remedies, dwangsommen en boetes aan aanbieders op te leggen. Als een aanbieder niet in de Unie is gevestigd, geen wettelijke vertegenwoordiger heeft aangewezen en ook niet reageert op communicatie van de ACM, dan kan worden aangenomen dat de inzet van deze bevoegdheden niet voldoende zal zijn om de inbreuken te beëindigen. In dat geval biedt artikel 53, derde lid, van de verordening aanvullende bevoegdheden voor de ACM. Voorwaarde is wel dat er sprake is van ‘ernstige schade’, die naast uitoefening van de bovengenoemde bevoegdheden, ook niet kan worden vermeden door de uitoefening van bevoegdheden buiten het kader van de digitaledienstenverordening. Daarbij kan bijvoorbeeld gedacht worden aan bevoegdheden in het kader van het strafrecht, tegen de gebruikers die de illegale inhoud plaatsen of tegen de aanbieder van de onlinedienst.[49] Is dat naar oordeel van de ACM het geval, dan kan zij eerst eisen dat het leidinggevend personeel van de aanbieder onverwijld een actieplan opstelt om de inbreuk te beëindigen.

Als de inbreuk dan alsnog blijft bestaan en de inbreuk bovendien neerkomt op een strafbaar feit waarbij het leven of de veiligheid van personen wordt bedreigd, dan kan de ACM, na het verkrijgen van een machtiging van de rechter-commissaris, besluiten dat de toegang tot de website in kwestie tijdelijk wordt beperkt (zie de artikelen 2.5, eerste lid, onderdeel c, en 2.6 van het wetsvoorstel). Deze maatregel houdt in dat de toegang tijdelijk wordt beperkt van afnemers tot de gehele dienst die bij de inbreuk is betrokken, of tot de online-interface daarvan. Bij dit laatste kan worden gedacht aan het laten blokkeren van de website die toegang biedt tot de betreffende tussenhandeldienst. De maatregel kan niet alleen worden opgelegd aan de aanbieder van de tussenhandeldienst die de verordening overtreedt, maar ook aan een derde die technisch in staat is om de maatregelen uit te voeren. Dat kan een internetprovider, een aanbieder van een hostingdienst, een aanbieder van een online platform zoals een app-store, of andere dienstaanbieder in de keten zijn.

Zoals is opgemerkt in het antwoord op vraag 74 van de leden van uw fractie, bestaat er op dit moment nog geen duidelijkheid over de reikwijdte van het begrip ‘strafbaar feit waarbij het leven of de veiligheid van personen wordt bedreigd’. De Europese Commissie zal daarover nog nadere duidelijkheid gaan verschaffen. Op dit moment is dan ook niet aan te geven of het online verspreiden van deepfakepornografie binnen de reikwijdte van dat begrip valt en of de bevoegdheid tot het tijdelijk blokkeren van websites toegepast kan worden ten aanzien van inbreuken op de verordening die met dat type illegale inhoud samenhangen.

Slachtoffers van dit type illegale inhoud hebben op grond van de verordening de mogelijkheid om bij de ACM een klacht in te dienen tegen de desbetreffende aanbieder wegens vermeende inbreuk

[49] Zie ook de brief van de minister voor Rechtsbescherming en de minister van Justitie en Veiligheid over de regulering van deepfakes en immersieve technologieën (Kamerstukken II, 2022/23, 26643, nr. 1041).

op de verplichtingen van de verordening. Daarnaast kan een slachtoffer bij de civiele rechter een procedure starten tegen deze aanbieder, omdat deze onrechtmatig handelt jegens hem of haar door de verplichtingen van de verordening te overtreden. Voor een beschrijving van de overige mogelijkheden buiten de digitaledienstenverordening voor het slachtoffer om op te treden tegen dit type illegale inhoud zij verwezen naar de brief van de minister voor Rechtsbescherming en de minister van Justitie en Veiligheid over de regulering van deepfakes en immersieve technologieën.[50]

81) *De tweede casus betreft ¨exposegroepen¨ en groepen waarin drugs wordt verkocht op Telegram. Soms betreft dit openbare groepen, soms betreft dit besloten groepen. Telegram heeft inmiddels een wettelijke vertegenwoordiger in België. Kan de regering aangeven welke middelen de DSA biedt om op te treden tegen dergelijke exposegroepen en groepen waarin drugs wordt verkocht op Telegram? Kan de regering aangeven wat de mogelijkheden zijn indien Telegram niet meewerkt met opgelegde maatregelen?*

Antwoord
De vraag maakt terecht een onderscheid tussen openbare en besloten groepen op Telegram. De applicatie Telegram bestaat namelijk uit verschillende diensten die anders gekwalificeerd moeten worden onder de verordening. De bepalingen van de verordening zijn alleen van toepassing op de diensten van een aanbieder die kwalificeren als tussenhandeldienst en niet op andere diensten van de aanbieder die geen tussenhandeldiensten zijn (overweging 15 bij de verordening). In het geval dat een aanbieder verschillende soorten tussenhandeldiensten aanbiedt, zijn op elke specifieke tussenhandeldienst van die aanbieder alleen die bepalingen van toepassing die gelden voor dat type tussenhandeldienst.

De applicatie Telegram maakt besloten communicatie tussen één of meerdere gebruikers mogelijk, maar ook openbare communicatie waarbij informatie in een openbare groep beschikbaar wordt gemaakt voor een mogelijk onbeperkt aantal derden. De besloten communicatie moet worden beschouwd als interpersoonlijke communicatiedienst in de zin van artikel 2, onder 5, van richtlijn 2018/1972/EU. Net zoals bijvoorbeeld de diensten van WhatsApp, Skype en Signal. Uit overweging 14 van de verordening blijkt dat interpersoonlijke communicatiediensten niet onder de definitie van een online platform vallen. Openbare groepen kwalificeren mogelijk wel als online platform in de zin van artikel 3, onderdeel i, van de verordening). De informatie in die groepen wordt op verzoek van gebruikers opgeslagen en verspreid bij het publiek. Verspreiding bij het publiek wordt in artikel 3, onderdeel k, van de verordening namelijk gedefinieerd als "*het op verzoek van de informatieverstrekkende afnemer van de dienst beschikbaar stellen van informatie aan een mogelijk onbeperkt aantal derden*". Dat lijkt voor openbare groepen op Telegram het geval.

Indien in de toezichtspraktijk en de rechtspraak dezelfde kwalificatie aan de verschillende diensten van de applicatie Telegram gegeven wordt, dan zijn de verplichtingen voor online platforms uit de verordening van toepassing op de openbare groepen van Telegram. Dit betekent onder meer dat Telegram een contactpersoon moet hebben voor lidstatelijke autoriteiten, de digitaledienstenraad, en de Europese Commissie (artikel 11 van de verordening). Er moet verder een mechanisme zijn waarmee illegale inhoud bij Telegram kan worden gemeld (artikel 16 van de verordening) waarbij meldingen van 'betrouwbare flaggers' prioritair en onverwijld moeten worden verwerkt en afgehandeld (artikel 22 van de verordening). Er moet tevens beleid worden ontwikkeld om misbruik te bestrijden en gebruikers die frequent kennelijk illegale inhoud verspreiden moeten voor een redelijke periode worden geschorst (artikel 23 van de verordening). Mocht het gebruik van openbare groepen ooit de grens van 45 miljoen maandelijks actieve gebruikers in de EU overschrijden dan kan de Europese Commissie deze dienst van Telegram aanwijzen als 'zeer groot online platform' waardoor ook de verplichtingen voor die diensten van toepassing worden.

De Belgische digitaledienstencoördinator is de bevoegd toezichthouder voor de online platformdienst van Telegram en moet toezien op naleving van de verordening. Daarbij kan gebruik worden gemaakt van de (samenwerkings)mechanismen die in het antwoord op vraag 53 zijn beschreven. Indien een digitaledienstencoördinator constateert dat een aanbieder inbreuk maakt op de verplichtingen van de DSA, dan dient zij eerst gebruik te maken van de in artikel 51, eerste

[50] Kamerstukken II, 2022/23, 26643, nr. 1041, blz. 3-4.

en tweede lid, van de verordening genoemde onderzoeks- en handhavingsbevoegdheden, waaronder de bevoegdheid om remedies, dwangsommen en boetes aan aanbieders op te leggen. In het geval de inzet van deze bevoegdheden niet voldoende is om de inbreuken te beëindigen, biedt artikel 53, derde lid, van de verordening aanvullende bevoegdheden voor de digitaledienstencooördinator. Voorwaarde is wel dat er sprake is van ‘ernstige schade’, die naast uitoefening van de bovengenoemde bevoegdheden, ook niet kan worden vermeden door de uitoefening van bevoegdheden buiten het kader van de digitaledienstenverordening. Daarbij kan bijvoorbeeld gedacht worden aan bevoegdheden in het kader van het strafrecht, tegen de gebruikers die de illegale inhoud plaatsen of tegen de aanbieder van de onlinedienst. Is dat het geval, dan kan de digitaledienstencoördinator eerst eisen dat het leidinggevend personeel van de aanbieder onverwijld een actieplan opstelt om de inbreuk te beëindigen. Als de inbreuk dan alsnog blijft bestaan en de inbreuk bovendien neerkomt op een strafbaar feit waarbij het leven of de veiligheid van personen wordt bedreigd, dan kan de digitaledienstencoördinator, na tussenkomst van de bevoegde gerechtelijke autoriteit, de toegang tot de website in kwestie tijdelijk beperken. Zie hiervoor nader het antwoord op vraag 80.