MEMORIE VAN TOELICHTING

Inhoud

A. ALGEMEEN DEEL VAN DE MEMORIE VAN TOELICHTING 4
1 Inleiding 4
1.1 Inleiding 4
1.2 De verordening in vogelvlucht 4
1.3 Totstandkoming van de verordening 5
1.4 Leeswijzer memorie van toelichting 5
2 Doel, reikwijdte en belangrijkste begrippen van de digitaledienstenverordening 6
2.1 Doel en achtergrond van de verordening 6
2.2 Volledige harmonisatie en ruimte voor aanvullende nationale regels 7
2.3 Reikwijdte van de verordening: tussenhandeldiensten aangeboden in de Unie 8
2.3.1 Het begrip “tussenhandeldienst” 8
2.3.2 Het begrip “dienst van de informatiemaatschappij” 8
2.3.3 De begrippen “mere conduit”, “caching” en “hosting” 9
2.3.4 Het begrip “aangeboden in de Unie” 10
2.4 Andere belangrijke begrippen in de verordening 11
2.4.1 Inleiding 11
2.4.2 Het begrip “illegale inhoud” 11
2.4.3 Het begrip “desinformatie of andere inhoud” 12
2.4.4 Het begrip “inhoudsmoderatie” 13
2.4.5 Het begrip “online platform” 13
2.4.6 Het begrip “online zoekmachine” 14
3 Aansprakelijkheid van aanbieders van tussenhandeldiensten 14
3.1 Inleiding 14
3.2 Het kader voor aansprakelijkheid van tussenhandeldiensten voor door afnemers verstrekte informatie 14
3.2.1 Inhoud verordening 14
3.2.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel 18
3.3 Verbod op algemene verplichting tot monitoring of actief feitenonderzoek 21
3.3.1 Inhoud verordening 21
3.3.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel 21
3.4 Eisen aan bevelen om op te treden tegen illegale inhoud of om informatie te verstrekken 21
3.4.1 Inhoud verordening 21
3.4.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel 23
4 Zorgvuldigheidsverplichtingen voor aanbieders van tussenhandeldiensten 25

4.1 Inleiding....25
4.2 Situatie onder de richtlijn elektronische handel....25
4.2.1 Het kader onder de richtlijn elektronische handel....25
4.2.2 Zorgvuldigheidsverplichtingen in het nationale recht....26
4.2.3 Zorgvuldigheidsverplichtingen in ander EU-recht....26
4.2.4 Gedragscodes....27
4.3 Inhoud verordening....28
4.3.1 Algemeen....28
4.3.2 Verplichtingen die gelden voor alle aanbieders van tussenhandeldiensten....30
4.3.3 Aanvullende verplichtingen voor aanbieders van hostingdiensten....32
4.3.4 Aanvullende verplichtingen voor online platforms....34
4.3.5 Aanvullende verplichtingen voor online-marktplaatsen waar handelaren producten of diensten aanbieden aan consumenten....40
4.3.6 Aanvullende verplichtingen voor zeer grote online platforms en zeer grote online zoekmachines....42
4.3.7 Normen, gedragscodes en crisisprotocollen....47
5 Uitvoering, samenwerking, toezicht en handhaving....48
5.1 Inleiding....48
5.2 Aanwijzing digitaledienstencoördinator en andere bevoegde autoriteiten....48
5.2.1 Inhoud verordening....48
5.2.2 Uitvoering in Nederland....49
5.3 Toezicht en handhaving....50
5.3.1 Afbakening bevoegdheid tot toezicht en handhaving....50
5.3.2 Onderzoeksbevoegdheden....53
5.3.3 Verbindendverklaring toezeggingen en bindende aanwijzingen....54
5.3.4 Voorlopige maatregelen bij ernstige schade....55
5.3.5 Maatregelen bij ernstige en aanhoudende inbreuken....55
5.3.6 Boete en dwangsom....59
5.3.7 Klachtrecht....62
5.3.8 Schadevergoeding....63
5.3.9 Wederzijdse bijstand, samenwerking en bijstand aan de Commissie....63
5.3.10 Toezicht en handhaving door de Commissie....64
5.4 Overige taken digitaledienstencoördinator....67
5.4.1 Inleiding....67
5.4.2 Ontvangen en doorzenden van afschriften van bevelen aan aanbieders....67
5.4.3 Certificering en toekenning formele statussen....67

5.4.4 Activiteitenverslag 68
5.4.5 Deelname digitaledienstenraad 69
6 Samenwerking en gegevensuitwisseling tussen autoriteiten....69
6.1 Samenwerking tussen de bevoegde autoriteiten en met andere autoriteiten....69
6.2 Gegevensuitwisseling 70
6.2.1 Gegevensuitwisseling tussen de AP en de ACM....70
6.2.2 Gegevensuitwisseling tussen de ACM, de politie en het OM 72
7 Verhouding tot ander EU-recht....73
7.1.1 Digitalemarktenverordening....75
7.1.2 Richtlijn audiovisuele mediadiensten 75
7.1.3 Verordening terroristische online-inhoud....76
7.1.4 Auteursrecht in de digitale eengemaakte markt....76
7.1.5 Consumentenrecht 77
7.1.6 Algemene verordening gegevensbescherming....77
7.1.7 Platform-to-business verordening....77
7.1.8 De verordening inzake algemene productveiligheid 78
8 Gevolgen....78
8.1 Regeldruk en nalevingslasten van de Uitvoeringswet....78
8.2 Uitvoeringslasten direct voortvloeiend uit de verordening....79
8.2.1 Gevolgen voor aanbieders van tussenhandeldiensten 80
8.2.2 Gevolgen voor het mkb 81
8.2.3 Gevolgen voor afnemers....81
8.2.4 Gevolgen voor toezichthouders 81
9 Adviezen en consultatie 82
9.1 ACM....82
9.2 AP 82
9.3 Internetconsultatie....82
B. ARTIKELSGEWIJZE TOELICHTING....83
C. BIJLAGE BIJ DE TOELICHTING....92

A. ALGEMEEN DEEL VAN DE MEMORIE VAN TOELICHTING

1 Inleiding

1.1 *Inleiding*

Met dit wetsvoorstel wordt uitvoering gegeven aan verordening 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 (digitaledienstenverordening) (PbEU 2022, L 277). De digitaledienstenverordening (hierna ook: de verordening) harmoniseert de regels die van toepassing zijn op tussenhandeldiensten, met als doel te zorgen voor een veilige, voorspelbare en betrouwbare online omgeving, waarin de verspreiding van illegale online-inhoud en de maatschappelijke risico's die de verspreiding van desinformatie of andere inhoud met zich kunnen brengen, worden aangepakt en waarin de grondrechten doeltreffend worden beschermd en innovatie wordt vergemakkelijkt. Daartoe bevat de verordening enerzijds een kader voor de aansprakelijkheid van aanbieders van tussenhandeldiensten voor door hun gebruikers verstrekte informatie en anderzijds een aantal zorgvuldigheidsverplichtingen waar deze aanbieders aan moeten voldoen bij het verlenen van hun diensten. De verordening wordt grotendeels op 17 februari 2024 van toepassing en op die datum moeten de lidstaten hebben voorzien in de aanwijzing van een digitaledienstencoördinator en de benodigde nationale uitvoeringswetgeving.[1]

Onderhavig wetsvoorstel voorziet in bepalingen ter uitvoering van de verordening. De verordening werkt rechtstreeks, dus in dit wetsvoorstel zijn enkel de bepalingen opgenomen die nodig zijn om de verordening uit te voeren in de Nederlandse rechtsorde. Hoofdstuk 1 van het wetsvoorstel bevat de begripsbepalingen. In de hoofdstukken 2 en 3 van het wetsvoorstel worden de Autoriteit Consument en Markt (hierna: ACM) aangewezen als digitaledienstencoördinator voor de toepassing van de verordening en als toezichthouder op het grootste deel van de verordening en de Autoriteit Persoonsgegevens (hierna: AP) als andere bevoegde autoriteit, voor het toezicht op twee bepalingen die zien op de verwerking van persoonsgegevens. Ook worden in deze hoofdstukken regels gesteld over de bevoegdheden voor het toezicht op en de handhaving van de zorgvuldigheidsverplichtingen voor aanbieders van tussenhandeldiensten. Hoofdstuk 4 van het wetsvoorstel bevat bepalingen over de samenwerking tussen de AP en de ACM en over gegevensuitwisseling. Hoofdstuk 5 van het wetsvoorstel bevat tot slot wijzigingen van andere wetgeving, dit onder meer in verband met het kader voor de aansprakelijkheid van aanbieders van tussenhandeldiensten. In de bijlage bij deze memorie van toelichting is een transponeringstabel opgenomen.

1.2 *De verordening in vogelvlucht*

De verordening bestaat uit 5 hoofdstukken. Hoofdstuk I van de verordening bevat algemene bepalingen en definities en regelt het onderwerp en toepassingsgebied van de verordening.

Hoofdstuk II van de verordening bevat voorwaardelijke vrijstellingen van aansprakelijkheid voor aanbieders van tussenhandeldiensten voor door hun gebruikers verstrekte informatie. Deze

[1] Met uitzondering van de artikelen 24, tweede, derde en zesde lid, 33, derde tot en met zesde lid, 37, zevende lid, 40, dertiende lid, 43, en de afdelingen 4, 5 en 6 van hoofdstuk IV. Deze artikelen zien met name op de aanwijzing van zeer grote online platforms en zeer grote online zoekmachines. Tot nu toe zijn 17 zeer grote online platforms en twee zeer grote online zoekmachines aangewezen. De verordening is voor hen van toepassing vanaf 25 augustus 2023. De Europese Commissie is vanaf die datum bevoegd tot toezicht en handhaving.

bepalingen waren voorheen neergelegd in artikel 12 tot en met 15 van de richtlijn inzake elektronische handel[2] en zijn nu opgenomen in de verordening met enkele verduidelijkingen.

Hoofdstuk III van de verordening bevat zorgvuldigheidsverplichtingen waar aanbieders van tussenhandeldiensten aan moeten voldoen. De verplichtingen verschillen al naar gelang het type dienst dat een onderneming aanbiedt en zijn rol, omvang en invloed op de maatschappij, de belangen van gebruikers en de economie. De verordening maakt daarbij onderscheid tussen vier categorieën aanbieders, namelijk aanbieders van (1) alle soorten tussenhandeldiensten, (2) hostingdiensten, (3) online platforms en (4) zeer grote online platforms en zeer grote online zoekmachines. Aan welke verplichtingen een onderneming moet voldoen, hangt af van de dienst of diensten die hij levert. De verplichtingen nemen met elke categorie toe. Aanbieders van zeer grote online platforms en zeer grote online zoekmachines moeten dus voldoen aan de zwaarste zorgvuldigheidsverplichtingen.

Hoofdstuk IV van de verordening bevat regels over de uitvoering, het toezicht op en de handhaving van de verordening. De verordening bepaalt dat elke lidstaat een digitaledienstencoördinator moet aanwijzen voor de uitvoering, het toezicht op en de handhaving van de verordening. De lidstaten kunnen verder een of meer andere bevoegde autoriteiten aanwijzen voor de uitvoering, het toezicht en de handhaving. Ook wordt er een onafhankelijke adviesgroep van digitaledienstencoördinatoren in het leven geroepen: de Europese Raad voor digitale diensten. De Europese Commissie (hierna: Commissie) wordt belast met het toezicht op en de handhaving van de verordening ten aanzien van de verplichtingen die uitsluitend gelden voor aanbieders van zeer grote online platforms en zeer grote online zoekmachines.

Hoofdstuk V van de verordening bevat de slotbepalingen. Hierin is onder andere voorzien in het vervallen van de artikelen 12 tot en met 15 van de richtlijn elektronische handel over de aansprakelijkheid voor aanbieders van tussenhandeldiensten, een evaluatie en de inwerkingtreding van de verordening.

1.3 *Totstandkoming van de verordening*

Op 15 december 2020 publiceerde de Commissie het voorstel voor de digitaledienstenverordening. Na ruim een jaar onderhandelen werd er op 23 april 2022 een onderhandelingsakkoord bereikt tussen de Raad, het Europees Parlement en de Commissie. Het Europees Parlement stemde op 5 juli 2022 in met de definitieve tekst. De Raad volgde op 4 oktober 2022. De verordening werd vervolgens op 27 oktober 2022 gepubliceerd in het Publicatieblad en trad op 16 november 2022 in werking.

1.4 *Leeswijzer memorie van toelichting*

In de hoofdstukken 2, 3, 4 en 5 van deze memorie van toelichting worden de bepalingen van de verordening toegelicht. Daarbij wordt de opbouw van de verordening gevolgd. In hoofdstuk 2 van de memorie van toelichting worden het doel, de reikwijdte en de belangrijkste begrippen van de verordening beschreven. Hoofdstuk 3 van de memorie van toelichting gaat nader in op het kader voor de aansprakelijkheid van aanbieders van tussenhandeldiensten neergelegd in de verordening. Hoofdstuk 4 van deze memorie van toelichting heeft betrekking op de zorgvuldigheidsverplichtingen waar de aanbieders van tussenhandeldiensten aan moeten voldoen. Hoofdstuk 5 van deze memorie van toelichting gaat in de op de uitvoering, het toezicht op en de handhaving van de verordening, waaronder de aanwijzing van de digitaledienstencoördinator en andere bevoegde autoriteiten.

[2] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG 2000, L 178).

Hoofdstuk 6 gaat in op de samenwerking en gegevensuitwisseling tussen autoriteiten. In hoofdstuk 7 van de memorie van toelichting wordt ingegaan op de verhouding tussen de verordening en andere Europese wetgeving. In hoofdstuk 8 wordt stilgestaan bij de gevolgen van de verordening en het wetsvoorstel. In hoofdstuk 9 van de memorie van toelichting wordt tot slot ingegaan op de ontvangen adviezen en consultatiereacties.

De verschillende artikelen van het wetsvoorstel worden in het algemene deel toegelicht samen met de bepaling van de verordening waar dat artikel van het wetsvoorstel uitvoering aan geeft. Daarbij wordt ook ingegaan op de uitvoering van de verordening in Nederland. Dat betekent dat in hoofdstuk 3 van deze memorie wordt ingegaan op de doorwerking van het kader voor aansprakelijkheid voor aanbieders van tussenhandeldiensten in de Nederlandse rechtsorde. In hoofdstuk 5 van deze memorie van toelichting worden de bepalingen in het wetsvoorstel met betrekking tot de uitvoering van, het toezicht op en de handhaving van de verordening door de ACM en de AP toegelicht. De bepalingen van de verordening inzake het doel, de reikwijdte en de belangrijkste begrippen (hoofdstuk I van de verordening) en de zorgvuldigheidsverplichtingen voor aanbieders van tussenhandeldiensten behoeven op zichzelf geen uitvoeringsregels in dit wetsvoorstel en de hoofdstukken 2 en 4 van deze memorie die daar betrekking op hebben, bevatten dan ook enkel een toelichting op de bepalingen van de verordening.

2 Doel, reikwijdte en belangrijkste begrippen van de digitaledienstenverordening

2.1 *Doel en achtergrond van de verordening*

Blijkens artikel 1, eerste lid, van de verordening beoogt deze bij te dragen aan een goede werking van de interne markt voor tussenhandeldiensten door te voorzien in geharmoniseerde regels voor een veilige, voorspelbare en betrouwbare onlineomgeving. Deze regels dienen verschillende doelen: enerzijds het aanpakken van de verspreiding van illegale online-inhoud en de maatschappelijke risico's van de verspreiding van desinformatie en andere inhoud en anderzijds de doeltreffende bescherming van de grondrechten zoals verankerd in het Handvest van de Grondrechten van de Europese Unie (hierna: het Handvest) en het vergemakkelijken van innovatie (zie overweging 9 bij de verordening).

Om op het internet het verspreiden en delen van informatie mogelijk te maken zijn er aanbieders van tussenhandeldiensten (ook wel tussenpersonen genoemd), die informatie van derden op hun verzoek doorgeven of al dan niet tijdelijk opslaan. De diensten van deze tussenpersonen kunnen ook worden gebruikt om illegale informatie te ontsluiten. Dat heeft de vraag opgeroepen in hoeverre deze dienstverleners verantwoordelijk zijn voor de door hen doorgegeven of opgeslagen informatie en in hoeverre zij daarvoor in juridische zin aansprakelijk zijn. Ten behoeve van de rechtszekerheid en de borging van de interne markt, zijn daarover op EU-niveau in 2000 regels vastgesteld in de richtlijn elektronische handel.

De richtlijn elektronische handel, en de daarin neergelegde regels over de aansprakelijkheid van tussenpersonen in het bijzonder, zijn belangrijk geweest voor de ontwikkeling van tussenhandeldiensten in de afgelopen twintig jaar en investeringen in de onderliggende infrastructuur. Denk bijvoorbeeld aan investeringen in de aanleg van glasvezelnetwerken, de bouw van datacentra en de ontwikkeling van online platforms en online marktplaatsen. De in de richtlijn elektronische handel vervatte beperking van aansprakelijkheid voor de informatie die tussenpersonen ten behoeve van hun klanten doorgeven of opslaan en het verbod op algemene toezichtverplichtingen, creëerde daarvoor de noodzakelijke rechts- en investeringszekerheid.

Sinds de vaststelling van de richtlijn elektronische handel in 2000 zijn veel nieuwe en innovatieve tussenhandeldiensten ontstaan, waaronder online platforms, sociale netwerken en online marktplaatsen. Grote spelers zoals Facebook, YouTube, Twitter en TikTok bestonden in 2000 bijvoorbeeld nog niet. Het gebruik van tussenhandeldiensten voor sociale, recreatieve, culturele, politieke en commerciële doeleinden is bovendien enorm toegenomen. Deze diensten hebben het dagelijks leven van de Unieburgers en de manier waarop zij communiceren, verbinding maken, consumeren en zakendoen, aanzienlijk veranderd. Ze zijn een drijvende kracht geworden achter maatschappelijke en economische veranderingen in de Unie en de rest van de wereld en ze hebben geleid tot allerlei innovaties. De economie en maatschappij zijn in grote mate afhankelijk geworden van digitale diensten. Dit werd bijvoorbeeld zichtbaar tijdens de COVID-19 pandemie. Het belang van tussenhandeldiensten voor de vrijheid van informatie, ondernemerschap en innovatie is dan ook alleen maar toegenomen.

Tegelijkertijd brengt het gebruik van die nieuwe en innovatieve tussenhandeldiensten ook nieuwe maatschappelijke risico's met zich mee, zoals de verspreiding van illegale inhoud en online desinformatie. Hoewel de bepalingen van de richtlijn elektronische handel over het algemeen technologie-neutraal zijn geformuleerd en de kernbeginselen van de richtlijn nog steeds overeind staan, achtte de Uniewetgever het nodig dit kader voor tussenhandeldiensten te moderniseren en uit te breiden. Om die reden heeft de Europese wetgever het kader voor de beperking van de aansprakelijkheid voor aanbieders van tussenhandeldiensten op onderdelen aangepast en aangevuld (zie hierover nader hoofdstuk 3 van deze memorie van toelichting).

Voorts is het uitgangspunt van de verordening dat tussenpersonen een dermate belangrijke rol spelen bij de verspreiding van informatie op het internet, dat verwacht mag worden dat zij bij het verlenen van hun diensten een grote mate van zorgvuldigheid betrachten. Dit uitgangspunt heeft geresulteerd in verschillende nieuwe geharmoniseerde zorgvuldigheidsverplichtingen voor deze aanbieders (zie hierover nader hoofdstuk 4 van deze memorie van toelichting). In overweging 27 bij de verordening wordt tegelijkertijd benadrukt dat, ondanks deze bijzondere positie van aanbieders van tussenhandelsdiensten, het probleem van illegale online-inhoud en illegale online-activiteiten niet mag worden aangepakt door zich uitsluitend te richten op deze aanbieders. Waar mogelijk moeten conflicten over dergelijke inhoud worden opgelost bij de bron, zonder deze aanbieders daarbij te betrekken.

2.2 *Volledige harmonisatie en ruimte voor aanvullende nationale regels*

De verordening voorziet blijkens artikel 1 van de verordening in geharmoniseerde regels over het aanbieden van tussenhandeldiensten op de interne markt. Blijkens overweging 9 bij de verordening harmoniseert de verordening de regels die van toepassing zijn op tussenhandeldiensten op de interne markt volledig. De lidstaten mogen derhalve geen aanvullende nationale eisen stellen of in stand houden die binnen het toepassingsgebied van de verordening vallen, tenzij daarin uitdrukkelijk is voorzien in de verordening, zo wordt gesteld in die overweging. Dat zou namelijk ten koste gaan van de rechtstreekse en uniforme toepassing van de volledig geharmoniseerde regels overeenkomstig de doelstellingen van de verordening.

Het kader voor de voorwaardelijke aansprakelijkheidsvrijstelling van aanbieders van tussenhandeldiensten (hoofdstuk II van de verordening) biedt de nodige ruimte voor nationale bepalingen. Net als de richtlijn elektronische handel, harmoniseert de verordening namelijk slechts de voorwaarden voor de aansprakelijkheidsvrijstellingen, maar laat zij het aan het nationale recht om te bepalen in welke gevallen aanbieders van tussenhandeldiensten *wel* aansprakelijk gesteld kunnen worden als zij niet aan die voorwaarden voldoen. In paragraaf 3.2.2 van deze memorie van

toelichting wordt toegelicht hoe daar in het huidige Nederlandse recht en in onderhavig wetsvoorstel invulling aan is gegeven. Ook ten aanzien van de minimumeisen aan bevelen die kunnen worden opgelegd aan aanbieders van tussenhandeldiensten voor het verwijderen van inhoud of het verstrekken van informatie over afnemers laat de verordening ruimte om in het nationale recht aanvullende en zelfs afwijkende eisen te stellen. Zie daarvoor paragraaf 3.4.2 van deze memorie van toelichting.

De regels over zorgvuldigheidsverplichtingen op maat voor bepaalde categorieën van aanbieders van tussenhandeldiensten (hoofdstuk III van de verordening) voorzien in volledige harmonisatie. 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. Het is dus ook niet mogelijk om zorgvuldigheidsverplichtingen die voor een bepaalde categorie van aanbieders van tussenhandeldiensten gelden, in het nationale recht op te leggen aan aanbieders die tot een andere categorie behoren. De verordening laat wel ruimte om zorgvuldigheidsverplichtingen op te leggen die een ander doel dienen dan de verordening, uiteraard met inachtneming van regels inzake het vrije verkeer van diensten van de informatiemaatschappij (artikelen 3 en 4 van de richtlijn elektronische handel).

2.3 *Reikwijdte van de verordening: tussenhandeldiensten aangeboden in de Unie*

2.3.1 Het begrip “tussenhandeldienst”

Een tussenhandeldienst is één van de in artikel 3, onderdeel g, van de verordening genoemde diensten van de informatiemaatschappij. Dat artikel onderscheidt mere conduitdiensten, cachingdiensten en hostingdiensten. Het onderscheid naar het type dienst is relevant voor de vraag welke bepalingen van de verordening van toepassing zijn op een bepaalde dienst.

Uit overweging 29 bij de verordening kan worden afgeleid dat onder het begrip “tussenhandeldiensten” een breed scala aan economische activiteiten valt, die online plaatsvinden, voor informatiedoorgifte zorgen en voortdurend evolueren. De beoordeling of een dienst beschouwd moet worden als een “tussenhandeldienst”, moet blijkens diezelfde overweging van geval tot geval gebeuren en hangt enkel af van de technische functies van de dienst. Tussenhandeldiensten kunnen afzonderlijk, als onderdeel van een andere soort tussenhandeldienst of gelijktijdig met een andere tussenhandeldienst worden aangeboden. Tot slot kan een tussenhandeldienst ook gelijktijdig met een andere dienst, die geen tussenhandeldienst is, worden aangeboden.

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, tot slot, 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.

Blijkens artikel 2, tweede lid, 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. Een voorbeeld is een schoonmaakdienst die wordt aangeboden via een online platform. De verordening doet dan ook geen afbreuk aan de eisen die in het Unierecht of het nationale recht aan de uitoefening van dergelijke diensten worden gesteld.

2.3.2 Het begrip “dienst van de informatiemaatschappij”

Tussenhandeldiensten zijn diensten van de informatiemaatschappij, zo volgt uit artikel 3, onderdeel g, van de verordening. Voor de definitie van het begrip "dienst van de informatiemaatschappij" verwijst de verordening naar artikel 1, onderdeel b, van de zogenoemde notificatierichtlijn. [3] Op grond van die definitie is een dienst van de informatiemaatschappij elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van die dienst wordt verricht. Het Hof van Justitie van de Europese Unie (hierna: HvJ EU) heeft verduidelijkt dat het begrip "dienst van de informatiemaatschappij" onder omstandigheden ook gratis diensten kan omvatten, bijvoorbeeld als de gratis dienst wordt verleend om reclame te maken voor andere goederen of diensten.[4]

Het begrip "dienst van de informatiemaatschappij" wordt ook gebruikt in de richtlijn elektronische handel en in verschillende arresten heeft het HvJ EU zich uitgesproken over de vraag of de online-verkoop van producten en de online verkoop van niet langs elektronische weg verleende diensten, beschouwd moeten worden als een dienst van de informatiemaatschappij. Dat is volgens het HvJ EU het geval als de online-verkoop los gezien kan worden van de levering van het product of de dienst. Zo ja, dan is de online-verkoop of -bemiddeling te beschouwen als "dienst van de informatiemaatschappij" waar de richtlijn elektronische handel op van toepassing is. Zo nee, dan moet worden bepaald waar het zwaartepunt ligt; dat is bepalend voor welk recht op het onlosmakelijk verbonden geheel aan diensten van toepassing is. Dit moet van geval tot geval worden beoordeeld.

Zo kan volgens het HvJ EU de online-verkoop van contactlenzen los gezien worden van de verplichting tot het ondergaan van een voorafgaande medische oogtest. [5] Een online-bemiddelingsdienst voor taxivervoer is verder een onlosmakelijk onderdeel van een pakket aan diensten waarvan het hoofdbestanddeel taxivervoer is. De onlosmakelijkheid volgt uit het feit dat de chauffeurs zonder online bemiddelingsdienst geen taxivervoer kunnen verrichten en de doorslaggevende invloed die de aanbieder van de bemiddelingsdienst heeft op onder meer de prijs en kwaliteit van het taxivervoer. [6] Een online-bemiddelingsdienst voor toeristische woningverhuur, daarentegen, is niet onlosmakelijk verbonden met de toeristische woningverhuur zelf, want ook zonder deze bemiddelingsdienst kunnen de woningen worden verhuurd en de aanbieder van de bemiddelingsdienst heeft geen doorslaggevende invloed op de verhuur zelf. [7]

2.3.3 De begrippen "mere conduit", "caching" en "hosting"

Om te kwalificeren als "tussenhandeldienst", moet een dienst het karakter hebben van een "mere-conduit"-dienst, "caching"-dienst of "hosting"-dienst (artikel 3, onderdeel g, van de verordening). Uit overweging 29 bij de verordening kan worden afgeleid dat mere conduit- en cachingdiensten in zijn algemeenheid betrekking hebben op diensten die een efficiënte informatiedoorgifte op het internet mogelijk maken. Hostingdiensten, daarentegen, maken het online delen van informatie en inhoud mogelijk, waaronder het opslaan en delen van bestanden.

---

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

4 HvJ EU 11 september 2014, zaak C-291/13, ECLI:EU:C:2014:2209 (Papasavvas) en HvJ EU 15 september 2016, zaak C-484/14, ECLI:EU:C:2016:689 (McFadden/Sony Music).

5 HvJ EU 2 december 2010, zaak C-108/09, ECLI:EU:C:2010:725 (Ker Optika), r.o. 33-40.

6 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).

7 HvJ EU 19 december 2019, zaak C-390/18, ECLI:EU:C:2019:1112 (Airbnb Ireland).

Mere conduitdiensten bestaan uit de doorgifte in een communicatienetwerk van door een afnemer van de dienst verstrekte informatie, of uit het verstrekken van toegang tot een communicatienetwerk (artikel 3, onderdeel g, onder i, van de verordening). De dienst fungeert in dat geval slechts als doorgeefluik, zoals de term "mere conduit" impliceert. Het begrip "communicatienetwerk" wordt niet gedefinieerd in de verordening, maar aangenomen kan worden dat hierbij gebruik kan worden gemaakt van de definitie van het begrip "elektronischcommunicatienetwerk" in artikel 2, onderdeel 1, van het Europese wetboek voor elektronische communicatie.[8] Voorbeelden van mere conduitdiensten zijn internet service providers[9], internetknooppunten, draadloze lokale netwerken[10], virtuele particuliere netwerken en voice over IP-diensten (zie overweging 29 bij de verordening).

Cachingdiensten omvatten de doorgifte in een communicatienetwerk van door een afnemer van de dienst verstrekte informatie, waarbij die informatie automatisch, tussentijds en tijdelijk wordt opgeslagen met als enige doel om de latere doorgifte van die informatie aan andere afnemers van de dienst op hun verzoek doeltreffender te maken (artikel 3, onderdeel g, onder ii, van de verordening). Kenmerkend aan cachingdiensten is dat ze beogen om informatie die gebruikers opvragen sneller toegankelijk te maken en daartoe tijdelijk een kopie van die informatie opslaan. Dit vergroot de kwaliteit van dienstverlening voor gebruikers. Voorbeelden zijn inhoudsleveringsnetwerken ("content delivery netwerken") en bepaalde proxydiensten (zie overweging 29 bij de verordening).

Hosting-diensten bestaan uit de opslag van de door een afnemer van de dienst verstrekte informatie, op diens verzoek (artikel 3, onderdeel g, onder iii, van de verordening). Hieronder vallen bijvoorbeeld diensten als cloudcomputing, webhosting, zoekmachineadvertentiediensten[11], elektronische marktplaatsen[12], sociale netwerken[13], videodeelplatformen[14] en meer in zijn algemeenheid diensten die het online opslaan en delen van informatie mogelijk maken (zie overweging 29 bij de verordening).

2.3.4 Het begrip "aangeboden in de Unie"

Op grond van artikel 2, eerste lid, van de verordening is de verordening van toepassing op tussenhandeldiensten die worden aangeboden aan afnemers van de dienst die gevestigd zijn of zich bevinden in de Unie, ongeacht waar de aanbieders van die tussenhandeldiensten hun plaats van vestiging hebben. Belangrijk is dat het gaat om de *diensten*, niet om de aanbieder als zodanig. Als een aanbieder meerdere diensten aanbiedt, is het goed mogelijk dat sommige daarvan wel en andere niet onder de verordening vallen. Voor toepasselijkheid van de verordening is dus voldoende dat een aanbieder natuurlijke of rechtspersonen de mogelijkheid biedt om gebruik te maken van de diensten van een tussenhandeldienst in de Unie. Dit kan, mits aan de definities in artikel 3, onderdelen d en e, van de verordening is voldaan, ook een zogenaamde "reseller" zijn, zoals een wederverkoper van hostingdiensten.

---

[8] Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (PbEU 2018, L 321).
[9] HvJ EU 24 november 2011, zaak C-70/10, ECLI:EU:C:2011:771 (Scarlet/SABAM) en HvJ EU 27 maart 2014, zaak C-314/12, ECLI:EU:C:2014:192, (UPC Telekabel Wien).
[10] HvJ EU 15 september 2016, zaak C-484/14, ECLI:EU:C:2016:689 (McFadden/Sony Music).
[11] HvJ EU 23 maart 2010, zaak C-236/08, ECLI:EU:C:2010:159 (Google France).
[12] HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay).
[13] HvJ EU 16 februari 2012, zaak C-360/10, ECLI:EU:C:2012:85 (SABAM/Netlog) en HvJ EU 3 oktober 2019, zaak C-18/18, ECLI:EU:C:2019:821 (Glawischnig-Piesczek).
[14] HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando).

Artikel 3, onderdelen d en e, van de verordening en de overwegingen bij de verordening verduidelijken wanneer precies sprake is van het aanbieden van diensten in de Unie, namelijk wanneer de tussenhandeldienst in kwestie een "wezenlijke band" heeft met de Unie. Dat is tenminste het geval wanneer de dienstaanbieder een vestiging heeft in de Unie of, bij gebreke daarvan, indien het aantal afnemers in een of meer lidstaten in verhouding tot de totale bevolking groot is. Een dienst hoeft dus niet in de hele Unie afnemers te hebben om toch een wezenlijke band met de Unie te hebben. Er is ook al sprake van wanneer de dienst in tenminste één lidstaat een aantal afnemers heeft dat groot is in verhouding tot de totale bevolking van die lidstaat. Zo is het bijvoorbeeld mogelijk dat een dienst die wordt aangeboden door een aanbieder die is gevestigd in Brazilië, maar die tevens in Portugal wordt gebruikt door een relatief groot aantal gebruikers, een wezenlijke band met de Unie heeft, en dus onder de reikwijdte van de verordening valt.

Een wezenlijke band kan verder blijken uit het feit dat de aanbieder zijn activiteiten "richt" op één of meerdere lidstaten. Gerichtheid kan worden afgeleid uit verschillende feitelijke omstandigheden en daarvan lijkt al snel sprake. Overweging 8 noemt als voorbeeld het gebruik van de voor een lidstaat gebruikelijke taal of munteenheid of de mogelijkheid voor afnemers om in een lidstaat diensten af te nemen of goederen te bestellen. Maar ook het via een app store beschikbaar maken van een applicatie in specifiek één of meerdere lidstaten, plaatselijk adverteren, adverteren in de nationale taal of het verlenen van klantenservice-diensten in de gangbare taal van een lidstaat, kunnen uitwijzen dat een aanbieder zijn diensten op één of meerdere lidstaten richt en dus een wezenlijke band met de Unie opleveren. Het enkele feit dat een website toegankelijk is in een lidstaat, is echter onvoldoende om van een wezenlijke band met de Unie te spreken.

2.4 *Andere belangrijke begrippen in de verordening*

2.4.1 Inleiding

Zoals genoemd in paragraaf 2.1 van deze memorie van toelichting, heeft de verordening mede tot doel om de verspreiding van illegale online-inhoud en de maatschappelijke risico's van de verspreiding van desinformatie en andere inhoud tegen te gaan. Hoofdstuk II van de verordening heeft betrekking op de aansprakelijkheid van aanbieders voor de door hen opgeslagen of doorgegeven informatie en hoofdstuk III van de verordening bevat verschillende verplichtingen voor aanbieders over hoe zij dienen om te gaan met illegale inhoud die met toepassing van hun diensten is opgeslagen of verspreid. Een deel van die verplichtingen ziet ook op inhoud die in strijd is met de algemene voorwaarden van de aanbieder. De maatregelen die de aanbieders nemen als er sprake is van illegale inhoud of inhoud in strijd met de algemene voorwaarden worden in de verordening aangeduid als "inhoudsmoderatie". Hoewel de begrippen "illegale inhoud", "desinformatie of andere inhoud" en "inhoudsmoderatie" niet bepalend zijn voor de reikwijdte van de verordening, is hun betekenis wel van belang voor een goed begrip van de werking van de verordening. Hetzelfde geldt voor de begrippen "online platform" en "online zoekmachine". Om die reden worden deze begrippen in deze paragraaf nader toegelicht.

2.4.2 Het begrip "illegale inhoud"

Het begrip "illegale inhoud" is 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, ongeacht het precieze voorwerp of de precieze aard van dat recht. Uit deze definitie volgt dat de begrippen "inhoud" en "informatie", die beide in de verordening worden gebruikt, voor de toepassing van de verordening dezelfde betekenis hebben. De beoordeling of de informatie illegaal is, dient te geschieden aan de hand van het Unierecht en het recht van de lidstaten en dus niet aan de hand van

de verordening zelf. Het gaat voorts om strijd met het recht, dus het handelen in strijd met contractuele bepalingen valt niet onder de definitie van "illegale inhoud". Verder volgt uit de definitie geen beperking ten aanzien van het type recht waar het om zou kunnen gaan (geschreven of ongeschreven recht), de aard van het recht (publiekrecht of privaatrecht) of de bron van het recht (centrale of decentrale overheid, wetgever in formele zin of gedelegeerde wetgever). Het kan dus gaan om alle informatie die strafbaar is (in strafrechtelijke zin) of onrechtmatig (in civielrechtelijke zin).

Informatie kan op grond van de definitie van het begrip "illegale inhoud" op twee manieren in strijd zijn met het recht: "op zichzelf" of "in verband met een activiteit". Bij informatie die op zichzelf in strijd is met het recht kan gedacht worden aan uitings- en verspreidingsdelicten, zoals terroristische, kinderpornografische of discriminerende inhoud, of informatie waarvan openbaarmaking of verspreiding in strijd is met het recht vanwege de status van die informatie, zoals bij de openbaarmaking van bedrijfsgeheimen of inbreuken op intellectuele eigendomsrechten. Bij informatie die in verband met een activiteit in strijd is met het recht kan worden gedacht aan informatie waarbij het onrechtmatige of strafbare gedrag niet primair in de informatie zelf ligt besloten, maar in de wijze waarop deze wordt verspreid, zoals in het geval van valsheid in geschrifte, oplichting, de verkoop of verspreiding van namaakproducten of niet conforme producten, de illegale verkoop van levende dieren, online stalking en het gebruik van malware.

2.4.3 Het begrip "desinformatie of andere inhoud"

Het begrip "desinformatie of andere inhoud", waarover wordt gesproken in overweging 9 bij de verordening, worden niet gedefinieerd in de verordening en worden in de tekst van de verordening zelf ook niet gebruikt. Desalniettemin beoogt de verordening de maatschappelijke risico's van de verspreiding van dit type inhoud aan te pakken. Zo bevat de verordening verschillende bepalingen over inhoudsmoderatie door aanbieders van tussenhandeldiensten (zie paragraaf 2.4.4 van deze memorie van toelichting). 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. Verder beschrijft artikel 34 van de verordening een aantal typen schadelijke inhoud die een zogenaamd "systeemrisico" kunnen vormen (zie paragraaf 4.3.6.3 van deze memorie van toelichting), zoals inhoud die een negatief effect heeft of kan hebben op verkiezingsprocessen of de volksgezondheid. Hieronder valt ook desinformatie.

Daarnaast kunnen reclames op basis van profilering bepaalde maatschappelijke risico's met zich brengen, ook als de inhoud daarvan niet illegaal is. Zo kunnen targetingtechnieken bijdragen aan desinformatiecampagnes en negatieve gevolgen hebben voor hele groepen en maatschappelijke schade versterken, bijvoorbeeld door bepaalde groepen te discrimineren (zie overweging 69 bij de verordening). Daarom stelt de verordening regels vast met betrekking tot het tonen van reclames op basis van profilering (artikel 26 en artikel 28, tweede lid, van de verordening). Tevens kan bepaalde inhoud, hoewel niet illegaal, in het bijzonder schadelijk zijn voor minderjarigen. Daarom dienen aanbieders van online platforms passende maatregelen te nemen om de bescherming van minderjarigen te waarborgen (artikel 28, eerste lid, van de veroordeling) en zijn negatieve gevolgen voor minderjarigen een aandachtsgebied voor vrijwillige gedragscodes (overweging 104).

De regels voor dit soort – schadelijke – inhoud zijn echter wezenlijk anders dan die voor illegale inhoud. Zo valt schadelijke inhoud, anders dan illegale inhoud, bijvoorbeeld niet onder de kennisgevings- en actiemechanismen waarin de verordening voorziet (zie paragraaf 4.3.3.1 van deze memorie van toelichting). Ook de bepalingen over betrouwbare flaggers en misbruik (paragrafen

4.3.4.3 en 4.3.4.4 van deze memorie van toelichting) hebben enkel betrekking op illegale inhoud en niet op schadelijke inhoud.

2.4.4 Het begrip "inhoudsmoderatie"

"Inhoudsmoderatie" is blijkens de definitie in artikel 3, onderdeel t, van de verordening een breed begrip. Het gaat daarbij om al dan niet geautomatiseerd uitgevoerde activiteiten door aanbieders van tussenhandeldiensten die gericht zijn op het opsporen, identificeren en aanpakken van illegale inhoud of informatie die niet verenigbaar is met hun algemene voorwaarden. Het aanpakken van deze informatie omvat ook maatregelen die gevolgen hebben voor de beschikbaarheid, zichtbaarheid en toegankelijkheid van die informatie, zoals demotie, uitschakeling van toegang ertoe, of verwijdering ervan, en maatregelen gericht op het wegnemen of verminderen van financiële prikkels (demonetisatie). De maatregelen kunnen ook betrekking hebben op de mogelijkheid van afnemers om gebruik te maken van de dienst, zoals de beëindiging of de schorsing van een account van een afnemer.

2.4.5 Het begrip "online platform"

Een subcategorie van hostingdiensten wordt gevormd door online platforms. Kenmerkend voor online platforms is dat zij de opgeslagen informatie op verzoek van de afnemer verspreiden bij het publiek (artikel 3, onderdeel i, van de verordening). Het onderscheid tussen hostingdiensten en online platforms is niet relevant voor de aansprakelijkheidsbeperking neergelegd in artikel 6 van de verordening, die van toepassing is op alle hostingdiensten. Het onderscheid is wel van belang voor de vraag welke zorgvuldigheidsverplichtingen van toepassing zijn. Voor online platforms gelden uit hoofde van de verordening namelijk meer zorgvuldigheidsverplichtingen dan voor andere hostingdiensten.

Onder "verspreiding bij het publiek" wordt verstaan het op verzoek van de informatieverstrekkende afnemer beschikbaar stellen van informatie aan een mogelijk onbeperkt aantal derden (artikel 3, onderdeel k, bij de verordening). Bepalend is dus of de dienst het voor de afnemer mogelijk maakt om informatie beschikbaar te maken voor een in potentie onbeperkt aantal personen, zonder dat de afnemer daar verder iets voor hoeft te doen en ongeacht of die derden de informatie daadwerkelijk raadplegen (zie overweging 14 bij de verordening). De verspreiding onder het publiek moet wel gebeuren op rechtstreeks verzoek van de informatieverstrekkende afnemer van de dienst.

Van verspreiding onder het publiek is geen sprake indien voor toegang tot de informatie eerst registratie nodig is of toelating tot een afgebakende groep, tenzij registratie automatisch plaatsvindt. Dit laatste betekent dat er geen menselijke beslissing of selectie van wie toegang krijgt, mag plaatsvinden. Interpersoonlijke communicatiediensten, zoals gedefinieerd in artikel 1, onderdeel 5, van het Europese wetboek voor elektronische communicatie, waaronder e-mails of particuliere berichtendiensten, vallen niet onder de definitie van online platform, omdat zij worden gebruikt voor interpersoonlijke communicatie tussen een door de afzender bepaald eindig aantal personen. Diensten waarmee informatie ter beschikking wordt gesteld via openbare groepen of vrij toegankelijke kanalen kunnen daarentegen wel als online platform worden beschouwd.

Van een online platform is blijkens de definitie in onderdeel i van artikel 3 van de verordening geen sprake als het verspreiden van de informatie onder het publiek slechts een klein of louter bijkomstig kenmerk is van een andere dienst en om objectieve en technische redenen niet kan worden gebruikt zonder die andere dienst. In overweging 13 bij de verordening wordt als mogelijk voorbeeld genoemd het deel van een online krant dat bestemd is voor reacties, waarbij het duidelijk is dat dit bijkomstig is bij de hoofddienst die bestaat uit de publicatie van nieuws onder de redactionele

verantwoordelijkheid van een uitgever. Uit artikel 3, onderdeel i, van de verordening volgt verder dat de integratie van het kenmerk of de functionaliteit in de andere dienst geen manier mag zijn om de toepasbaarheid van de verordening te omzeilen. Hieruit volgt dat deze uitzondering strikt moet worden toegepast.

2.4.6 Het begrip "online zoekmachine"

Afdeling 5 van hoofdstuk III van de verordening bevat zorgvuldigheidsverplichtingen die mede van toepassing zijn op zeer grote online zoekmachines. Opgemerkt zij dat de categorie "zeer grote online zoekmachine" niet voorkwam in het oorspronkelijke Commissievoorstel voor de verordening. Deze uitbreiding van het materiële toepassingsbereik is tijdens het Europese wetgevingsproces toegevoegd. Gelet op de cruciale rol die zeer grote online zoekmachines spelen bij het lokaliseren en online oproepbaar maken van informatie (zie overweging 75 bij de verordening), werd besloten dat de verplichtingen uit afdeling 5 ook moeten gelden voor dergelijke diensten. Uit de definitie van online zoekmachine volgt dat zij een tussenhandeldienst zijn (artikel 3, onderdeel j, van de verordening), meer specifiek een tussenhandeldienst die gebruikers de mogelijkheid biedt zoekopdrachten in te voeren om zoekacties uit te voeren op in beginsel alle websites of alle websites in een bepaalde taal, op basis van een zoekopdracht over eender welk onderwerp in de vorm van een trefwoord, een gesproken verzoek, een frase of andere input, en die resultaten in eender welk formaat oplevert met informatie over de opgevraagde inhoud. Als tussenhandeldienst zullen online zoekmachines, inclusief de zeer grote, moeten voldoen aan de bepalingen die voor tussenhandeldiensten gelden, zoals de verplichtingen in afdeling 1 van hoofdstuk III van de verordening. Afhankelijk van de functionaliteiten van een specifieke online zoekmachine, kan een online zoekmachine tevens aan te merken zijn als mere conduit-, caching- of hostingdienst. In dat geval gelden ook de regels van de verordening voor het aanbieden van die categorie tussenhandeldiensten.

3 Aansprakelijkheid van aanbieders van tussenhandeldiensten

3.1 *Inleiding*

De artikelen 4, 5 en 6 van de verordening bevatten de voorwaardelijke vrijstellingen van aansprakelijkheid, die voorheen waren opgenomen in de artikelen 12, 13 en 14 van de richtlijn elektronische handel. Ook het verbod op het opleggen van een algemene verplichting tot monitoring (artikel 8 van de verordening) is ongewijzigd overgenomen uit artikel 15 van de richtlijn elektronische handel. De Uniewetgever heeft van de gelegenheid gebruik gemaakt om enkele bepalingen aan het aansprakelijkheidskader voor tussenpersonen toe te voegen. Deze bepaling hebben betrekking op vrijwillige onderzoeken naar illegale inhoud op eigen initiatief van de aanbieder (artikel 7 van de verordening) en op bevelen van bevoegde autoriteiten aan aanbieders om illegale informatie te verwijderen of om informatie over afnemers te verstrekken (artikelen 9 en 10 van de verordening). In dit hoofdstuk worden deze bepalingen toegelicht, evenals de bijbehorende jurisprudentie van het HvJ EU, voor zover die relevant blijft onder de verordening.

3.2 *Het kader voor aansprakelijkheid van tussenhandeldiensten voor door afnemers verstrekte informatie*

3.2.1 Inhoud verordening

3.2.1.1 Algemeen

Met het aansprakelijkheidskader voor aanbieders van tussenhandeldiensten heeft de Uniewetgever een evenwicht tot stand willen brengen tussen de verschillende betrokken belangen en

grondrechten, waaronder de vrijheid van ondernemerschap van de aanbieder van de tussenhandeldienst, de vrijheid van meningsuiting en informatie, de bescherming van persoonsgegevens en privacy van de gebruikers van de tussenhandeldienst en de bescherming van de rechten van derden, zoals hun (intellectuele) eigendomsrechten.[15]

Het aansprakelijkheidskader voor tussenpersonen harmoniseert de voorwaarden op grond waarvan deze aanbieders *niet* aansprakelijk zijn voor informatie van derden die zij opslaan of doorgeven. Deze voorwaardelijke vrijstellingen van aansprakelijkheid regelen alleen wanneer een aanbieder *niet* aansprakelijk is voor informatie die door de afnemers van de dienst wordt verstrekt. De artikelen vormen dus niet een positieve basis om vast te stellen wanneer een aanbieder *wel* aansprakelijk is. Wanneer een tussenhandeldienst geen aanspraak kan maken op één van de vrijstellingen, dan moet de vraag of hij in dat geval aansprakelijk is worden beantwoord aan de hand van het toepasselijke Unierecht of het nationale recht. De vrijstelling is horizontaal en geldt dus voor alle vormen van aansprakelijkheid: de civielrechtelijke aansprakelijkheid uit hoofde van een onrechtmatige daad, maar ook de strafrechtelijke of bestuursrechtelijke aansprakelijkheid van de tussenpersoon.

3.2.1.2 Voorwaarden voor aansprakelijkheidsvrijstelling

Op grond van de artikelen 4, 5 en 6 van de verordening zijn de aanbieders van mere conduit-, caching- en hostingdiensten onder voorwaarden vrijgesteld van aansprakelijkheid voor de informatie van derden die zij doorgeven of opslaan. De vrijstellingen van aansprakelijkheid laten de mogelijkheid onverlet dat dienstverleners in een concreet geval door een rechter of administratieve autoriteit kunnen worden bevolen om maatregelen te nemen om inbreuken te beëindigen of voorkomen. Deze bepalingen zijn ongewijzigd overgenomen uit de richtlijn elektronische handel. Hierna worden kort de voorwaarden per categorie aanbieder beschreven.

Mere conduitdiensten

De aanbieder van een mere conduit-dienst is niet aansprakelijk voor doorgegeven of geraadpleegde informatie, op voorwaarde dat de aanbieder de doorgifte niet initieert, de ontvanger van de doorgifte niet selecteert en de doorgegeven informatie niet selecteert of wijzigt (artikel 4, eerste lid, van de verordening). Technische handelingen die tijdens de doorgifte of toegang plaatsvinden ten behoeve van die doorgifte of toegang, zoals de omzetting van een optisch signaal in glasvezel naar een radiosignaal voor doorgifte via WiFi, moeten niet worden beschouwd als een wijziging van de informatie. Het tweede lid verduidelijkt dat de doorgifte en toegangsverschaffing bij mere conduitdiensten ook de automatische, tussentijdse en tijdelijke opslag van de doorgegeven informatie omvat, als die opslag uitsluitend dient voor dat doel en de informatie niet langer wordt bewaard dan redelijkerwijs noodzakelijk.

Cachingdiensten

De aanbieder van een caching-dienst is niet aansprakelijk voor de automatisch, tussentijds en tijdelijk opgeslagen informatie, als aan een aantal voorwaarden is voldaan (artikel 5, eerste lid, van de verordening). In de eerste plaats mag de aanbieder de informatie niet wijzigen. In de tweede plaats gelden er enkele voorwaarden die sterk samenhangen met de aard van de caching-dienst: de aanbieder moet de voorwaarden voor toegang tot de informatie in acht nemen, de alom erkende en in de sector gangbare regels betreffende de bijwerking van informatie naleven en niets wijzigen aan het alom erkende en in de sector gangbare rechtmatige gebruik van technologie voor het verkrijgen

[15] Zie overweging 41 bij de richtlijn, zoals onder meer uitgelegd in HvJ EU 15 september 2016, zaak C-484/14, ECLI:EU:C;2016:689 (McFadden/Sony Music), r.o. 68 en HvJ EU 3 oktober 2019, zaak C-18/18, ECLI:EU:C:2019:821 (Glawischnig-Piesczek), r.o. 43.

van gegevens over het gebruik van de informatie. Tot slot moet de aanbieder in twee gevallen prompt handelen om de opgeslagen informatie te verwijderen of de toegang ertoe onmogelijk te maken: als hij daadwerkelijk kennis heeft dat de informatie op de oorspronkelijke plek is verwijderd of dat de toegang tot die plek onmogelijk is gemaakt, of als hij door een gerechtelijke of administratieve autoriteit daartoe wordt gelast.

Hostingdiensten

Om een beroep te kunnen doen op de aansprakelijkheidsvrijstelling voor hostingdiensten mag de aanbieder niet daadwerkelijk kennis hebben van illegale activiteiten die hij mogelijk maakt met zijn dienstverlening of van illegale inhoud die zijn klanten bij hem opslaan (artikel 6, eerste lid, onderdeel a, van de verordening). Het HvJ EU heeft in zijn jurisprudentie over artikel 14 van de richtlijn elektronische handel verduidelijkt dat dit vereiste betrekking heeft op concrete onwettige activiteiten en informatie. Met andere woorden: het enkele feit dat een dienstverlener zich in het algemeen ervan bewust is dat zijn platform ook gebruikt kan worden om illegale content te delen en hij dus in abstracto kennis heeft van de illegale beschikbaarstelling van content, is onvoldoende om te oordelen dat aan deze bepaling niet is voldaan.[16] Het feit dat een aanbieder een geautomatiseerde indexering van de op zijn dienst geüploade informatie verricht, dat de dienst over een zoekfunctie beschikt of informatie aanbeveelt op basis van de profielen of voorkeuren van de afnemers van de dienst, is voorts niet voldoende om te veronderstellen dat de aanbieder "concrete" kennis heeft van op dat platform ontplooide illegale activiteiten of opgeslagen illegale inhoud.[17]

Als het een civielrechtelijke vordering tot schadevergoeding betreft, dan is de voorwaarde ruimer geformuleerd; het gaat dan om kennis van feiten of omstandigheden waaruit de illegale activiteit of de illegale inhoud duidelijk blijkt. Over dit laatste heeft het HvJ EU in een zaak over een elektronische marktplaats geoordeeld dat het moet gaan om kennis van feiten of omstandigheden op grond waarvan een behoedzame marktdeelnemer de onwettigheid van de betrokken informatie in kwestie had moeten vaststellen.[18]

Wanneer een aanbieder van hostingdiensten daadwerkelijke kennis van de illegale activiteit of illegale inhoud krijgt, dan moet hij prompt handelen om die inhoud te verwijderen of ontoegankelijk te maken (artikel 6, eerste lid, onderdeel b, van de verordening). Doet hij dat, dan is hij niet aansprakelijk. Als het verwijderen of ontoegankelijk maken geschiedt naar aanleiding van een kennisgeving van een derde, dan moet deze kennisgeving voldoende nauwkeurig en gemotiveerd zijn om een zorgvuldige marktdeelnemer in staat te stellen de illegale inhoud zonder grondig juridisch onderzoek redelijkerwijs te identificeren en te beoordelen.[19] De aansprakelijkheidsvrijstelling is tot slot niet van toepassing indien de afnemer van de dienst handelt op gezag of onder toezicht van de dienstaanbieder.

De verordening voorziet ten opzichte van de richtlijn inzake elektronische handel in een nieuwe uitzondering op de aansprakelijkheidsvrijstelling voor hostingdiensten voor online platforms die consumenten de mogelijkheid bieden om overeenkomsten op afstand met handelaren te sluiten, ook wel "*Business-to-Consumer*" (B2C) online marktplaatsen genoemd (artikel 6, derde lid, van de verordening). Als zulke aanbieders bij de gemiddelde consument de indruk wekken dat de informatie

[16] HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 111-113.
[17] Overweging 22. Vgl. HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 111-114.
[18] HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay).
[19] Vgl. HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 115-116.

of de aangeboden producten of diensten door henzelf – en dus niet door de betrokken handelaar – worden verstrekt, dan wel door handelaren die onder hun gezag of toezicht handelen, dan kunnen zij zich voor mogelijke aansprakelijkheid onder het consumentenrecht niet beroepen op de aansprakelijkheidsvrijstelling. Dit kan het geval zijn indien het online platform de identiteit van de handelaar niet duidelijk weergeeft of diens gegevens achterhoudt (zie in dit verband ook paragraaf 4.3.5 van deze memorie van toelichting), of indien hij producten of diensten in eigen naam in de handel brengt, zo blijkt uit overweging 24 bij de verordening. Voor de toepassing van artikel 6, derde lid, van de verordening is dus niet relevant of het online platform daadwerkelijk zelf de informatie, dienst of product verstrekt of daadwerkelijk een gezagsrelatie met de handelaar heeft, maar of een gemiddelde consument dat zou geloven.

3.2.1.3 Alleen vrijstelling als tussenpersoon neutraal optreedt

Het HvJ EU heeft in haar jurisprudentie over de richtlijn elektronische handel uitgemaakt dat een aanbieder van een mere-conduit-, caching- of hostingdienst enkel valt binnen de werkingssfeer van de aansprakelijkheidsvrijstelling voor deze diensten als hij geen actieve rol heeft ten aanzien van de informatie van zijn gebruikers die hij opslaat of doorgeeft.[20] Dit volgt volgens het HvJ EU uit de context en de doelstellingen van de aansprakelijkheidsvrijstelling. Voor toepassing van de vrijstelling is volgens het HvJ EU tevens essentieel dat de verlener van de dienst een "als tussenpersoon optredende dienstverlener" is in de zin die de Uniewetgever in afdeling 4 van hoofdstuk II van de richtlijn elektronische handel daaraan heeft willen geven.[21] Dat is niet het geval als de dienstverlener een actieve rol heeft waardoor hij kennis van of controle over de gegevens heeft 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.[22] Overweging 18 bij de verordening verwijst naar dit criterium.

Blijkens de rechtspraak van het HvJ EU moet de actieve rol betrekking hebben op de concrete onwettige informatie of gegevens die de dienstverlener voor zijn klanten opslaat, bijvoorbeeld doordat hij deze creëert, selecteert, bekijkt of controleert.[23] Niet iedere vorm van controle leidt dus tot een actieve rol en dus tot niet-toepasselijkheid van de aansprakelijkheidsvrijstelling. Zo beschikt de aanbieder van hostingdiensten over de technische mogelijkheden om informatie te verwijderen of de toegang ertoe onmogelijk te maken, bijvoorbeeld om informatie van servers te verwijderen of servers (tijdelijk) uit te schakelen. Dat is onvoldoende om van een "actieve rol" te spreken.

Recentelijk heeft het HvJ EU verduidelijkt dat als een dienstverlener vrijwillig technische maatregelen treft om illegale inhoud te detecteren, dat niet betekent dat die dienstverlener daardoor een actieve

---

[20] HvJ EU 23 maart 2010, zaak C-236/08, ECLI:EU:C:2010:159 (Google France), r.o. 120, HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay), r.o. 111, HvJ EU 7 augustus 2018, zaak C-521/17, ECLI:EU:C:2018:639 (SNB-REACT), r.o. 48, HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 106 en HvJ EU 26 april 2022, zaak C-401/19, ECLI:EU:C:2022:297 (Polen/Parlement en Raad), r.o. 28.

[21] HvJ EU 23 maart 2010, zaak C-236/08, ECLI:EU:C:2010:159 (Google France), r.o. 112, HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay), r.o. 112 en HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 105.

[22] HvJ EU 23 maart 2010, zaak C-236/08, ECLI:EU:C:2010:159 (Google France), r.o. 120, HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay), r.o. 113, 116, HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 106 en HvJ EU 26 april 2022, zaak C-401/19, ECLI:EU:C:2022:297 (Polen/Parlement en Raad), r.o. 120.

[23] HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay), r.o. 111, 112 en 118 en HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 109.

rol speelt waardoor hij kennis heeft van of controle heeft over de inhoud.[24] Het gevolg zou anders zijn, zo stelt het HvJ EU, dat aanbieders van diensten van de informatiemaatschappij die maatregelen treffen die juist bedoeld zijn om inbreuken tegen te gaan, zouden worden uitgesloten van de voorziene vrijstelling van aansprakelijkheid. In artikel 7 van de verordening heeft de Uniewetgever dit principe, ook wel de "Barmhartige Samaritaan"-bepaling genoemd, gecodificeerd. Deze nieuwe bepaling beoogt rechtszekerheid te creëren en daarmee een stimulans te geven aan vrijwillige activiteiten gericht op het tegengaan van illegale inhoud.[25]

Artikel 7 van de verordening verduidelijkt dat aanbieders van tussenhandeldiensten een beroep kunnen doen op de aansprakelijkheidsvrijstellingen in de artikelen 4, 5 en 6 van de verordening, ook in het geval zij te goeder trouw en zorgvuldig vrijwillige onderzoeken op eigen initiatief uitvoeren naar illegale inhoud, of andere maatregelen nemen die zijn gericht op het opsporen, identificeren en verwijderen van, of het uitschakelen van toegang tot, illegale inhoud. Op de maatregelen die volgen op dergelijke vrijwillige onderzoeken zijn wel de zorgvuldigheidsverplichtingen van hoofdstuk III van de verordening van toepassing. Zie hiervoor nader hoofdstuk 4 van deze memorie van toelichting. Ook het nemen van de nodige maatregelen ter naleving van het Unierecht of het nationale recht leidt niet tot uitsluiting van de aansprakelijkheidsvrijstellingen van de artikelen 4, 5 en 6 van de verordening. Dat geldt ook voor de zorgvuldigheidsverplichtingen die zijn opgenomen in hoofdstuk III van de verordening.

Overweging 20 verduidelijkt verder dat een aanbieder van een tussenhandeldienst die opzettelijk met een afnemer samenwerkt om illegale activiteiten te ontplooien geen neutrale dienst verricht en daarom niet in aanmerking komt voor de aansprakelijkheidsvrijstellingen. Dat is blijkens die overweging bijvoorbeeld het geval wanneer de aanbieder zijn dienst aanbiedt met als voornaamste doel om illegale activiteiten te faciliteren, bijvoorbeeld door daar uitdrukkelijk op te wijzen, daarvoor te adverteren of door gebruikers aan te sporen illegale activiteiten te verrichten. Het enkele feit dat een dienst versleutelde doorgifte of het afschermen van de identiteit van de afnemer mogelijk maakt, is volgens overweging 20 evenwel onvoldoende om te concluderen dat de dienst illegale activiteiten faciliteert.

De vraag of een aanbieder opzettelijk samenwerkt met een afnemer om illegale activiteiten te ontplooien, 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).[26] 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.

3.2.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel

[24] HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 109.
[25] De Commissie had eerder al soortgelijke uitspraken gedaan in niet-bindende documenten, zoals haar aanbeveling van 2018 over illegale inhoud online; Aanbeveling (EU) 2018/334 van de Commissie van 1 maart 2018 over maatregelen om illegale online-inhoud effectief te bestrijden, overweging 26.
[26] Zie onder meer Kamerstukken II, 2019/20, 26 643, nr. 696, blz. 5.

3.2.2.1 Civielrechtelijke aansprakelijkheid

In het met de Aanpassingswet richtlijn inzake elektronische handel[27] ingevoegde artikel 196c van Boek 6 van het BW zijn de aansprakelijkheidsvrijstelling voor aanbieders van mere conduit-, caching- en hostingdiensten en de bijbehorende voorwaarden uit de richtlijn één-op-één overgenomen. Het gevolg daarvan is dat de aanbieders van deze diensten niet aansprakelijk zijn op grond van onrechtmatige daad overeenkomstig artikel 162 van Boek 6 van het BW, indien zij aan de gestelde voorwaarden voldoen. Onder de digitaledienstenverordening werkt de aansprakelijkheidsvrijstelling voor aanbieders van mere conduit-, caching- en hostingdiensten met bijbehorende voorwaarden rechtstreeks door in de Nederlandse rechtsorde. Het is dus niet nodig om artikel 196c van Boek 6 van het BW te handhaven. Artikel 5.4 van onderhavig wetsvoorstel voorziet daarom in het vervallen van dit artikel. Deze wijziging heeft geen rechtsgevolgen.

3.2.2.2 Strafrechtelijke aansprakelijkheid

In artikel 54a van het Wetboek van Strafrecht (Sr) is gevolg gegeven aan de voorwaardelijke aansprakelijkheidsvrijstelling uit de richtlijn elektronische handel door middel van een vervolgingsuitsluitingsgrond. Op grond van dat artikel wordt een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens afkomstig van een derde, niet strafrechtelijk vervolgd als hij voldoet aan een bevel van de officier van justitie om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken. De ratio van deze regeling is de bescherming van de vrijheid van meningsuiting, door te voorkomen dat de aanbieder zich genoodzaakt voelt tot preventieve censuur teneinde strafrechtelijke aansprakelijkheid te voorkomen. De regeling dient een onbelemmerde informatie-uitwisseling; een grondbeginsel van de democratische rechtsstaat.[28]

Ter uitvoering van de artikelen 4 tot en met 6 van de verordening wordt artikel 54a Sr gehandhaafd. In artikel 54a Sr is een vervolgingsuitsluitingsgrond opgenomen voor de tussenpersoon die een communicatiedienst verleent bestaande uit een of meer van in de verordening onderscheiden activiteiten, te weten mere conduit, caching en hosting. Die activiteiten worden door de zinsne de "doorgifte of opslag van gegevens die van een ander afkomstig zijn" gevangen. Indien een strafbaar feit wordt begaan met gebruikmaking van een communicatiedienst, is strafrechtelijke vervolging van de tussenpersoon als zodanig uitgesloten indien hij voldoet aan een bevel als bedoeld in artikel 125p van het Wetboek van Strafvordering (Sv) of een beslissing als bedoeld in artikel 3, eerste lid, van verordening 2021/784.[29]

In artikel 125p Sv is neergelegd het bevel tot het ontoegankelijk maken van gegevens ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. Artikel 3, eerste lid, van verordening 2021/784 ziet op het verwijderingsbevel van terroristische online-inhoud.

De vervolgingsuitsluitingsgrond is zoals gezegd ingevoerd bij de Aanpassingswet richtlijn inzake elektronische handel. Aanvankelijk was in artikel 125p Sv zowel de vervolgingsuitsluitingsgrond als het bevel tot het ontoegankelijk maken van gegevens neergelegd. Bij invoering van de Wet computercriminaliteit III is het bevel tot het ontoegankelijk maken van gegevens overgeheveld naar het Sv als zelfstandige bevoegdheid.[30] Bij de Uitvoeringswet verordening terroristische online-inhoud

---

[27] Stb. 2004, 210.
[28] Kamerstukken II, 2001/02, 28197, nr. 3, blz. 63.
[29] Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud (PbEU 2021, L 172).
[30] Stb. 2018, 322.

is het verwijderingsbevel van terroristische online-inhoud toegevoegd aan de bepaling over de vervolgingsuitsluitingsgrond.[31]

Met de inwerkingtreding van de digitaledienstenverordening is artikel 54a Sr niet langer gebaseerd op de artikelen 12 tot en met 14 van de richtlijn elektronische handel maar op de artikelen 4 tot en met 6 van de verordening. Anders dan een richtlijn is een verordening rechtstreeks toepasselijk. Desalniettemin wordt het noodzakelijk geacht artikel 54a Sr te handhaven. In de artikelen 4 tot en met 6 van de verordening is bepaald dat een tussenpersoon in bepaalde gevallen niet-aansprakelijk is. Hoe zulks doorwerkt in het strafrecht, dat niet op het niveau van de EU is geharmoniseerd, volgt evenwel niet uit de verordening. Aldus is uitvoeringsregelgeving nodig om de bij de verordening bepaalde gevallen van niet-aansprakelijkheid te plaatsen in het strafrecht. Artikel 54a Sr zal deze functie (blijven) vervullen.

De vervolgingsuitsluitingsgrond moet worden uitgelegd in het licht van de artikelen 4 tot en met 6 van de verordening. In de verordening zijn voorwaarden gesteld aan de niet-aansprakelijkheid van de tussenpersoon. Zo stelt artikel 6, eerste lid, onderdeel b, van de verordening als voorwaarde dat de aanbieder van hostingdiensten prompt handelt om de illegale inhoud te verwijderen of de toegang daartoe onmogelijk te maken zodra hij dergelijke kennis of dergelijk besef krijgt. Deze en andere voorwaarden uit de verordening worden gevangen door de afbakening van de vervolgingsuitsluitingsgrond tot de tussenpersoon als zodanig. In de memorie van toelichting bij de Aanpassingswet richtlijn inzake elektronische handel is stilgestaan bij deze term.[32]

In de rechtspraak is recent de vraag aan de orde geweest of aan een tussenpersoon die wordt vervolgd voor medeplichtigheid een bevel dient te zijn gegeven tot het ontoegankelijk maken van gegevens. Het Hof Den Haag beantwoordde deze vraag ontkennend.[33] Indien een tussenpersoon kennis heeft van strafbaar handelen van een klant en dat handelen vervolgens blijft toestaan of adviezen geeft omtrent dat strafbaar handelen, staat de afwezigheid van een bevel niet aan vervolging in de weg. De regering sluit zich als medewetgever aan bij deze uitleg, die aansluit bij de jurisprudentie van het HvJ EU waarin wordt bepaald dat enkel neutraal handelende tussenpersonen onder de reikwijdte van de aansprakelijkheidsvrijstellingen voor aanbieders van tussenhandeldiensten vallen. Zie hiervoor nader paragraaf 3.2.1.3 van deze memorie van toelichting.

3.2.2.3 Bestuursrechtelijke aansprakelijkheid

Bij de implementatie van de richtlijn elektronische handel door middel van de Aanpassingswet richtlijn inzake elektronische handel werd het niet nodig geacht om de aansprakelijkheidsvrijstellingen te implementeren in het bestuursrecht, omdat het op grond van het bestuursrecht niet mogelijk was om een tussenpersoon aansprakelijk te stellen voor zijn bijdrage aan het ontsluiten van onwettige informatie en het bestuursrecht geen algemene aansprakelijkheidsregeling kent.[34] Hoofdstuk 5 van de Awb inzake bestuurlijke handhaving stamt van na de inwerkingtreding van de Aanpassingswet richtlijn inzake elektronische handel[35], dus het vraagstuk van bestuursrechtelijke aansprakelijkheid van tussenpersonen voor hun bijdrage aan het ontsluiten van onwettige informatie moet nu worden bezien in het licht van de definities van de begrippen “overtreding” en “overtreder” in artikel 5:1 van de Awb. Op basis van die definities en afhankelijk van de formulering van het wettelijk voorschrift dat overtreden wordt, is niet uit te

[31] Stb. 2023, 122.
[32] Kamerstukken II, 2001/02, 28197, nr. 3, p. 64-65.
[33] Hof Den Haag 23 augustus 2022, ECLI:NL:GHDHA:2022:1550.
[34] Kamerstukken II, 2001/02, 28197, nr. 3, p. 25.
[35] De vierde tranche van de Awb is in werking getreden op 1 juli 2009.

sluiten dat een tussenpersoon bestuursrechtelijk gesanctioneerd kan worden voor zijn bijdrage aan het ontsluiten van onwettige informatie. In die gevallen zijn de aansprakelijkheidsvrijstellingen uit de verordening van toepassing. Onder de verordening werken de aansprakelijkheidsvrijstellingen met bijbehorende voorwaarden rechtstreeks door in de Nederlandse rechtsorde, dus is het – net als het geval is bij het civiele recht – niet nodig om te voorzien in omzetting van deze bepalingen in het nationale bestuursrecht.

3.3 *Verbod op algemene verplichting tot monitoring of actief feitenonderzoek*

3.3.1 Inhoud verordening

De ruimte om maatregelen op te leggen aan dienstverleners om onwettige inhoud of activiteiten op te sporen wordt beperkt door artikel 8 van de verordening, dat bepaalt dat aan dienstverleners geen verplichting wordt opgelegd tot monitoring van de door hen opgegeven of opgeslagen informatie of tot actief onderzoek naar feiten of omstandigheden die duiden op illegale activiteiten. Deze bepaling is gelijk aan artikel 15, eerste lid, van de richtlijn elektronische handel.

Volgens het HvJ EU volgt uit deze bepaling onder meer 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.[36] Ook heeft het HvJ EU geoordeeld dat een internetprovider niet kan worden verplicht om een filtersysteem in te voeren voor alle elektronische communicatie via zijn diensten, dat zonder onderscheid op al zijn klanten wordt toegepast, dat preventief werkt, dat uitsluitend door hem wordt bekostigd en dat geen beperking in de tijd kent.[37] Tegelijkertijd heeft het HvJ EU bevestigd dat het verbod op algemeen toezicht niet geldt voor toezichtverplichtingen "in speciale gevallen", zoals bleek uit overweging 47 bij de richtlijn elektronische handel. Een dergelijk special geval kan onder meer zijn oorsprong vinden in specifieke 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. Hetzelfde geldt voor informatie die inhoudelijk overeenstemt met eerder onwettig verklaarde informatie, op voorwaarde dat het toezicht op en het onderzoek van de informatie waarop een dergelijk bevel betrekking heeft, beperkt blijft tot de specifiek in het bevel genoemde gegevens, en dat de verschillen tussen de formulering van die overeenstemmende inhoud en de formulering van de eerder onwettig verklaarde inhoud niet van dien aard zijn dat de betrokken hostingprovider verplicht is die inhoud autonoom te beoordelen.[38]

3.3.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel

Deze bepaling uit de verordening heeft rechtstreekse werking en behoeft geen uitvoeringsregels in het nationale recht.

3.4 *Eisen aan bevelen om op te treden tegen illegale inhoud of om informatie te verstrekken*

3.4.1 Inhoud verordening

[36] HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay), r.o. 139-142.
[37] HvJ EU 24 november 2011, zaak C-70/10, ECLI:EU:C:2011:771 (Scarlet/SABAM), r.o. 47-52 en HvJ EU 16 februari 2012, zaak C-360/10, ECLI:EU:C:2012:85 (SABAM/Netlog).
[38] HvJ EU 3 oktober 2019, zaak C-18/18, ECLI:EU:C:2019:821 (Glawischnig-Piesczek).

De artikelen 9 en 10 van de verordening bevatten regels over de bevelen die nationale gerechtelijke of bestuursrechtelijke autoriteiten aan aanbieders van tussenhandeldiensten kunnen richten ten aanzien van het bestrijden van illegale inhoud of het verstrekken van informatie over afnemers van de diensten. De twee artikelen schrijven een aantal minimumeisen voor over de inhoud van dergelijke bevelen en de opvolging ervan, zodat zulke bevelen op een efficiënte en doeltreffende manier kunnen worden uitgevoerd, met name ook in een grensoverschrijdende context. De artikelen 9 en 10 van de verordening vormen geen zelfstandige rechtsgrondslag voor het uitvaardigen van bevelen. Die rechtsgrondslag moet elders in het Unierecht of het nationale recht zijn voorzien. Uit deze regels vloeien derhalve ook geen nieuwe bevoegdheden voort voor gerechtelijke of administratieve autoriteiten voor het uitvaardigen van bevelen. De bestaande rechtspraak van het HvJ EU over de bevelen die aan tussenpersonen kunnen worden opgelegd blijft ook onder de verordening relevant.[39] Overweging 38 van de verordening verduidelijkt dat het uitvaardigen van dergelijke bevelen niet valt onder de reikwijdte van het zogenoemde land-van-oorsprongbeginsel (artikel 3 van de richtlijn elektronische handel). De bevoegde autoriteiten van alle lidstaten kunnen daarom in principe zulke bevelen uitvaardigen, ongeacht of de dienstaanbieder in die lidstaat is gevestigd of elders.

Het tweede lid van de artikelen 9 en 10 van de verordening bevat de minimumeisen waar de bevelen aan moeten voldoen. Op grond van de artikelen 9, tweede lid, onderdeel a, en 10, tweede lid, onderdeel a, van de verordening dienen de bevelen in elk geval de volgende elementen te bevatten: de rechtsgrondslag van het bevel, informatie over de uitvaardigende autoriteit en de autoriteit aan wie informatie over het nakomen van het bevel moet worden verstrekt, informatie om de illegale informatie of afnemer waar het bevel betrekking op heeft te kunnen identificeren, een motivering voor het bevel en de beschikbare verhaalmechanismen. Het bevel dient voorts te worden uitgevaardigd in de taal waarvan de dienstaanbieder krachtens artikel 11, derde lid, van de verordening heeft aangegeven dat die kan worden gebruikt om met hem te communiceren (de artikelen 9, tweede lid, onderdeel c, en 10, tweede lid, onderdeel c, van de verordening).

Op grond van artikel 9, tweede lid, onderdeel b, van de verordening moet het territoriale toepassingsgebied van het bevel beperkt zijn tot wat strikt noodzakelijk is om de doelstelling ervan te verzekeren. Dit moet blijkens deze bepaling gebeuren op basis van de toepasselijke regels van het Unierecht en het nationale recht, met inbegrip van het Handvest, en de algemene beginselen van internationaal recht. Blijkens overweging 36 bij de verordening moeten in een grensoverschrijdende situatie de gevolgen van het bevel in principe beperkt blijven tot het grondgebied van de uitvaardigende lidstaat, tenzij de illegaliteit van de inhoud rechtstreeks voortvloeit uit het Unierecht of indien de uitvaardigende autoriteit van mening is dat de betrokken rechten een ruimere territoriale reikwijdte behoeven, overeenkomstig het Unierecht en het internationale recht, rekening houdend met de internationale hoffelijkheid. Deze overweging sluit aan bij de jurisprudentie van het HvJ EU, waarin het Hof bepaalde dat de richtlijn elektronische handel er niet aan in de weg staat dat rechterlijke bevelen wereldwijd gevolgen sorteren, binnen de grenzen van het relevante internationale recht.[40]

De overige leden van de artikelen 9 en 10 van de verordening bevatten de minimumeisen over de opvolging van dergelijke bevelen. In het eerste lid van beide artikelen is bepaald dat de aanbieder

[39] HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay), HvJ EU 24 november 2011, zaak C-70/10, ECLI:EU:C:2011:771 (Scarlet/SABAM), HvJ EU 16 februari 2012, zaak C-360/10, ECLI:EU:C:2012:85 (SABAM/Netlog), HvJ EU 27 maart 2014, zaak C-314/12, ECLI:EU:C:2014:192, (UPC Telekabel Wien) en HvJ EU 3 oktober 2019, zaak C-18/18, ECLI:EU:C:2019:821 (Glawischnig-Piesczek).
[40] HvJ EU 3 oktober 2019, zaak C-18/18, ECLI:EU:C:2019:821 (Glawischnig-Piesczek), r.o. 50-52.

aan wie een bevel is gericht, de autoriteit die het bevel uitvaardigt onverwijld in kennis dient te stellen van de ontvangst van het bevel en het gevolg dat de aanbieder aan het bevel geeft. Dit laatste kan ook betekenen dat de aanbieder kennisgeeft van het feit dat hij geen gevolg geeft aan het bevel of dat pas op een later moment zal doen. Uit deze leden volgt dus geen verplichting om een dergelijk bevel op te volgen; het is aan het toepasselijke nationale recht of Unierecht om daarin te voorzien en te voorzien in handhaving in het geval een dergelijke verplichting niet wordt nagekomen (zie ook overweging 32 bij de verordening). Het niet voldoen aan de plicht om een kennisgeving te doen en de handhaving van de niet-naleving daarvan, valt daarentegen wel onder de reikwijdte van de verordening.

Op grond van artikel 9 en 10, derde lid, van de verordening dient de beveluitvaardigende autoriteit het bevel samen met de van de aanbieder van tussenhandeldiensten ontvangen informatie over het aan het bevel gegeven gevolg, door te zenden aan de digitaledienstencoördinator van de lidstaat van de uitvaardigende autoriteit. De digitaledienstencoördinator moet het bevel op grond van het vierde lid van beide artikelen doorzenden naar alle andere digitaledienstencoördinatoren. Het vijfde lid van de artikelen 9 en 10 van de verordening schrijft verder voor dat aanbieders van tussenhandeldiensten de afnemer van de betrokken dienst in kenn is moeten stellen van het ontvangen bevel en het daaraan gegeven gevolg. Ook moeten afnemers op de hoogte worden gesteld van een motivering en de bestaande verhaalmogelijkheden. Deze informatie moet uiterlijk worden verstrekt op het tijdstip waarop gevolg is gegeven aan het bevel of, in voorkomend geval, op het door de uitvaardigende autoriteit in haar bevel bepaalde tijdstip.

In het op een bevel toepasselijke Unierecht of nationale recht kan worden voorzien in aanvullende eisen (zie ook overweging 32 bij de verordening). Het zesde lid van de artikelen 9 en 10 van de verordening bepaalt in dat licht dat de voorwaarden en vereisten van deze artikelen geen afbreuk doen aan het nationale burgerlijk recht en strafprocesrecht. In overweging 34 bij de verordening wordt verduidelijkt dat als dat recht voorziet in voorwaarden die onverenigbaar zijn met de artikelen 9 en 10 van de verordening, de voorwaarden uit de verordening buiten toepassing kunnen worden gelaten of worden aangepast. Als voorbeeld wordt genoemd het achterwege laten van het zenden van kopieën van bevelen aan de digitaledienstencoördinatoren van andere lidstaten in de context van strafprocedures. Ook kan de verplichting dat een bevel een motivering moet bevatten van de illegaliteit van de betreffende inhoud, worden aangepast als dat nodig is met het oog op de voorkoming, opsporing en vervolging van strafbare feiten. Tot slot wordt de mogelijkheid genoemd van het uitstellen van het in kennis stellen van de afnemer van de dienst van de tenuitvoerlegging van een bevel, overeenkomstig het toepasselijke nationale of Unierecht.

3.4.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel

3.4.2.1 Uitvoering in het civielrecht

De bevelen waar de artikelen 9 en 10 van de verordening betrekking op hebben, zijn in het civiele recht rechtsvorderingen in de zin van artikel 296 van boek 3 van het BW. De veroordeling tot uitvoering van hetgeen gevorderd is, gebeurt in het dictum van de uitspraak van de civiele rechter in het geding waarin de rechtsvordering is ingesteld door de gerechtigde. Het BW en het Wetboek van Burgerlijke Rechtsvordering (Rv) bevatten verder geen specifieke inhoudelijke of procedurele eisen aan een dergelijke rechtsvordering. De artikelen 9 en 10 van de verordening werken rechtstreeks, dus de civiele rechter is van rechtswege gehouden om bij het opstellen van een uitspraak, waarin een bevel als bedoeld in de artikelen 9 en 10 van de verordening wordt gegeven, rekening te houden met de minimumeisen van het tweede lid van die artikelen. In de praktijk voldoen de rechterlijke uitspraken, waar deze eisen relevant voor zijn, al aan deze eisen. De gevolgen van de verordening op

dit punt zijn dan ook beperkt. De eisen aan de taal waarin de bevelen worden gesteld in de artikelen 9, tweede lid, onderdeel c, en 10, tweede lid, onderdeel c, van de verordening sluiten aan bij het bepaalde daarover in artikel 56 van het Rv.

Op grond van het derde lid van de artikelen 9 en 10 van de verordening moet de civiele rechter een afschrift van het bevel aan de digitaledienstencoördinator sturen. In de praktijk zal de civiele rechter dus een kopie van de uitspraak aan de ACM moeten verzenden. In het voorgestelde nieuwe negende lid van artikel 28 van het Rv wordt de griffier aangewezen als degene die de afschriften van de betreffende vonnissen, arresten en beschikkingen verstrekt (artikel 5.6 van het wetsvoorstel). De verstrekking van afschriften door gerechten die onder de Raad voor de rechtspraak ressorteren, geschiedt door tussenkomst van de Raad voor de rechtspraak. De griffier van de Hoge Raad voorziet in verstrekking van afschriften van arresten en beschikkingen van de Hoge Raad zonder de tussenkomst van de Raad voor de rechtspraak. Voorts wordt erin voorzien dat ter bescherming van zwaarwegende belangen van anderen, waaronder die van partijen, de griffier kan volstaan met de verstrekking van een geanonimiseerd afschrift van het vonnis, het arrest of de beschikking. Het zesde lid van de artikelen 9 en 10 van de verordening maakt het tot slot mogelijk om voorwaarden uit de verordening buiten toepassing te laten of aan te passen, met name als het strafvorderlijke belang dat vereist. Dat is in de civielrechtelijke context niet aan de orde.

3.4.2.2 Uitvoering in het strafrecht

In het strafrecht is het bevel van artikel 9 van de verordening, het bevel om op te treden tegen illegale inhoud, neergelegd in artikel 125p Sv. Het bevel van artikel 10 van de verordening, het bevel om informatie te verstrekken, is neergelegd in de artikelen 126n/u/zh Sv en de artikelen 126ng/ug/zl Sv.

De vereisten en voorwaarden van artikelen 9 en 10 van de verordening doen volgens het zesde lid geen afbreuk aan het nationaal strafprocesrecht. Tegen de achtergrond van overweging 34 van de verordening houdt dit in dat deze voorwaarden en vereisten in zoverre buiten toepassing kunnen worden gelaten. Deze hiërarchiebepaling heeft met name gevolgen voor de uitvoering van artikel 9 respectievelijk 10, derde tot en met het vijfde lid, van de verordening. Het belang van de opsporing en vervolging kan ertoe nopen dat de officier van justitie in een concreet geval de doorzending van een afschrift van het bevel aan de digitaledienstencoördinator uitstelt (derde lid) of bepaalt dat het afschrift nog niet wordt doorgezonden aan alle andere digitaledienstencoördinator (vierde lid). Zulks geldt gelijkerwijs voor het in kennisstellen van de afnemer van de betrokken dienst (vijfde lid). Ten aanzien van de vormvoorschriften en minimumeisen van het tweede lid geldt dat deze reeds volgen uit artikel 125p Sv of in de strafrechtspraktijk reeds worden uitgevoerd.

3.4.2.3 Uitvoering in het bestuursrecht

De artikelen 9 en 10 van de verordening werken rechtstreeks, dus het bestuursorgaan dat, of de toezichthoudende ambtenaar die, een dergelijk bevel verstrekt is van rechtswege gehouden rekening te houden met de minimumeisen van het tweede lid, onderdelen a en b, van die artikelen. Het bevel om op te treden tegen illegale inhoud (artikel 9 van de verordening) moet zijn grondslag vinden in sectorale wetgeving, de Awb bevat daar geen algemene grondslag voor.[41] Het bevel om informatie over afnemers te verstrekken (artikel 10 van de verordening) is, als het wordt gedaan in het kader van het toezicht op en handhaving van sectorale wetgeving, te beschouwen als een vordering tot inlichtingen (artikel 5:16 van de Awb) of een vordering tot inzage van zakelijke gegevens en bescheiden (artikel 5:17 van de Awb). De Awb laat open of dergelijke vorderingen mondeling dan wel

[41] Zie bijvoorbeeld artikel 33a, onderdeel b, van de Huisvestingswet 2014.

schriftelijk worden gegeven. Om aan de minimumeisen van artikel 10 van de verordening te voldoen, ligt het in de rede dat de vordering op schrift wordt gesteld. Het gevolg dat de Awb daaraan verbindt, is dat de vordering het karakter heeft van een besluit in de zin van artikel 1:3, eerste lid, van de Awb. Voor het overige hebben deze in de verordening genoemde minimumeisen geen gevolgen voor de bestuursrechtelijke praktijk.

De eisen aan de taal waarin de bevelen worden gesteld in de artikelen 9, tweede lid, onderdeel c, en 10, tweede lid, onderdeel c, van de verordening zijn te beschouwen als wettelijk voorschrift als bedoeld in artikel 2:6 van de Awb, waarmee in voorkomend geval kan worden afgeweken van de eis dat bestuursorganen de Nederlandse taal gebruiken. Het bestuursorgaan en de toezichthoudende ambtenaar moeten bevelen onverwijld aan de ACM sturen, op grond van het derde lid van artikel 9 van de verordening. Deze bepaling werkt rechtstreeks en behoeft geen nadere regeling in dit wetsvoorstel. Het zesde lid maakt het tot slot mogelijk om voorwaarden uit de verordening buiten toepassing te laten of aan te passen, met name als het strafvorderlijke belang dat vereist. Dat is in de bestuursrechtelijke context niet aan de orde.

4 Zorgvuldigheidsverplichtingen voor aanbieders van tussenhandeldiensten

4.1 *Inleiding*

Hoofdstuk III van de verordening bevat zorgvuldigheidsverplichtingen voor aanbieders van tussenhandeldiensten, die – blijkens de titel van het hoofdstuk – dienen bij te dragen aan een transparante en veilige online omgeving. Blijkens overweging 2 is de aanleiding om deze zorgvuldigheidseisen te harmoniseren gelegen in het feit dat lidstaten in toenemende mate nationale wetten hebben ingevoerd, of overwogen hebben dat te doen, met specifieke zorgvuldigheidseisen voor aanbieders van tussenhandeldiensten. Dergelijke uiteenlopende nationale wetten hadden een negatieve invloed op de interne markt, met name het vrije verkeer van goederen en diensten en de vrijheid van vestiging, mede in het licht van het grensoverschrijdende karakter van het internet.

In paragraaf 4.2 van dit hoofdstuk wordt eerst kort beschreven welke zorgvuldigheidsverplichtingen er golden vóór de totstandkoming van de verordening. In paragraaf 4.3 worden de verschillende zorgvuldigheidsverplichtingen uit de verordening kort toegelicht. Zoals opgemerkt in paragraaf 1.4 van deze memorie van toelichting, behoeven deze zorgvuldigheidsverplichtingen op zichzelf geen uitwerking in nationale wetgeving. Dat geldt wel voor de uitvoerings-, toezichts- en handhavingstaken die in verband met deze zorgvuldigheidsverplichtingen aan nationale bevoegde autoriteiten worden opgedragen in de verordening. De uitvoering van deze taken en de daarvoor benodigde uitvoeringsbepalingen in het wetsvoorstel worden toegelicht in hoofdstukken 5 en 6 van deze memorie van toelichting.

4.2 *Situatie onder de richtlijn elektronische handel*

4.2.1 Het kader onder de richtlijn elektronische handel

De richtlijn elektronische handel bevatte geen verplichtingen voor tussenpersonen ten aanzien van de omgang met inhoud die met gebruikmaking van hun diensten werd opgeslagen of verspreid. Dat betekent niet dat de Uniewetgever geen aandacht had voor dergelijke verplichtingen, die op drie manieren vorm konden krijgen: in nationale wetgeving, in sectorale Uniewetgeving of in de vorm van vrijwillige overeenkomsten tussen alle betrokken partijen, zoals gedragscodes. Hierna wordt elk van deze vormen kort besproken.

4.2.2 Zorgvuldigheidsverplichtingen in het nationale recht

Blijkens overweging 48 van de richtlijn elektronische handel laat die richtlijn de mogelijkheid onverlet voor lidstaten om in hun nationale wetgeving zorgvuldigheidsverplichtingen op te leggen aan dienstverleners die door afnemers van hun dienst verstrekte informatie toegankelijk maken. In het Nederlandse recht bestaan geen in wetgeving neergelegde specifiek aan tussenpersonen gerichte zorgvuldigheidsverplichtingen. Wel volgt uit de maatschappelijke zorgvuldigheidsnorm (artikel 6:162 van het BW) dat van een tussenpersoon verlangd kan worden dat hij redelijkerwijs maatregelen neemt om het ontstaan of voortbestaan van schade van derden te voorkomen. In de contractuele relatie tussen de tussenpersoon en zijn gebruiker dient de tussenpersoon zich verder te gedragen overeenkomstig de redelijkheid en billijkheid (artikel 6:2 van het BW) en, indien de contractuele relatie tussen de tussenpersoon en zijn gebruiker te beschouwen is als overeenkomst van opdracht, moet de tussenpersoon de zorg van een goed opdrachtnemer in acht nemen (artikel 7:401 van het BW).

Handhaving van deze zorgvuldigheidsnormen vindt civielrechtelijk plaats. De mogelijkheid om dit soort verplichtingen in het concrete geval op te leggen wordt begrensd door wat er in redelijkheid van de tussenpersoon kan worden verwacht en het verbod op het opleggen van een algemene plicht tot monitoring van informatie (zie nader paragraaf 3.3 van deze memorie van toelichting). Zo heeft het Hof Leeuwarden in het geval van een hostingdienst (een online marktplaats) verduidelijkt dat een host doorgaans geen onzorgvuldig handelen zal kunnen worden tegengeworpen indien hij voldoet aan de voorwaarden die gelden om voor de hosting vrijwaring in aanmerking te komen. Geheel uitgesloten is dit echter niet. Onder bijzondere omstandigheden zal, gelet op de concrete belangen, wellicht toch onzorgvuldig handelen kunnen worden aangenomen waardoor in dat geval – ook al zal schadevergoeding vanwege de vrijwaring niet mogelijk zijn – op de voet van artikel 3:296 BW een verbod of bevel kan worden gegeven. In het geval echter dat aan de voorwaarden voor vrijwaring is voldaan en daarnaast de van de host gevergde verplichting onevenredig is, zal het nalaten van de host om aan die verplichting te voldoen niet als strijdig met de zorgvuldigheidsnorm kunnen worden beschouwd – een host is niet gehouden tot voor hem onevenredig nadelige maatregelen – zodat in dat geval naar Nederlands recht ook geen verbod of bevel kan worden opgelegd.[42]

4.2.3 Zorgvuldigheidsverplichtingen in ander EU-recht

Artikel 1, derde lid, van de richtlijn elektronische handel bepaalt voorts dat de richtlijn een aanvulling vormt op het communautaire recht dat van toepassing is op de diensten van de informatiemaatschappij en niet afdoet aan het in de communautaire besluiten en nationale wetgeving ter uitvoering daarvan vastgelegde niveau van bescherming. De richtlijn laat dus ruimte voor het opnemen van zorgvuldigheidsverplichtingen in andere Europese wetgeving, die van toepassing is op bepaalde typen diensten van de informatiemaatschappij of ten aanzien van bepaalde soorten illegale inhoud. In de periode tussen de totstandkoming van de richtlijn elektronische handel en de totstandkoming van de digitaledienstenverordening is er op dit vlak veel gebeurd. Er is de afgelopen jaren een reeks aan wetgeving aangenomen ter bestrijding van bepaalde soorten illegale inhoud, zoals voor inbreuken op het auteursrecht[43], terroristische inhoud[44], materiaal

[42] Hof Leeuwarden 22 mei 2012, ECLI:NL:GHLEE:2012:BW6296 (Stokke/Marktplaats).

[43] Richtlijn 2019/790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG (PbEU 2019, L 130).

[44] Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud (PbEU 2021, L 172).

over seksueel misbruik van kinderen[45] en bepaalde illegale producten.[46] De herziene richtlijn audiovisuele mediadiensten bevat verder specifieke verplichtingen voor videoplatforms met betrekking tot content die minderjarigen zou kunnen schaden, haatzaaiende content of terroristische content.[47] Commissievoorstellen voor wetgeving ter bestrijding van seksueel misbruik van kinderen[48] en van geweld tegen vrouwen[49] zijn momenteel aanhangig. Ook is er op dit moment een verordeningsvoorstel betreffende transparantie en gerichte politieke reclame in behandeling. [50]

4.2.4 Gedragscodes

Uit overweging 40 bij de richtlijn elektronische handel volgt dat de Uniewetgever het kader voor aansprakelijkheidsvrijstellingen in de richtlijn zag als passende basis voor de uitwerking van mechanismen om illegale inhoud te verwijderen en ontoegankelijk te maken, in de vorm van vrijwillige overeenkomsten tussen alle betrokken partijen, zoals gedragscodes. Het was aan de Commissie en de lidstaten om de totstandkoming van dergelijke gedragscodes te stimuleren (artikel 16 van de richtlijn elektronische handel).[51]

De uitwerking van mechanismen om illegale inhoud te verwijderen en ontoegankelijk te maken heeft in Nederland plaatsgevonden in de zogenoemde '*Notice and takedown*-code', een gedragscode die in 2008 is opgesteld in samenwerking tussen de overheid, het bedrijfsleven en belangenverenigingen.[52] De gedragscode is vrijwillig en beschrijft hoe particulieren en bedrijven in de online sector omgaan met klachten over onrechtmatige inhoud op het internet. Daarnaast biedt de gedragscode richtsnoeren bij het bepalen of een klacht terecht is en welke stappen bij afhandeling gevolgd dienen te worden.

Een ander voorbeeld is de Gedragscode Abusebestrijding.[53] De gedragscode is vrijwillig en beschrijft de stappen die de aangesloten partijen moeten nemen om gebruik van hun digitale infrastructuur voor onrechtmatige activiteiten te voorkomen en te bestrijden. Onder digitale infrastructuur vallen ook mere conduit-, caching-, en hostingdiensten en online platforms in de zin van de verordening. Onder onrechtmatige activiteiten worden zaken verstaan die tevens illegale inhoud in de zin van de verordening kunnen zijn, zoals phishing, het verspreiden van malware of DDoS-aanvallen.

---

[45] Verordening (EU) 2021/1232 van het Europees Parlement en de Raad van 14 juli 2021 betreffende een tijdelijke afwijking van sommige bepalingen van Richtlijn 2002/58/EG ten aanzien van het gebruik van technologieën door aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten voor de verwerking van persoonsgegevens en andere gegevens ten behoeve van de bestrijding van online seksueel misbruik van kinderen (PbEU 2021, L 274).

[46] Verordening (EU) 2019/1148 van het Europees Parlement en de Raad van 20 juni 2019 over het op de markt brengen en het gebruik van precursoren voor explosieven, tot wijziging van Verordening (EG) nr. 1907/2006 en tot intrekking van Verordening (EU) nr. 98/2013 (PbEU 2019, L 186).

[47] Richtlijn (EU) 2018/1808 van het Europees Parlement en de Raad van 14 november 2018 tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten) in het licht van een veranderende marktsituatie (PbEU 2018, L 303).

[48] Voorstel voor een Verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen, COM(2022) 209 final.

[49] Voorstel voor een Richtlijn van het Europees Parlement en de Raad ter bestrijding van geweld tegen vrouwen en huiselijk geweld, COM(2022) 105 final.

[50] Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende transparantie en gerichte politieke reclame, COM(2021) 731 final.

[51] Zie overweging 48 bij de richtlijn.

[52] Zie https://noticeandtakedowncode.nl/.

[53] Zie https://www.cleannetworks.net/wp-content/uploads/2021/11/gedragscode_20211125.pdf.

Op EU-niveau kwam de Commissie in 2016 verder met een aantal grote platforms een "Code of Conduct on countering illegal hate speech" overeen. Ook kwam de Commissie in 2011 met online platforms en houders van rechten een Memorandum of Understanding (MoU) overeen over de verkoop van namaakgoederen op het internet, met als doel te voorkomen dat aanbiedingen van namaakgoederen op online marktplaatsen verschijnen. Dit MoU is in 2016 aangepast.[54]

Er is verder steeds meer aandacht voor de maatschappelijke risico's voortvloeiend uit de verspreiding van onwenselijke informatie, waaronder desinformatie, bijvoorbeeld met betrekking tot COVID-19 en democratische verkiezingen. Het gaat hierbij om informatie die op zichzelf legaal is, maar die desondanks onwenselijk is vanwege de daarmee gepaard gaande risico's. Ter bestrijding van de maatschappelijke risico's van desinformatie is in 2018 een praktijkcode tegen desinformatie[55] in het leven geroepen, die in 2022 is versterkt en ondertekend door 34 partijen. Deze en andere gedragscodes kunnen worden gebruikt door de civiele rechter ter invulling van de algemene zorgvuldigheidsnormen.[56]

4.3 ***Inhoud verordening***

4.3.1 Algemeen

De zorgvuldigheidsverplichtingen zijn in de verordening geordend naar categorie tussenhandeldienst, waarbij de vijf afdelingen van hoofdstuk III een gelaagde structuur vormen. Afdeling 1 bevat verplichtingen die van toepassing zijn op alle tussenhandeldiensten. Afdeling 2 bestaat uit aanvullende verplichtingen die enkel gelden voor hostingdiensten. Afdeling 3 bevat aanvullende verplichtingen voor online platforms, terwijl afdeling 4 enkele aanvullende verplichtingen bevat voor online marktplaatsen. Afdeling 5 omvat aanvullende verplichtingen voor zogenaamde *zeer grote* online platforms en *zeer grote* online zoekmachines. Aanbieders van zeer grote online platforms moeten dus aan de verplichtingen uit alle afdelingen van hoofdstuk III voldoen. Omgekeerd hoeft een internettoegangsdienst, die kwalificeert als mere conduit-dienst, alleen aan de verplichtingen voor tussenhandeldiensten te voldoen (afdeling 1). In het geval een aanbieder meerdere typen tussenhandeldiensten aanbiedt, moet de aanbieder ten aanzien van elke tussenhandeldienst voldoen aan de verplichtingen die gelden voor dat type dienst. Afdeling 6 bevat ten slotte bepalingen over het opstellen van vrijwillige normen en gedragscodes die bijdragen aan de correcte toepassing van de verordening.

De in de verordening opgenomen zorgvuldigheidsverplichtingen zijn verschillend van aard. Zo heeft een deel van de verplichtingen betrekking op de zorgvuldigheid die de tussenpersoon in acht moet nemen jegens zijn afnemers (consumenten en zakelijke gebruikers), terwijl er ook verplichtingen zijn die (mede) betrekking hebben op een zorgvuldige omgang met derden, zoals melders van illegale inhoud. Een deel van de verplichtingen heeft voorts betrekking op de inhoud die met behulp van de tussenhandeldienst wordt verspreid of opgeslagen, maar de verordening bevat ook verplichtingen die betrekking hebben op andere facetten van de tussenhandeldienst, zoals de inrichting van de online-interface, de omgang met persoonsgegevens, online reclames en de bescherming van minderjarigen in het algemeen. Tot slot heeft een deel van de verplichtingen een concreet en

[54] Memorandum of understanding on the sale of counterfeit goods on the internet.
[55] Richtsnoeren van de Europese Commissie ter versterking van de praktijkcode betreffende desinformatie (COM(2021) 262 final).
[56] Zie bijvoorbeeld Rb. Amsterdam (vzr.) 18 augustus 2021, ECLI:NL:RBAMS:2021:4308 (YouTube/Van Haga) en Rb. Amsterdam (vzr.) 15 september 2021, ECLI:NL:RBAMS:2021:5117 (FvD/YouTube).

specifiek karakter, terwijl een ander deel veel meer het karakter heeft van een open en algemene norm. Voorbeelden van zulke open en algemene normen in de verordening zijn:

- de verplichting voor aanbieders van tussenhandeldiensten om zorgvuldig, objectief en evenredig te handelen bij het toepassen van inhoudsmoderatie (artikel 14, vierde lid, van de verordening);
- de verplichting voor aanbieders van online platforms om te goeder trouw samen te werken met buitengerechtelijke geschillenbeslechtingsorganen (artikel 21, tweede lid, van de verordening);
- de verplichting voor aanbieders van online platforms om hun online-interfaces zodanig te ontwerpen, organiseren en beheren dat zij afnemers niet misleiden, manipuleren of hun vermogen ondermijnen om vrije en geïnformeerde beslissingen te nemen (artikel 25, eerste lid, van de verordening);
- de verplichting voor aanbieders van online platforms om passende en evenredige maatregelen te nemen om een hoog niveau van privacy, veiligheid en bescherming van minderjarigen te waarborgen (artikel 28, eerste lid, van de verordening).

Een ander relevant onderscheid is dat sommige zorgvuldigheidsverplichtingen altijd gelden, ongeacht of er in een concreet geval sprake is van illegale informatie of informatie in strijd met de algemene voorwaarden. Een ander deel van de verplichtingen ziet, daarentegen, op de wijze waarop een aanbieder zorgvuldig moet handelen als hij op de hoogte raakt van de aanwezigheid van dergelijke informatie op zijn dienst. Bij dit laatste type verplichtingen is het belangrijk om te benadrukken dat de verordening niet bepaalt wat illegale informatie of informatie in strijd met de algemene voorwaarden is. De beoordeling daarvan dient te geschieden op basis van het toepasselijke nationale of Unierecht of de toepasselijke algemene voorwaarden. De verordening bevat als zodanig ook geen verplichting voor aanbieders om dergelijke informatie te verwijderen of ontoegankelijk te maken[57], maar enkel verplichtingen over hoe hij besluiten daarover zorgvuldig moet nemen. De verplichting om de inhoud te verwijderen of ontoegankelijk te maken moet ook volgen uit het toepasselijke nationale of Unierecht en moet worden opgelegd door een op grond van dat recht bevoegde autoriteit.

In overweging 41 wordt benadrukt dat de zorgvuldigheidsverplichtingen los gezien moeten worden van de kwestie van aansprakelijkheid van deze aanbieders. Dat betekent onder meer dat de toepasselijkheid van de aansprakelijkheidsvrijstellingen niet afhankelijk is van het voldoen aan de zorgvuldigheidsverplichtingen uit de verordening en vice versa. Voor de toepasselijkheid van de zorgvuldigheidsverplichtingen is voldoende dat een dienst te beschouwen is als tussenhandeldienst, terwijl om te bepalen of die dienst binnen de werkingssfeer van de aansprakelijkheidsvrijstelling valt, moet worden beoordeeld of aan de voorwaarden van de artikelen 4, 5 en 6 van de verordening is voldaan. Ook de consequenties moeten onderscheiden worden. Als een aanbieder van een tussenhandeldienst niet aan een zorgvuldigheidsverplichting voldoet, heeft de bevoegde autoriteit verschillende bevoegdheden om hierop te handhaven, zoals het uitvoeren van inspecties of het opleggen van geldboeten (zie paragraaf 5.3 van deze memorie van toelichting). De consequentie van het niet voldoen aan de voorwaarden van de artikelen 4, 5 of 6 van de verordening, daarentegen, is dat de aanbieder van de tussenhandeldienst zich niet kan beroepen op de aansprakelijkheidsvrijstelling (zie paragraaf 3.2.1 van deze memorie van toelichting).

[57] Het niet verwijderen of ontoegankelijk maken kan wel tot gevolg hebben dat de aanbieder geen beroep kan doen op de aansprakelijkheidsvrijstelling van artikel 6 van de verordening.

4.3.2 Verplichtingen die gelden voor alle aanbieders van tussenhandeldiensten

4.3.2.1 Contactpunten en wettelijke vertegenwoordiger van de aanbieder

De artikelen 11, 12 en 13 van de verordening bevatten verplichtingen voor aanbieders van tussenhandeldiensten die tot doel hebben de communicatie met hen te vergemakkelijken. Op grond van artikel 11 van de verordening moeten zij een centraal elektronisch contactpunt instellen voor communicatie over de toepassing van de verordening met de autoriteiten van de lidstaten, de Commissie en de digitaledienstenraad. In overweging 42 bij de verordening wordt genoemd dat ook betrouwbare *flaggers* (zie nader paragraaf 4.3.4.3 van deze memorie van toelichting) en beroepsorganisaties gebruik kunnen maken van dit contactpunt. Aanbieders moeten ook aangeven in welke taal of talen met hen gecommuniceerd kan worden. Het derde lid van artikel 11 van de verordening bevat daar nadere regels over. Deze talen zijn onder meer van belang voor de bevelen van autoriteiten aan aanbieders om informatie te verwijderen of informatie te verstrekken (zie paragraaf 3.4 van deze memorie van toelichting).

Voor aanbieders die niet in de Unie zijn gevestigd, geldt de verplichting om een wettelijk vertegenwoordiger in de Unie aan te wijzen, die naast of in plaats van de aanbieder kan worden geraadpleegd door de bevoegde autoriteiten van de lidstaten, de Commissie en de digitaledienstenraad en zelfstandig aansprakelijk kan worden gesteld voor niet-naleving van de verordening (artikel 13 van de verordening). Hiermee wordt gewaarborgd dat ook diensten die buiten de Unie gevestigd zijn effectief kunnen worden aangesproken op niet-naleving van de verordening. In overweging 44 bij de verordening wordt verduidelijkt dat een in de Unie gevestigde dochteronderneming of moederonderneming van de aanbieder kan worden aangewezen als wettelijk vertegenwoordiger.

De verplichting om een centraal contactpunt in te stellen geldt ook voor het contact tussen de aanbieder en zijn afnemers (artikel 12 van de verordening). Het contactpunt moet het afnemers mogelijk maken om rechtstreeks, snel, langs elektronische weg en op een gebruiksvriendelijke manier contact te hebben met de aanbieder. De afnemers moeten voorts in staat zijn om zelf het communicatiemiddel te kiezen. De beschikbare communicatiemiddelen mogen niet uitsluitend gebaseerd zijn op geautomatiseerde hulpmiddelen.

4.3.2.2 Verplichtingen ten aanzien van inhoudsmoderatie

Aanbieders van tussenhandeldiensten hebben een contractuele verhouding met de afnemers van hun diensten. 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. Blijkens overweging 45 bij de verordening heeft de Uniewetgever het desondanks nodig geacht om regels te stellen over deze contractuele verhouding in het belang van de transparantie, de bescherming van afnemers en het voorkomen van oneerlijke of willekeurige resultaten. In artikel 14 van de verordening worden daarom regels gesteld over de eventuele beperkingen die de aanbieders aan het gebruik van hun dienst opleggen in hun algemene voorwaarden met betrekking tot door de afnemers van de dienst verstrekte informatie. Op grond van het eerste lid dienen aanbieders in hun algemene voorwaarden duidelijk te zijn over eventuele inhoudsmoderatie die zij toepassen en de maatregelen, procedures en instrumenten die zij daarvoor gebruiken, met inbegrip van informatie over algoritmische besluitvorming en menselijke controle. Het begrip “inhoudsmoderatie” is toegelicht in paragraaf 2.4.4 van deze memorie van toelichting en heeft zowel betrekking op illegale informatie als op informatie die in strijd is met de algemene voorwaarden van de aanbieder. “Algemene voorwaarden” zijn volgens artikel 3, onderdeel u, van de

verordening alle bepalingen, ongeacht hun naam of vorm, die van toepassing zijn op de contractuele verhouding tussen de aanbieder van de tussenhandeldiensten en de afnemers van de dienst.

De betreffende informatie moet in duidelijke, eenvoudige, begrijpelijke, gebruiksvriendelijke en ondubbelzinnige taal beschreven zijn en openbaar beschikbaar zijn. Het tweede, derde, vijfde en zesde lid van artikel 14 van de verordening bevatten een aantal aanvullende eisen aan de toegankelijkheid van de algemene voorwaarden, onder meer over de begrijpelijkheid voor minderjarigen en de gebruikte taal.

Op grond van artikel 14, vierde lid, van de verordening dienen aanbieders bij de toepassing en handhaving van inhoudsmoderatie op een zorgvuldige, objectieve en evenredige wijze te handelen. Blijkens overweging 47 bij de verordening volgt hieruit dat aanbieders bij het ontwerpen, toepassen en handhaven van de beperkingen die zij aan het gebruik van hun dienst opleggen op een niet-willekeurige en niet-discriminerende wijze te werk gaan. Voorts moeten zij gepaste aandacht hebben voor de rechten en legitieme belangen van alle betrokkenen. Onder deze rechten en legitieme belangen moeten worden begrepen de grondrechten van de afnemers van de dienst, zoals de vrijheid van meningsuiting, de vrijheid en pluriformiteit van de media en andere fundamentele rechten en vrijheden, zoals verankerd in het Handvest. In overweging 47 bij de verordening worden in dit verband ook de leidende beginselen van de Verenigde Naties inzake bedrijfsleven en mensenrechten genoemd. In dezelfde overweging wordt gesteld dat met name aanbieders van zeer grote online platforms naar behoren rekening moeten houden met de vrijheid van meningsuiting en informatie, met inbegrip van de vrijheid en de pluriformiteit van de media. 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.

Artikel 14, vierde lid, van de verordening veronderstelt daarmee de horizontale werking van grondrechten, waaronder de fundamentele rechten en vrijheden van het Handvest. Dit is in lijn met de jurisprudentie van het HvJ EU, waarin het HvJ EU de horizontale werking van de rechten in het Handvest heeft vastgesteld.[58] Ook door de Nederlandse rechter wordt de horizontale werking van grondrechten geaccepteerd.[59] De algemene beginselen waar de aanbieders zich aan moeten houden (zorgvuldigheid, proportionaliteit, niet-willekeurigheid en non-discriminatie), zijn in al dan niet gecodificeerde vorm onderdeel van het Nederlandse civiele recht. Artikel 14, vierde lid, van de verordening brengt dus in elk geval voor wat betreft de toepassing van het Nederlandse civiele recht geen nieuwe normen met zich. Op de handhaving van deze norm door de digitaledienstencoördinator wordt in paragraaf 5.3.6.2 van deze memorie van toelichting nader ingegaan.

Artikel 15 van de verordening voorziet in een jaarlijkse rapportageverplichting voor aanbieders van tussenhandeldiensten. Deze rapporten moeten op duidelijke en makkelijk te begrijpen wijze inzicht geven in de inhoudsmoderatie die de aanbieder heeft uitgevoerd. Meer specifiek gaat het om

---

[58] HvJ EU 6 november 2018, zaken C-569/16 en C-570/16, ECLI:EU:C:2018:871 (Bauer en Broßonn), HvJ EU 6 november 2018, zaak C-619/16, ECLI:EU:C:2018:872 (Kreuziger) en HvJ EU 6 november 2018, zaak C-684/16, ECLI:EU:C:2018:874 (Max-Planck-Gesellschaft).

[59] Een dergelijke horizontale werking wordt in de (lagere) Nederlandse rechtspraak reeds erkend en toegepast. Zie Rb. Amsterdam (vzr.) 9 september 2020, ECLI:NL:RBAMS:2020:4435 (Café Weltschmerz / YouTube), Rb. Amsterdam (vzr.) 13 oktober 2020, ECLI:NL:RBAMS:2020:4966 (Viruswaarheid/Facebook), Rb. Amsterdam (vzr.) 18 augustus 2021, ECLI:NL:RBAMS:2021:4308 (YouTube/Van Haga), Rb. Amsterdam (vzr.) 15 september 2021, ECLI:NL:RBAMS:2021:5117 (FvD /YouTube), Rb. Rotterdam (vzr.) 29 oktober 2021, ECLI:NL:RBROT:2021:10459 (Willem Engel/Facebook), Rb. Noord-Holland 6 oktober 2021 , ECLI:NL:RBNHO:2021:8539 (Van Haga/LinkedIn).

informatie over hoe is omgegaan met de ontvangen bevelen van lidstatelijke autoriteiten (paragraaf 3.4), meldingen van vermeend illegale inhoud door afnemers en derden (paragraaf 4.3.3.1), inhoudsmoderatie op eigen initiatief (paragraaf 4.3.2.2) en klachtenafhandeling (paragraaf 4.3.4.2). Dit stelt afnemers in staat om geïnformeerde keuzes te maken over het gebruik van de desbetreffende tussenhandeldienst. Het is ook een nuttige bron van informatie voor journalisten, onderzoekers, politici, beleidsmakers en toezichthouders. Om onevenredige lasten te voorkomen, gelden de transparantierapportageverplichtingen niet voor aanbieders die micro-of kleine ondernemingen zijn in de zin van Aanbeveling 2003/361/EG.[60] Voor (zeer grote) online platforms en (zeer grote) online zoekmachines gelden op grond van artikel 24 en 42 van de verordening aanvullende rapportageverplichtingen (zie verder paragrafen 4.3.4.5 en 4.3.6.8 van deze memorie van toelichting).

4.3.3 Aanvullende verplichtingen voor aanbieders van hostingdiensten

4.3.3.1 Kennisgevings- en actiemechanisme voor illegale inhoud

Aanbieders van hostingdiensten zijn op grond van artikel 16, eerste lid, van de verordening verplicht om te voorzien in mechanismen om personen en entiteiten de mogelijkheid te geven om hen in kennis te stellen van de aanwezigheid van inhoud die deze personen of entiteiten als illegaal beschouwen. De betreffende meldingen kunnen dus door een ieder worden gedaan en niet enkel door de afnemers van de dienst. Blijkens overweging 51 bij de verordening moet de melding worden gericht tot de aanbieder die zowel technisch als operationeel in staat is actie te ondernemen tegen de specifieke illegale inhoud waar het om gaat. De mogelijkheid om deze meldingen te ontvangen en verwerken wordt ook wel een *notice-and-action*-procedure genoemd. Op grond van het tweede lid van artikel 16 van de verordening moeten de aanbieders deze mechanismen zo vormgeven dat ze de indiening van voldoende nauwkeurige en gemotiveerde meldingen vergemakkelijken. Meer specifiek moeten ze de indiening van meldingen mogelijk maken en vergemakkelijken die een aantal specifieke elementen bevatten: een motivering waarom de informatie illegaal is, de exacte elektronische locatie van de informatie, de naam en het emailadres van de melder (behoudens uitzonderingsgevallen)[61], en een verklaring dat de melding te goeder trouw wordt gedaan en nauwkeurig en volledig is. Dit zijn overigens geen verplichte elementen van een melding, maar de aanbieder moet het op grond van artikel 16, tweede lid, van de verordening mogelijk maken dat deze elementen onderdeel zijn van de melding.

In het derde lid van artikel 16 van de verordening wordt bepaald dat dit soort meldingen worden verondersteld aanleiding te geven tot werkelijke kennis of bekendheid van de betrokken informatie voor de toepassing van artikel 6 van de verordening, indien de melding een zorgvuldige aanbieder in staat stelt het illegale karakter van de betrokken activiteit of informatie vast te stellen zonder een

---

[60] Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PbEU 2003, L 124). Volgens deze Aanbeveling is een micro-onderneming een onderneming waar minder dan 10 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 2 miljoen EUR niet overschrijdt. Een kleine onderneming wordt gedefinieerd als een onderneming waar minder dan 50 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 10 miljoen EUR niet overschrijdt.

[61] Over het vermelden van de naam en contactgegevens van de melder wordt in de overwegingen bij de verordening gesteld dat dit geen verplicht onderdeel is van een melding, maar dat het wel verplicht is om de melder te verzoeken zijn identiteit bekend te maken om misbruik van het kennisgevingsmechanisme te voorkomen (overwegingen 50 en 53). Voor sommige soorten gemelde informatie is evenwel de identiteit van de melder nodig om te beoordelen of de betrokken informatie illegale inhoud vormt. Het vragen naar de identiteit moet voorts achterwege blijven als de melding betrekking heeft op bepaalde strafbare feiten op het gebied van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie.

uitgebreid juridisch onderzoek. Dit is in lijn met de jurisprudentie van het HvJ EU over de aansprakelijkheidsvrijstelling voor aanbieders van hostingdiensten (zie nader paragraaf 3.2.1.2 van deze memorie van toelichting).[62] In het vierde en vijfde lid is bepaald dat de melder een ontvangstbevestiging en een afschrift van het besluit dient te ontvangen over de informatie waarop de melding betrekking heeft. Deze verplichtingen gelden uiteraard enkel als de melding de elektronische contactgegevens van de melder bevat.

Artikel 16, zesde lid, van de verordening bepaalt dat de hostingdienst ontvangen meldingen op een tijdige, zorgvuldige, niet-willekeurige en objectieve wijze moet verwerken en behandelen. Deze verplichting overlapt deels met artikel 14, vierde lid, van de verordening. Wat "tijdig" betekent, hangt blijkens overweging 52 af van het type illegale inhoud en de urgentie om actie te ondernemen. Zo dienen hostingdiensten onverwijld te handelen als het illegale inhoud betreft die een bedreiging vormt voor het leven of de veiligheid van personen. Het besluit naar aanleiding van een melding kan blijkens overweging 51 bij de verordening ook inhouden dat de aanbieder de betreffende inhoud om technische of operationele redenen niet kan verwijderen.

4.3.3.2 Motiveringsplicht bij inhoudsmoderatie

Artikel 17, eerste lid, van de verordening bepaalt dat aanbieders van hostingdiensten de betrokken afnemers een duidelijke en specifieke motivering moeten verstrekken als zij overgaan tot inhoudsmoderatie, om de afnemers in staat te stellen om beslissingen van aanbieders over beperkingen goed te begrijpen en eventueel aan te vechten. De motiveringsplicht geldt ongeacht of de beslissing is genomen naar aanleiding van een melding op grond van artikel 16 van de verordening of naar aanleiding van een onderzoek op eigen initiatief van de aanbieder. Deze plicht geldt niet als de inhoudsmoderatie geschiedt op basis van een bevel als bedoeld in artikel 9 van de verordening. In artikel 9, vijfde lid, van de verordening wordt voorgeschreven hoe de aanbieder zijn afnemer over het opvolgen van een dergelijk bevel moet informeren.

In het derde lid van artikel 17 van de verordening worden de elementen genoemd waar de motivering ten minste uit moet bestaan. In het vierde lid van artikel 17 is bepaald dat de verstrekte informatie duidelijk en makkelijk te begrijpen moet zijn en zo nauwkeurig en specifiek als redelijk gezien mogelijk is in de gegeven omstandigheden. De motivering kan achterwege blijven als de aanbieder niet beschikt over de contactgegevens van de afnemer of als de informatie deel uitmaakt van misleidende grootschalige commerciële inhoud (artikel 17, tweede lid, van de verordening).

4.3.3.3 Meldplicht strafbare feiten met gevaar voor leven of veiligheid personen

Artikel 18 van de verordening verplicht aanbieders van hostingdiensten om melding te doen bij de rechtshandhavings- of gerechtelijke autoriteiten van de betrokken lidstaat van een vermoeden van een strafbaar feit waarbij het leven of de veiligheid van een persoon wordt bedreigd. De aanbieder moet daarbij alle relevante informatie verstrekken waarover hij beschikt. Het gaat bij deze meldingsplicht om strafbare feiten die zijn of worden gepleegd op het moment van de melding, maar ook strafbare feiten die waarschijnlijk in de toekomst zullen worden gepleegd. De 'betrokken lidstaat' is de lidstaat waarvan de aanbieder vermoedt dat het feit daar is begaan of waar de dader of slachtoffer zich bevindt of verblijft. Kan de aanbieder de betrokken lidstaat niet bepalen, dan brengt hij de instanties op de hoogte van de lidstaat waar hij of zijn wettelijk vertegenwoordiger is gevestigd. Een vergelijkbare meldplicht voor hostingdiensten is, voor wat betreft terroristische

[62] HvJ EU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (L'Oréal/eBay), r.o. 122 en HvJ EU 22 juni 2021, zaken C-682/18 en C-683/18, ECLI:EU:C:2021:503 (YouTube en Cyando), r.o. 116.

inhoud die een onmiddellijk levensbedreigend gevaar inhoudt, neergelegd in de verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud.[63]

4.3.4 Aanvullende verplichtingen voor online platforms

Het zwaartepunt van de verordening bestaat uit de regeling die van toepassing is op online platforms, de aanbieders van diensten bestaande uit de opslag én publieke verspreiding van informatie van gebruikers (zie paragraaf 2.4.5). Afdeling 3 van hoofdstuk III bevat regels voor online platforms in het algemeen (dus ongeacht hun grootte). Afdeling 4 bevat bijkomende bepalingen die alleen gelden voor aanbieders van online platforms die consumenten de mogelijkheid bieden overeenkomsten op afstand te sluiten met handelaren (B2C online marktplaatsen, zie paragraaf 4.3.5). Afdeling 5 bevat aanvullende regels voor online platforms (en online zoekmachines) die zijn aan te merken als "zeer groot" (zie paragraaf 4.3.6).

4.3.4.1 Uitzondering micro- en kleine ondernemingen

Om onevenredige lasten te voorkomen, zijn online platforms die kwalificeren als micro- en kleine onderneming in de zin van aanbeveling 2003/361/EG[64] in artikel 19 van de verordening uitgezonderd van de verplichtingen in afdeling 3, met uitzondering van de verplichting om informatie te verstrekken over het gemiddelde maandelijks aantal actieve afnemers (artikel 24, derde lid, van de verordening). Als een dergelijk platform de drempels om te kwalificeren als micro- en kleine onderneming overstijgt, dan moet het platform 12 maanden na dat moment aan alle verplichtingen van deze afdeling voldoen. Deze uitzondering geldt verder niet voor micro- en kleine ondernemingen die kwalificeren als zeer groot online platform (derde lid van artikel 19).

4.3.4.2 Verhaalsmogelijkheden bij inhoudsmoderatie voor gebruikers

Diverse bepalingen in afdeling 3 beogen het gebruikers makkelijker te maken om besluiten over inhoudsmoderatie van online platforms te betwisten. Te denken valt aan besluiten om informatie te verwijderen, om accounts van gebruikers te schorsen of de dienstverlening tijdelijk te staken. Dat geldt zowel wanneer het besluit genomen is omdat het (vermeende) illegale inhoud betreft als ook vanwege vermeende schendingen van de algemene voorwaarden.

Voor dit doeleinde moeten aanbieders van online platforms op grond van artikel 20 van de verordening een intern klachtenafhandelingssysteem instellen waarmee gebruikers gemakkelijk, elektronisch en gratis klachten kunnen indienen tegen dergelijke besluiten. Die mogelijkheid moeten zij hebben tot ten minste zes maanden nadat zij van het besluit in kennis zijn gesteld. Op grond van het vierde lid moeten klachten tijdig, op niet-discriminerende, zorgvuldige en niet-willekeurige wijze worden afgehandeld. Besluiten over klachten moeten worden genomen door gekwalificeerd personeel en mogen niet louter op basis van geautomatiseerde middelen worden genomen. De klager moet onverwijld in kennis worden gesteld van het gemotiveerde besluit op een klacht.

Afnemers kunnen op grond van artikel 21, eerste lid, van de verordening voorts geschillen met een online platform over inhoudsmoderatie voorleggen aan gecertificeerde buitengerechtelijke geschillenbeslechtingsorganen. De uitkomst van de procedure is niet bindend en dus behouden partijen het recht om hetzelfde geschil aan de rechter voor te leggen. Op grond van artikel 21, tweede lid, zijn partijen verplicht te goeder trouw samen te werken met gecertificeerde

[63] Artikel 14, vijfde lid, van de verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud (PbEU 2021, L 172).
[64] Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PbEU 2003, L 124).

buitengerechtelijke geschillenbeslechtingsorganen. Aanbieders van online platforms kunnen echter weigeren aan buitengerechtelijke geschilbeslechting deel te nemen indien er eerder een geschil is beslecht met betrekking tot dezelfde informatie en dezelfde gronden voor vermeende illegaliteit of onverenigbaarheid met de algemene voorwaarden. Het orgaan geeft binnen 90 dagen een beslissing; deze termijn kan in complexe gevallen eenmalig worden verlengd (vierde lid). Als de afnemer gelijk krijgt, dan draagt het online platform de kosten van de procedure. In andere gevallen worden de kosten gedeeld, tenzij de afnemer te kwader trouw handelde (vijfde lid).

Buitengerechtelijke geschillenbeslechtingsorganen kunnen worden gecertificeerd door de digitaledienstencoördinator in de lidstaat waar zij gevestigd zijn, indien zij voldoen aan eisen op het gebied van onafhankelijkheid, professionaliteit en deskundigheid (artikel 21, derde lid, van de verordening). Het certificaat wordt verleend voor een verlengbare periode van maximaal vijf jaar en is vervolgens geldig in alle lidstaten. De Commissie houdt een actuele lijst bij van gecertificeerde organen, en waar van toepassing, de specifieke expertise van deze organen. Gecertificeerde organen dienen jaarlijks verslag uit te brengen aan de digitaledienstencoördinator die hen heeft gecertificeerd. Een digitaledienstencoördinator kan het certificaat intrekken als een orgaan niet langer voldoet aan de voorwaarden voor certificering. Tot slot biedt het zesde lid van artikel 21 de mogelijkheid aan lidstaten om zelf buitengerechtelijke geschillenbeslechtingsorganen op te richten of de activiteiten van een of meer buitengerechtelijke geschillenbeslechtingsorganen te ondersteunen.

4.3.4.3 Meldingen van illegale inhoud door betrouwbare flaggers

In artikel 22, eerste lid, van de verordening is bepaald dat aanbieders van online platforms meldingen van illegale inhoud, die via het kennisgevingsmechanisme als bedoeld in artikel 16 van de verordening worden gedaan en afkomstig zijn van een betrouwbare flagger, prioritair en onverwijld dienen te verwerken en af te handelen. De digitaledienstencoördinator kent de status van betrouwbare flagger op verzoek toe aan entiteiten die voldoen aan de in artikel 22, tweede lid, gestelde eisen inzake deskundigheid, onafhankelijkheid en professionaliteit. Meldingen van partijen die aan die eisen voldoen zullen in algemene zin betrouwbaar zijn en daarom ligt het in de rede om deze meldingen voorrang te geven. Dit laat overigens onverlet dat online platforms ook andere meldingen tijdig en zorgvuldig dienen te verwerken en af te handelen (artikel 16, zesde lid, van de verordening). Uit overweging 61 bij de verordening volgt dat het aantal betrouwbare flaggers onder de verordening beperkt moet blijven, omdat anders de effectiviteit van het mechanisme afneemt.

Slechts entiteiten kunnen de status van betrouwbare flagger krijgen. Natuurlijke personen kunnen dit dus niet. Entiteiten is een breed begrip en omvat zowel publieke als private organisaties. Overweging 61 noemt als voorbeelden onder meer eenheden voor meldingen van internetuitingen van nationale rechtshandhavingsinstanties en van Europol met betrekking tot terroristische inhoud. Te denken valt hierbij aan de EU Internet Referral Unit. Ook organisaties die deel uitmaken van het INHOPE-netwerk van meldpunten voor het melden van materiaal over seksueel misbruik van kinderen en organisaties die zich bezighouden met racistische en xenofobe uitingen online worden als voorbeeld genoemd. In Nederland valt dan te denken aan het Expertisebureau Online Kindermisbruik (EOKM) en het Meldpunt internet Discriminatie (MiND). Overweging 61 moedigt verder met name industrieverenigingen die de belangen van hun leden behartigen aan om de status van betrouwbare flagger aan te vragen. Te denken valt dan bijvoorbeeld aan industrieverenigingen die belangen behartigen op het gebied van inbreuken op intellectuele eigendomsrechten in het algemeen, en namaak en piraterij in het bijzonder.

De digitaledienstencoördinator kan de status van betrouwbare flagger op grond van de verordening schorsen of intrekken wanneer een entiteit niet langer aan die voorwaarden voldoet of zich schuldig

maakt aan misbruik, bijvoorbeeld doordat hij een aanzienlijk aantal onvoldoende nauwkeurige, onjuist of niet voldoende gemotiveerde meldingen heeft gedaan. De Commissie houdt een openbaar toegankelijke databank bij met daarin alle entiteiten die in de EU de status van betrouwbare flagger hebben. In die databank staan ook schorsingen en intrekkingen vermeld.

4.3.4.4 Schorsing van gebruikers

Op grond van artikel 23, eerste lid, van de verordening moeten aanbieders van online platforms afnemers schorsen die frequent kennelijk illegale inhoud verstrekken. Het gaat hier dus om het tijdelijk weren van afnemers die herhaaldelijk de fout in zijn gegaan. Belangrijk daarbij is dat het verspreiden frequent moet hebben plaatsgevonden en dat het om kennelijk illegale informatie gaat. De afnemer moet dus meerdere malen illegale inhoud hebben verstrekt waarvan hij zelf wist of had kunnen weten dat het illegaal was. In de praktijk komt dit neer op een zogenaamd "repeat infringer policy". Voordat een dergelijke schorsing aan de orde is, zal de aanbieder de afnemer voor elke keer dat hij heeft vastgesteld dat de afnemer illegale inhoud heeft verstrekt, op de hoogte moeten hebben gebracht van het gevolg dat hij daaraan heeft gegeven. Is de afnemer het niet eens met die vaststelling of het daaraan gegeven gevolg, dan kan hij daartegen in verweer komen (zie paragraaf 4.3.4.2 van deze memorie van toelichting). Dat proces staat los van de schorsing van de afnemer op grond van dit artikel, die pas aan de orde is als de afnemer frequent kennelijk illegale inhoud heeft verstrekt.

Artikel 23, tweede lid, van de verordening voorziet in het schorsen van de verwerking van meldingen op grond van het kennisgevingsmechanisme of klachten in het kader van het intern klachtenafhandelingssysteem, van melders of klagers die regelmatig meldingen doen of klachten indienen die kennelijk ongegrond zijn.

Voor de toepassing van zowel het eerste als het tweede lid van artikel 23 van de verordening geldt dat de betrokken afnemer, melder of klager voorafgaand aan de schorsing moet zijn gewaarschuwd en dat de schorsing beperkt blijft tot een redelijke periode. Ook moeten aanbieders elke zaak individueel en zorgvuldig bekijken en moeten zij 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). Ten slotte moeten zij in hun algemene voorwaarden duidelijkheid geven over hun beleid op dit punt (artikel 23, vierde lid, van de verordening).

4.3.4.5 Aanvullende informatieverplichtingen

Op grond van artikel 24, eerste lid, van de verordening moeten aanbieders van online platforms aanvullende informatie opnemen in de rapportages over inhoudsmoderatie die zij op grond van artikel 15 van de verordening moeten maken. Het gaat om informatie over het aantal geschillen dat is voorgelegd aan buitengerechtelijke geschillenbeslechtigingsorganen en het aantal schorsingen dat krachtens artikel 23 is opgelegd. Op grond van artikel 24, vijfde lid, van de verordening moeten aanbieders van online platforms hun besluiten omtrent inhoudsmoderatie onverwijld indienen bij de Commissie, met het oog op opname daarvan in een door de Commissie beheerde openbare databank.

Voorts moeten aanbieders van online platforms en online zoekmachines halfjaarlijks rapporteren over het gemiddelde aantal maandelijks actieve gebruikers dat zij hebben in de Europese Unie en moeten zij daarover op verzoek aanvullende informatie verstrekken aan de digitaledienstencoördinator van het land van vestiging of de Commissie (artikel 24, tweede en derde

lid, van de verordening).[65] Dit maakt het mogelijk om te beoordelen of zij kwalificeren als zeer groot online platform of zeer grote online zoekmachine in de zin van artikel 33 van de verordening. Voor een nadere toelichting op de aanwijzing van zeer grote online platforms of zeer grote online zoekmachines wordt verwezen naar paragraaf 4.3.6.2 van deze memorie van toelichting.

4.3.4.6 Vormgeving online-interfaces

Artikel 25, eerste lid, van de verordening bepaalt dat aanbieders van online platforms hun online-interfaces niet zodanig ontwerpen, organiseren of beheren dat zij afnemers misleiden of manipuleren of hun vermogen om vrije en geïnformeerde beslissingen te nemen, anderszins wezenlijk verstoren of ondermijnen. Het begrip "online-interface" moet breed worden opgevat, zo blijkt uit de definitie in artikel 3, onderdeel m, van de verordening: het omvat alle software, met inbegrip van een website of gedeelte daarvan en apps, waaronder mobiele apps. Deze verplichting staat dus los van de inhoud die via het online platform wordt verspreid en of die te beschouwen is als illegale inhoud of inhoud die in strijd is met de algemene voorwaarden van de aanbieder van het platform.

De op grond van deze bepaling verboden praktijken worden ook wel "dark patterns" genoemd: praktijken die het vermogen van afnemers om autonome en weloverwogen keuzes te maken of beslissingen te nemen, wezenlijk verstoren of belemmeren. Die praktijken kunnen worden gebruikt om de afnemers van de dienst te bewegen tot ongewenste gedragingen of tot ongewenste beslissingen die negatieve gevolgen voor hen hebben. Voorbeelden van dergelijke technieken die worden genoemd in overweging 67 bij de verordening zijn:

- het tonen van keuzes aan afnemers van de dienst op een niet-neutrale manier, bijvoorbeeld door bepaalde keuzes meer gewicht te geven door middel van visuele, auditieve of andere componenten;
- een reeds gemaakte keuze opnieuw aan een afnemer voorleggen;
- het omslachtiger maken van de procedure om een dienst te annuleren dan om erop in te tekenen;
- het moeilijker of tijdrovender maken van bepaalde keuzes dan andere;
- het onredelijk moeilijk maken om aankopen te staken of zich af te melden van een bepaald online platform;
- het sturen ("nudgen") van consumenten om de kans te vergroten dat ze bepaalde beslissingen nemen over transacties; en
- het zeer moeilijk maken om standaardinstellingen te wijzigen.

Artikel 25, tweede lid, van de verordening bepaalt dat het verbod niet van toepassing is op praktijken die onder de Richtlijn oneerlijke handelspraktijken[66] (hierna: richtlijn OHP) of de Algemene verordening gegevensbescherming[67] (hierna: AVG) vallen. Op grond van de richtlijn OHP zijn

[65] De Europese Commissie heeft hierover een toelichtend document gepubliceerd: https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers.

[66] 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).

[67] 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).

oneerlijke handelspraktijken van ondernemingen jegens consumenten verboden, in het bijzonder misleidende en agressieve praktijken. In de AVG worden eisen gesteld aan de toestemming voor het verwerken van persoonsgegevens, in het geval de grondslag van de verwerking van persoonsgegevens berust op toestemming van de betrokkene (artikel 6, eerste lid, onderdeel a, van de AVG). Vereist is onder meer dat die toestemming vrij, specifiek en geïnformeerd moet zijn gegeven. Indien een op grond van artikel 25, eerste lid, van de verordening verboden techniek reeds kwalificeert als een oneerlijke handelspraktijk jegens een consument onder de richtlijn OHP of als een manier om – in strijd met de AVG – op ongeoorloofde wijze toestemming voor gegevensverwerking van een betrokkene te verkrijgen, dan is de verordening dus niet van toepassing.

4.3.4.7 Online reclame

Artikel 26 van de verordening bevat verplichtingen voor aanbieders van online platforms met betrekking tot reclames op hun online-interface. In overweging 68 bij de verordening wordt het belang van online reclames onderstreept. Zo wordt de aanbieding van de dienst in veel gevallen geheel of gedeeltelijk gefinancierd met reclame-inkomsten. Online reclame kan echter aanzienlijke risico's met zich brengen, bijvoorbeeld als de inhoud van de reclame op zichzelf illegaal is of als de weergave van reclame op discriminerende wijze geschiedt of kwetsbaarheden van mensen aanspreekt of misbruikt. Dit risico speelt met name bij het toepassen van profilering in de zin van artikel 4, punt 4, van de AVG om aan afnemers reclames te tonen die aansluiten bij hun interesses. Dit targeten, waarvoor veelal (bijzondere) persoonsgegevens worden verwerkt, kan aanzienlijke risico's met zich meebrengen. De verordening beoogt deze risico's te adresseren

Het eerste lid van artikel 26 van de verordening vereist dat aanbieders van online platforms bij elke specifieke reclame op hun online-interface aan hun afnemers duidelijk maken dat de getoonde informatie reclame is, namens wie de reclame wordt getoond en wie de reclame heeft gefinancierd. Dit laatste is relevant in het geval adverteerders gebruikmaken van zogenaamde wederverkopers van advertentieruimte ("resellers"). Ook moet nuttige informatie worden verstrekt over de belangrijkste parameters die worden gebruikt om te bepalen aan welke afnemers een reclame wordt getoond. De afnemer moet ook worden geïnformeerd over de middelen waarover hij beschikt om dergelijke parameters te wijzigen. Artikel 26, tweede lid, van de verordening bepaalt dat aanbieders van online platforms hun afnemers de functionaliteit moeten bieden om te verklaren dat de inhoud die zij verstrekken commerciële communicatie bevat. Als de afnemer van die functionaliteit gebruik maakt, dan moet de aanbieder van het online platform ervoor zorgen dat de andere afnemers, als zij toegang krijgen tot die informatie, kunnen vaststellen dat er met betrekking tot die informatie een dergelijke verklaring is afgelegd. Hiermee wordt het vergemakkelijkt om te voldoen aan de verplichting neergelegd in artikel 6 van de richtlijn elektronische handel, zoals in Nederland geïmplementeerd in artikel 3:15e van het BW. Indien commerciële communicatie deel uitmaakt van een dienst van de informatiemaatschappij, moet degene in wiens opdracht de commerciële communicatie geschiedt op grond van deze artikelen ervoor zorgen dat de commerciële communicatie duidelijk herkenbaar is.

Het derde lid van artikel 26 van de verordening verbiedt het tonen van reclame gebaseerd op basis van profilering met gebruikmaking van bijzondere categorieën persoonsgegevens. Profilering is in artikel 4, punt 4, van de AVG gedefinieerd als elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij bepaalde persoonlijke aspecten van een natuurlijke persoon worden geanalyseerd of voorspeld. Bijzondere categorieën persoonsgegevens zijn persoonsgegevens die onder meer betrekking hebben op etnische afkomst, politieke opvattingen of seksuele geaardheid. Op grond van artikel 22 van de AVG heeft een betrokkene het recht om niet te worden onderworpen

aan een uitsluitend op grond van profilering op basis van bijzondere categorieën persoonsgegevens gebaseerd besluit dat hem in aanmerkelijke mate treft, tenzij de betrokkene uitdrukkelijk toestemming heeft gegeven of de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang. Artikel 26, derde lid, van de verordening vult die bepaling van de AVG aan, door te bepalen dat het gebruik van profilering op basis van bijzondere categorieën persoonsgegevens om online reclames te tonen op online platforms in alle gevallen verboden is en dus ook niet meer mogelijk is met uitdrukkelijke toestemming van de afnemer of om redenen van zwaarwegend algemeen belang.

4.3.4.8 Transparantie over aanbevelingssystemen

Artikel 27, eerste en tweede lid, van de verordening bepaalt dat aanbieders van online platforms in hun algemene voorwaarden moeten aangeven wat de belangrijkste parameters zijn die worden gebruikt in hun aanbevelingssystemen en welke opties afnemers van de dienst eventueel hebben om die parameters aan te passen. Zij moeten de parameters voor dergelijke aanbevelingssystemen op eenvoudig begrijpelijke wijze presenteren zodat de afnemers van de dienst begrijpen hoe informatie voor hen wordt geprioriteerd. Die parameters moeten ten minste de voornaamste criteria omvatten waarmee bepaald wordt welke informatie aan de afnemer van de dienst wordt aanbevolen, alsook de redenen voor het relatieve belang ervan. Onder "aanbevelingssysteem" wordt verstaan een geheel of gedeeltelijk geautomatiseerd systeem om informatie onder de aandacht van afnemers te brengen, te rangschikken of te prioriteren (artikel 3 onderdeel s, van de verordening). Op grond van het derde lid van artikel 27 van de verordening moeten de aanbieders een functionaliteit beschikbaar stellen waarmee afnemers kunnen kiezen uit de verschillende opties om de parameters van het aanbevelingssysteem te wijzigen, als de aanbieder meerdere opties aanbiedt. Deze functionaliteit moet te allen tijde en gemakkelijk toegankelijk worden aangeboden.

4.3.4.9 Maatregelen ter bescherming van minderjarigen

Artikel 28, eerste lid, van de verordening verplicht aanbieders van online platforms tot het nemen van passende en evenredige maatregelen om een hoog niveau van privacy, veiligheid en bescherming van minderjarigen te waarborgen binnen hun dienst. Deze verplichting is beperkt tot online platforms die toegankelijk zijn voor minderjarigen, hetgeen blijkens overweging 71 bij de verordening het geval is als de algemene voorwaarden minderjarigen toestaan de dienst te gebruiken, als de dienst gericht is op of voornamelijk wordt gebruikt door minderjarigen, of als de aanbieder op een andere manier weet dat sommige afnemers van zijn dienst minderjarig zijn, zoals uit de verwerking van persoonsgegevens voor andere doeleinden.

De norm van artikel 28, eerste lid, van de verordening heeft het karakter van een doelvoorschrift, waarin het doel een hoog niveau van privacy, veiligheid en bescherming van minderjarigen is. Er wordt niet voorgeschreven hoe dat doel moet worden bereikt, behoudens dat de te nemen maatregelen "passend en evenredig" dienen te zijn. Het is dus aan de aanbieders van online platforms om zelf te bepalen welke maatregelen zij nemen om aan deze verplichting te voldoen. Wel kan de Commissie op grond van het vierde lid van artikel 28 van de verordening richtsnoeren opstellen om aanbieders bij te staan bij de toepassing van het eerste lid. Overweging 71 bij de verordening geeft wel enkele voorbeelden van maatregelen, namelijk:

- het standaard ontwerpen van online-interfaces op een manier die het hoogste niveau van privacy, veiligheid en beveiliging waarborgt voor minderjarigen;
- het vaststellen van normen voor de bescherming van minderjarigen;
- deelname aan gedragscodes ter bescherming van minderjarigen; en

- rekening houden met de beste praktijken en beschikbare richtsnoeren, zoals die in de mededeling van de Commissie over 'Een digitaal decennium voor kinderen en jongeren: de nieuwe Europese strategie voor een beter internet voor kinderen (BIK+)'.[68]

De bescherming van minderjarigen is een belangrijke en brede Europese beleidsdoelstelling. Veel Europese en nationale wetgeving bevatten voorschriften die kunnen worden beschouwd als een maatregel om een hoog niveau van privacy, veiligheid en bescherming van minderjarigen te waarborgen. Zo strekken de verplichtingen van de AVG ook tot bescherming van de privacy van afnemers van online platforms, waaronder minderjarigen. Artikel 8 van de AVG voorziet zelfs in aanvullende bescherming van kinderen in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan kinderen. Ook de herziene richtlijn audiovisuele mediadiensten bevat in artikel 6bis en 28ter verplichtingen voor aanbieders van mediadiensten en videoplatforms die strekken ter bescherming van minderjarigen.[69] Dit doet de vraag rijzen of naleving van de AVG en de richtlijn audiovisuele mediadiensten, zoals geïmplementeerd in de Mediawet 2008, voldoende is om een hoog niveau van privacy, veiligheid en bescherming van minderjarigen te waarborgen, of dat aanvullende maatregelen vereist zijn om aan artikel 28, eerste lid, van deze verordening te voldoen. De richtsnoeren die de Commissie op grond van het vierde lid vaststelt, kunnen op dit punt duidelijkheid scheppen.

Het tweede lid van artikel 28 van de verordening bevat voorts een verbod voor aanbieders van online platforms om reclame op basis van profilering te tonen met gebruikmaking van persoonsgegevens van een afnemer waarvan zij zich er met redelijke zekerheid van bewust zijn dat die minderjarig is. Op het gebruik van profilering in relatie tot online reclames is nader ingegaan in paragraaf 4.3.4.7 van deze memorie van toelichting. In artikel 28, derde lid, van de verordening wordt tot slot verduidelijkt dat de naleving van het eerste en tweede lid van artikel 28 er niet toe verplicht om over te gaan tot de aanvullende verwerking van persoonsgegevens om te beoordelen of een afnemer minderjarig is. Dat zou immers haaks staan op het doel om een hoog niveau van privacy van minderjarigen te waarborgen.

4.3.5 Aanvullende verplichtingen voor online-marktplaatsen waar handelaren producten of diensten aanbieden aan consumenten

4.3.5.1 Inleiding

Afdeling 4 van hoofdstuk III van de verordening bevat verplichtingen voor aanbieders van online platforms die consumenten de mogelijkheid bieden overeenkomsten op afstand te sluiten met handelaren. Het betreft hier dus een subcategorie van de online platforms. De begrippen "consument" en "handelaar" zijn gedefinieerd in artikel 3, onderdelen c en f, van de verordening. Voor het begrip "overeenkomst op afstand" wordt verwezen naar de definitie van dat begrip in de richtlijn consumentenrechten.[70] Deze online platforms worden ook wel B2C online marktplaatsen

[68] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de regio's, 'Een digitaal decennium voor kinderen en jongeren: de nieuwe Europese strategie voor een beter internet voor kinderen (BIK+)', COM(2022) 212 final.
[69] Richtlijn (EU) 2018/1808 van het Europees Parlement en de Raad van 14 november 2018 tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten) in het licht van een veranderende marktsituatie (PbEU 2018, L 303).
70 Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad (PbEU 2011, L 304).

(B2C: *business to consumer*) genoemd, welk begrip hierna zal worden gebruikt. De verplichtingen uit afdeling 4 zijn niet van toepassing op B2C online marktplaatsen die kwalificeren als micro- of kleine onderneming (artikel 29 van de verordening). Zie voor een nadere toelichting op het begrip "micro- of kleine onderneming" paragraaf 4.3.4.1 van deze memorie van toelichting.

4.3.5.2 Traceerbaarheid van handelaren

Artikel 30, eerste lid, van de verordening bepaalt dat B2C online marktplaatsen ervoor moeten zorgen dat handelaren hun dienst enkel kunnen gebruiken voor het aanbieden van producten of diensten aan consumenten in de Unie, indien zij vooraf bepaalde informatie aan de aanbieder hebben verstrekt. De informatie heeft onder meer betrekking op de naam en contactgegevens van de handelaar, een kopie van een identificatiedocument en gegevens over de inschrijving in het handelsregister. Dit wordt ook wel een "*know your business customer* (KYBC)-verplichting" genoemd. Op grond van het tweede lid van artikel 30 van de verordening moeten de aanbieders vervolgens alles in het werk stellen om de betrouwbaarheid en volledigheid van de verstrekte informatie te beoordelen, bijvoorbeeld door gebruik te maken van officiële online databanken en online-interfaces zoals het handelsregister en het btw-uitwisselingssysteem. Handelaren die onjuiste informatie weigeren te verbeteren, moeten worden geschorst (artikel 30, derde lid, van de verordening).

Een deel van de informatie moet toegankelijk zijn voor de afnemers van de dienst (artikel 30, zevende lid, van de verordening). Dit stelt consumenten in staat om betrouwbare informatie te verkrijgen over met wie zij overeenkomsten sluiten via een online platform. Voor het overige kan de aanbieder van het online platform de informatie alleen verstrekken aan derden als de verplichting daartoe volgt uit ander recht, bijvoorbeeld omdat een rechter daartoe verplicht of omdat een bevoegde overheidsinstantie om inzage in de informatie verzoekt (artikel 30, zesde lid, van de verordening). Artikel 10 van de verordening is van toepassing op bevelen tot het verstrekken van dergelijke informatie (zie nader paragraaf 3.4.1 van deze memorie van toelichting).

4.3.5.3 Op conformiteit met Unierecht gericht ontwerp van de online-interface

Op grond van artikel 31, eerste lid, van de verordening moeten aanbieders van B2C online marktplaatsen hun online-interfaces zo ontwerpen en organiseren dat handelaren kunnen voldoen aan hun verplichtingen inzake het verstrekken van precontractuele informatie en informatie over productveiligheid en conformiteit. Dit wordt ook wel op conformiteit gericht ontwerp, ofwel "*compliance by design*" genoemd. Het gaat om informatieverplichtingen die zijn opgenomen in "het toepasselijke Unierecht", waarbij de markttoezichtverordening[71] in het bijzonder wordt genoemd. Verder kan gedacht worden aan de informatieverplichtingen die zijn neergelegd in de artikelen 6 en 8 van de richtlijn consumentenrechten[72], artikel 7 van de richtlijn OHP, de artikelen 5 en 6 van de richtlijn elektronische handel en artikel 3 van de richtlijn prijsaanduiding producten[73]. In aanvulling

[71] Verordening (EU) 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van producten en tot wijziging van Richtlijn 2004/42/EG en de Verordeningen (EG) nr. 765/2008 en (EU) nr. 305/2011 (PbEU 2019, L 169).

[72] Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad (PbEU 2011, L 304). Artikel 6 en 8 van deze richtlijn bevat informatievoorschriften voor overeenkomsten op afstand en buiten verkoopruimten gesloten overeenkomsten.

[73] Richtlijn 98/6/EG van het Europees Parlement en de Raad van 16 februari 1998 betreffende de bescherming van de consument inzake de prijsaanduiding van aan de consument aangeboden producten (PbEG 1998, L 080).

daarop wordt in het tweede lid van artikel 31 van de verordening bepaald dat de online-interface het voor handelaren mogelijk moet maken om ten minste informatie te verstrekken over de identificatie van de aangeboden producten of diensten, identificatietekens van de handelaar en informatie over etikettering en markering.

Het derde lid van artikel 31 van de verordening verplicht de aanbieders van B2C online marktplaatsen om alles in het werk te stellen om te beoordelen of een handelaar alle in het eerste en tweede lid bedoelde informatie heeft verstrekt. Dit moeten zij doen voordat zij de handelaar toestaan gebruik te maken van het online platform. Ook moeten deze aanbieders redelijke inspanningen leveren om steeksproefgewijs te controleren of de op hun platform aangeboden producten of diensten als illegaal zijn aangemerkt in een officiële en vrij toegankelijke onlinedatabank of online-interface. Bij dit laatste kan worden gedacht aan het Safety Gate Portal, het EU-systeem voor waarschuwingen afkomstig van nationale autoriteiten die verantwoordelijk zijn voor productveiligheid over producten die een risico vormen voor consumenten en professionele gebruikers.

De nieuwe verordening inzake algemene productveiligheid[74] bevat, wat betreft productveiligheid, specifieke voorschriften voor aanbieders van B2C online marktplaatsen ter invulling van de verplichtingen neergelegd in artikel 31 van de digitaledienstenverordening. De verordening inzake algemene productveiligheid, die kwalificeert als lex specialis ten opzichte van de digitaledienstenverordening, moet zo gelezen worden dat aanbieders van online marktplaatsen slechts aan artikel 31 van de digitaledienstenverordening kunnen voldoen als zij voldoen aan de in artikel 22, zevende en negende lid, van de verordening inzake algemene productveiligheid neergelegde verplichtingen. Dat laat onverlet dat zij ook aan de overige vereisten van artikel 31 van de digitaledienstenverordening moeten voldoen.

4.3.5.4 Plicht om consumenten te informeren over illegale producten of diensten

Indien aanbieders van B2C online marktplaatsen kennis krijgen van het feit dat een illegaal product of een illegale dienst via hun dienst wordt aangeboden, dan moeten zij op grond van artikel 32, eerste lid, van de verordening de consumenten die in de zes maanden daaraan voorafgaand een dergelijk product of dienst hebben gekocht via hun dienst, daarvan op de hoogte stellen en informatie verstrekken over de identiteit van de handelaar en de beschikbare verhaalmiddelen. Beschikt de aanbieder niet over de contactgegevens van alle betrokken consumenten, dan moet hij de informatie openbaar maken op zijn online-interface (artikel 32, tweede lid, van de verordening).

4.3.6 Aanvullende verplichtingen voor zeer grote online platforms en zeer grote online zoekmachines

4.3.6.1 Inleiding

De meest vergaande zorgvuldigheidsverplichtingen zijn neergelegd in afdeling 5 van hoofdstuk III van de verordening en gelden alleen voor aanbieders van “zeer grote online platforms” en “zeer grote online zoekmachines”. De eerste 17 zeer grote online platforms en 2 zeer grote online zoekmachines zijn op 25 april 2023 door de Commissie aangewezen.[75] Zeer grote online platforms, zoals Facebook,

---

Artikel 3 schrijft voor welke prijsinformatie moet worden vermeld voor producten die een verkoper aan de consument aanbiedt.

[74] Verordening (EU) 2023/988 van het Europees Parlement en de Raad van 10 mei 2023 inzake algemene productveiligheid, tot wijziging van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad en Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad, en tot intrekking van Richtlijn 2001/95/EG van het Europees Parlement en de Raad en Richtlijn 87/357/EEG van de Raad (PbEU 2023, L 135).

[75] Zie https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.

Amazon, YouTube, TikTok en Twitter, hebben een enorm bereik en spelen daarom een belangrijke rol in het faciliteren van het publieke debat, het doen van economische transacties en de verspreiding bij het publiek van informatie, meningen en ideeën. De rol van dit type dienstverleners is "systemisch" te noemen; zij zijn niet meer weg te denken uit het dagelijkse leven. Dergelijke platforms hebben daarmee veel invloed op de wijze waarop afnemers informatie online verkrijgen en doorgeven. Zeer grote online zoekmachines, zoals Google en Bing, spelen op hun beurt een cruciale rol bij het vinden en online beschikbaar maken van informatie.

De sterke invloed die zeer grote online platforms en zeer grote online zoekmachines kunnen hebben op de vorming van de publieke opinie en het publieke debat, op de online handel en op de online veiligheid, brengt ook risico's voor de samenleving met zich mee. Dit klemt temeer nu de manier waarop deze aanbieders hun diensten ontwerpen over het algemeen geoptimaliseerd is ten behoeve van hun (veelal op reclame gebaseerde) bedrijfsmodellen. Dit kan maatschappelijke problemen veroorzaken. Gelet op de potentiële risico's die het ontwerp, de werking en het gebruik van deze diensten met zich meebrengen, achtte de Uniewetgever het noodzakelijk om regels te stellen die de schadelijke maatschappelijke en economische gevolgen die zij kunnen veroorzaken te beperken.

4.3.6.2 Actieve afnemers

De afbakening van de categorie zeer grote online platforms en zeer grote online zoekmachines vindt plaats op basis van het bereik van de dienst, uitgedrukt in het aantal maandelijks actieve afnemers. De verordening legt de grens bij online platforms[76] en online zoekmachines[77] die gemiddeld 45 miljoen maandelijks actieve gebruikers hebben (artikel 33, eerste lid, van de verordening). Dat komt overeen met 10% van de bevolking van de Europese Unie. Artikel 33, tweede lid, van de verordening voorziet in een mechanisme om de drempelwaarde aan te passen bij aanmerkelijke schommelingen in het bevolkingsaantal.

Om het bereik van een online platform of een online zoekmachine te bepalen, moet het gemiddelde aantal actieve afnemers van elke dienst afzonderlijk worden vastgesteld (zie ook paragraaf 4.3.1 van deze memorie van toelichting). Op grond van artikel 24, tweede lid, van de verordening moeten alle online platforms en online zoekmachines hier halfjaarlijks over rapporteren met ingang van 17 februari 2023. Blijkens overweging 77 gaat het bij actieve afnemers van een online platform om alle afnemers die in de desbetreffende periode van zes maanden daadwerkelijk minstens eenmaal met de dienst in aanraking komen, doordat ze worden blootgesteld aan informatie die via de online-interface van dat platform wordt verspreid. Dat is bijvoorbeeld het geval wanneer ze dergelijke informatie bekijken of beluisteren, of wanneer zij zelf informatie verstrekken. Het begrip is dus niet beperkt tot geregistreerde gebruikers van een dienst, maar omvat elke gebruiker die blootgesteld wordt aan informatie die via het platform wordt verspreid. Wat online zoekmachines betreft, zijn actieve afnemers van de dienst degenen die informatie (zoekresultaten) op hun online-interface bekijken. Daaronder vallen niet de eigenaren van de websites die door de online zoekmachine zijn geïndexeerd, omdat zij de dienst niet actief gebruiken.

---

[76] Zie artikel 3, onderdeel i, van de verordening voor de definitie van "online platform". Zie ook paragraaf 2.4.5 van deze memorie van toelichting.

[77] Artikel 3, onderdeel j, van de verordening definieert een "online zoekmachine" als "een tussenhandeldienst die gebruikers de mogelijkheid biedt zoekopdrachten in te voeren om zoekacties uit te voeren op in beginsel alle websites of alle websites in een bepaalde taal, op basis van een zoekopdracht over eender welk onderwerp in de vorm van een trefwoord, een gesproken verzoek, een frase of andere input, en die resultaten in eender welk formaat oplevert met informatie over de opgevraagde inhoud". Zie ook paragraaf 2.4.6 van deze memorie van toelichting.

De precieze methodiek voor het vaststellen van het aantal actieve gebruikers kan door middel van een gedelegeerde handeling van de Commissie worden uitgewerkt (artikel 33, derde lid, van de verordening). Vooruitlopend daarop publiceerde de Commissie op 1 februari 2023 een aantal vragen en antwoorden over de identificatie en telling van het aantal actieve afnemers.[78]

4.3.6.3 Systeemrisico's

De verplichtingen in afdeling 5 van hoofdstuk III van de verordening draaien voor een belangrijk deel om de identificatie en beheersing van zogenaamde "systeemrisico's". Het gaat daarbij om risico's die het individu overstijgen en die de potentie hebben om de samenleving of economie als geheel ernstige schade toe te brengen. Op grond van de verordening zijn aanbieders van zeer grote online platforms en van zeer grote online zoekmachines verplicht om alle zogenaamde systeemrisico's die samenhangen met het ontwerp, de werking en de daaraan verbonden (algoritmische) systemen en het gebruik van hun diensten in kaart te brengen (artikel 34 van de verordening). Als zij, of de externe onafhankelijke auditors die dit ook moeten onderzoeken (artikel 37 van de verordening), vaststellen dat hun dienst(en) dergelijke systeemrisico's in zich hebben, dan moeten ze die aanpakken door daartoe maatregelen te nemen (artikel 35 van de verordening). Het kan daarbij onder meer gaan om het aanpassen van bepaalde kenmerken van de betrokken dienst, algoritmische systemen, inhoudsmoderatiesystemen, het nemen van bewustmakingsmaatregelen, het aanpassen van de algemene voorwaarden of interne processen en het samenwerken met betrouwbare flaggers. De risicobeoordeling moet jaarlijks worden doorlopen en daarnaast ook vóór de uitrol van functionaliteiten die waarschijnlijk kritieke gevolgen zullen hebben voor de in artikel 34 van de verordening genoemde systeemrisico's.

Meer specifiek zijn zeer grote online platforms en zeer grote online zoekmachines verplicht om de volgende vier categorieën systeemrisico's grondig te beoordelen:

1. Systeemrisico's die voortvloeien uit de verspreiding van illegale inhoud via hun diensten (artikel 34, eerste lid, onderdeel a, van de verordening). Hieronder vallen alle soorten misbruik van de diensten voor strafbare feiten of het uitvoeren van illegale activiteiten. Variërend van de verspreiding van kinderporno tot de verkoop van door het Unierecht of het nationale recht verboden producten of diensten, zoals gevaarlijke producten of namaakproducten. Gelet op de schaal waarop zeer grote online platforms en zeer grote online zoekmachines actief zijn, kan (de toegang tot) illegale inhoud zich snel en op grote schaal verspreiden, hetgeen een aanzienlijk systeemrisico kan vormen.
2. Een tweede categorie systeemrisico's betreft de werkelijke of voorzienbare negatieve effecten van de dienst op de uitoefening van de grondrechten, zoals die zijn beschermd door het Handvest. Artikel 34, eerste lid, onderdeel b, van de verordening noemt in dit verband (maar is niet beperkt tot) de menselijke waardigheid; de vrijheid van meningsuiting en van informatie, met inbegrip van de vrijheid en pluriformiteit van de media; het recht op een privéleven; het recht op gegevensbescherming; het recht op non-discriminatie; de rechten van het kind en de consumentenbescherming.[79] Grondrechtelijke risico's kunnen bijvoorbeeld voortvloeien uit misbruik van de dienst door het indienen van onjuiste meldingen of het ontwerp van algoritmische systemen. Het ontwerp van een algoritmisch systeem kan bijvoorbeeld een negatief effect hebben op de uitoefening van grondrechten doordat een algoritme systematisch discrimineert op sociaal-economische afkomst of huidskleur.

[78] https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers.
[79] De artikelen 1, 7, 8, 11, 21, 24 en 38 van het Handvest.

3. Een derde categorie systeemrisico's betreft werkelijke of voorzienbare negatieve effecten op de burgerdialoog en verkiezingsprocessen, en op de openbare veiligheid (artikel 34, eerste lid, onderdeel c, van de verordening). Hierbij kan bijvoorbeeld gedacht worden aan desinformatie die het verkiezingsproces beïnvloedt. Het recente verleden heeft immers laten zien dat zeer grote online platforms grote invloed kunnen hebben op – bijvoorbeeld – het verloop van verkiezingen en het organiseren van verstoringen van de openbare orde.
4. De vierde categorie systeemrisico's omvat de werkelijke of voorzienbare negatieve effecten met betrekking tot gendergerelateerd geweld, de bescherming van de volksgezondheid, minderjarigen en ernstige negatieve gevolgen voor het lichamelijke en geestelijke welzijn van een persoon (artikel 34, eerste lid, onderdeel d, van de verordening). Dergelijke risico's kunnen blijkens overweging 83 bijvoorbeeld voortvloeien uit online-interface-ontwerpen die gedragsverslavingen bij afnemers van de dienst kunnen stimuleren, of uit gecoördineerde desinformatiecampagnes.

Bij de tweede tot en met de vierde categorie systeemrisico's richt de verordening zich dus niet alleen op het bestrijden van illegale inhoud, maar ook op informatie die weliswaar legaal is, maar niettemin negatieve effecten kan hebben.

Bij de risicobeoordeling op grond van artikel 34 van de verordening moeten aanbieders rekening houden met de ernst van de potentiële impact en de waarschijnlijkheid van de systeemrisico's. Relevant in dit verband is bijvoorbeeld of de potentiële negatieve impact een groot aantal personen kan betreffen en of die potentieel onomkeerbaar is. Van belang is ook hoe moeilijk het is om die potentiële negatieve impact te verhelpen en de situatie van vóór de potentiële impact te herstellen. Op grond van het tweede lid moeten aanbieders bij het uitvoeren van de risicobeoordeling alle systemen en elementen van hun dienst in ogenschouw nemen die tot de systeemrisico's kunnen bijdragen, waaronder hun aanbevelingssystemen en algoritmes, hun inhoudsmoderatiesystemen, de toepasselijke algemene voorwaarden, hun reclamesystemen en datagerelateerde praktijken. Ook moet rekening worden gehouden met opzettelijke manipulatie van hun diensten. Hierbij valt onder meer te denken aan niet-authentiek gebruik of geautomatiseerde exploitatie, zoals het aanmaken van nepaccounts of het gebruik van bots, al dan niet door statelijke actoren.

Als aanbieders van zeer grote online platforms en zeer grote online zoekmachines vaststellen dat hun diensten dergelijke systeemrisico's in zich hebben dan moeten ze op grond van artikel 35 van de verordening redelijke, evenredige en doeltreffende risicobeperkende maatregelen treffen om de geïdentificeerde systeemrisico's te adresseren. Hierbij dient de aanbieder bijzondere aandacht te hebben voor de effecten van die maatregelen op de grondrechten. Deze risicobeheersingsregeling is een belangrijk novum voor de regulering van tussenhandeldiensten. Deze nieuwe aanpak moet in de komende jaren leiden tot een jaarlijkse evaluatie en herziening van de diensten van zeer grote online platforms en zeer grote online zoekmachines. De regeling maakt het mogelijk om elk jaar lessen te trekken en diensten naar aanleiding daarvan te verbeteren. De regeling is ook nieuw omdat ze zich richt op risico's die zich op het niveau van de samenleving en economie als geheel kunnen voordoen, in plaats van op individueel niveau.

4.3.6.4 Crisisresponsmechanisme

Artikel 36 van de verordening voorziet in een crisisresponsmechanisme. Het artikel geeft de Commissie bevoegdheden in relatie tot aanbieders van zeer grote online platforms en van zeer grote online zoekmachines in geval van een crisis. Daarvan is volgens het tweede lid sprake wanneer buitengewone omstandigheden leiden tot een ernstige bedreiging van de openbare veiligheid of de volksgezondheid in de Unie of in een aanzienlijk deel daarvan. De COVID-19-pandemie en de oorlog

in Oekraïne vormden de achtergrond voor deze bepaling. Het mechanisme houdt in dat aanbieders van zeer grote online platforms en zeer grote online zoekmachines door de Commissie, op aanbeveling van de digitaledienstenraad, kunnen worden verplicht om te onderzoeken in hoeverre hun diensten bijdragen aan een ernstige bedreiging van de openbare veiligheid of de volksgezondheid. Vervolgens kunnen zij worden verplicht de nodige maatregelen te nemen om die bedreiging(en) te voorkomen, weg te nemen of te beperken en om daarover verslag uit te brengen, zoals de in artikel 35 van de verordening genoemde risicobeperkingsmaatregelen, het prominent weergeven van informatie over de crisissituatie of het aanwijzen van een specifiek contactpunt voor crisisbeheer. De keuze van de specifieke maatregelen die moeten worden genomen, blijft berusten bij de aanbieder.

4.3.6.5 Transparantie met betrekking tot online reclame

Reclamesystemen van zeer grote online platforms en van zeer grote online zoekmachines brengen bijzondere risico's met zich mee. Om die reden moeten aanbieders van zeer grote online platforms en zeer grote online zoekmachines die reclame tonen op hun online-interface op grond van artikel 39 van de verordening een publiek toegankelijk en doorzoekbaar register bijhouden en beschikbaar stellen via hun online-interface. Deze verplichting geldt in aanvulling op de regels voor reclame die gelden voor alle aanbieders van online platforms, die is neergelegd in artikel 26 van de verordening (zie nader paragraaf 4.3.4.7 van deze memorie van toelichting). De registers moeten onder meer informatie bevatten over de inhoud en het onderwerp van de reclame, gegevens over de adverteerder en of de reclame gericht was op bepaalde groepen van afnemers van de dienst. Ook moet worden vermeld hoeveel afnemers de reclame heeft bereikt, opgesplitst per lidstaat. De registers dienen om het toezicht en onderzoek naar de opkomende risico's als gevolg van de verspreiding van online reclame te faciliteren (zie overweging 95 bij de verordening).

4.3.6.6 Aanbevelingssystemen

In aanvulling op de verplichtingen met betrekking tot aanbevelingssystemen voor aanbieders van alle online platforms (artikel 27 van de verordening; zie paragraaf 4.3.4.8 van deze memorie van toelichting) moeten aanbieders van zeer grote online platforms en zeer grote online zoekmachines op grond van artikel 38 van de verordening tenminste één optie aanbieden voor elk van hun aanbevelingssystemen die niet gebaseerd is op profilering in de zin van de AVG. Omdat zeer grote online platforms en zeer grote online zoekmachines vaak enorme hoeveelheden informatie bevatten en moeten kiezen welke daarvan te presenteren aan een gebruiker is het waarschijnlijk dat er in deze optie toch ordening van de informatie moet plaatsvinden om de dienst bruikbaar en overzichtelijk te houden. Dat kan dan bijvoorbeeld worden gedaan door chronologische, thematische, of alfabetische ordening van informatie, of aan de hand van het tijdstip van de dag.

4.3.6.7 Interne en externe controle op naleving van de verordening

De verordening voorziet zowel in intern als extern toezicht op de correcte naleving van de regels door aanbieders van zeer grote online platforms en zeer grote online zoekmachines. Artikel 37 van de verordening voorziet in de verplichting om jaarlijkse onafhankelijke externe controles (audits) te laten uitvoeren over de naleving van de verplichtingen in de verordening (artikel 37 van de verordening). Een gedelegeerde handeling over dit onderwerp is op het moment van schrijven in voorbereiding door de Europese Commissie.[80] Voor het interne toezicht verplicht artikel 41 van de verordening aanbieders om in hun organisatie te voorzien in een zogenoemde onafhankelijke

[80] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en.

compliancefunctie. De functionarissen die deze functie uitvoeren, moeten worden betrokken bij alle kwesties die verband houden met de verordening, waaronder bij de te verrichten risicobeoordeling en -beperking.

Artikel 40, eerste tot en met derde lid, van de verordening verplicht aanbieders van zeer grote online platforms en zeer grote online zoekmachines 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. Het betreft onder meer gegevens met betrekking tot algoritmen. Ook erkende onderzoekers moeten toegang tot gegevens van zeer grote online platforms en zeer grote online zoekmachines krijgen, om onderzoek te kunnen uitvoeren dat bijdraagt aan het opsporen, vaststellen en begrijpen van systeemrisico's (artikel 40, vierde tot en met zevende lid, van de verordening). Achtergrond van deze bepaling is dat door onderzoekers uitgevoerde studies naar de evolutie en de ernst van online systeemrisico's met name belangrijk zijn om een beter begrip hiervan te ontwikkelen. Dat is relevant voor aanbieders van online platforms en online zoekmachines zelf, voor hun gebruikers, bevoegde autoriteiten, de Commissie, politici, journalisten, onderzoekers, wetenschappers en het bredere publiek.

Onderzoekers die toegang willen tot informatie van zeer grote online platforms en zeer grote online zoekmachines moeten aan een aantal criteria voldoen (artikel 40, achtste lid, van de verordening). Zo moeten zij onder meer aantonen dat zij zijn aangesloten bij een onderzoeksorganisatie, onafhankelijk zijn van commerciële belangen, en dat zij in staat zijn om gegevensbeveiligings- en vertrouwelijkheidsvereisten in acht te nemen en persoonsgegevens te beschermen. De digitaledienstencoördinator toetst, na een aanvraag, of onderzoekers aan deze vereisten voldoen. Als dat zo is, dan kent deze de status van "erkend onderzoeker" toe.

4.3.6.8 Transparantie

Voor zeer grote online platforms en zeer grote online zoekmachines gelden ten slotte aanvullende transparantievereisten. In aanvulling op de rapportageverplichtingen neergelegd in de artikelen 15 en 24 van de verordening, moeten zij op grond van artikel 42 van de verordening ook rapporteren over de gemiddelde maandelijkse afnemers van de dienst voor elke lidstaat, uitgevoerde risicobeoordelingen en de daarop genomen risicobeperkende maatregelen.

4.3.7 Normen, gedragscodes en crisisprotocollen

Afdeling 6 van hoofdstuk III bevat diverse bepalingen over de ontwikkeling en uitvoering van vrijwillige normen en gedragscodes (de artikelen 44 en 45 van de verordening). De Commissie moet de totstandkoming van zulke normen en gedragscodes bevorderen en vergemakkelijken. Deelname aan dergelijke gedragscodes is vrijwillig. De verordening noemt in het bijzonder gedragscodes voor online reclame, toegankelijkheid en de aanpak van crises (de artikelen 46, 47 en 48 van de verordening).

De verordening probeert ook op andere manieren het gebruik van dergelijke vrijwillige normen en gedragscodes te stimuleren. Zo kan deelname aan een gedragscode voor minderjarigen een manier zijn om invulling te geven aan de verplichting om minderjarigen te beschermen (artikel 28 van de verordening) en om risicobeperkende maatregelen te nemen (artikel 35 van de verordening). Het belang van gedragscodes wordt ook onderstreept door het feit dat de externe audits (artikel 37 van de verordening) tevens moeten zien op de naleving van vrijwillige normen en gedragscodes. Hoewel deelname aan en uitvoering van vrijwillige normen en gedragscodes kan helpen bij het naleven van de verordening, houdt dit niet in dat daarmee automatisch de verordening wordt nageleefd (zie overweging 104 bij de verordening). Als de ondertekenaars een gedragscode systematisch niet

naleven, kunnen de Commissie en de digitaledienstenraad hen verzoeken de nodige maatregelen te nemen op grond van artikel 45, vierde lid, van de verordening. De eerder aangehaalde versterkte praktijkcode tegen desinformatie is een voorbeeld van een vrijwillige gedragscode die relevant is in het licht van artikel 45 van de verordening.

5 Uitvoering, samenwerking, toezicht en handhaving

5.1 *Inleiding*

Hoofdstuk IV van de verordening bevat bepalingen over de uitvoering van, het toezicht op en de handhaving van de verordening. Deze taken worden uitgevoerd door nationale autoriteiten en door de Europese Commissie. Het hoofdstuk voorziet ook in bepalingen over de samenwerking tussen verschillende bevoegde autoriteiten binnen één lidstaat, tussen de bevoegde autoriteiten van verschillende lidstaten en tussen nationale autoriteiten en de Commissie.

In paragraaf 5.2 van deze memorie van toelichting wordt ingegaan op de aanwijzing van de digitaledienstencoördinator en andere bevoegde autoriteiten in Nederland. In paragraaf 5.3 wordt vervolgens het toezicht en de handhaving toegelicht en in paragraaf 5.4 wordt tot slot ingegaan op de overige uitvoeringstaken op grond van de verordening. Daarbij wordt telkens eerst beschreven wat de verordening ter zake bepaalt en vervolgens op welke wijze de uitvoering in Nederland en in dit wetsvoorstel geschiedt.

5.2 *Aanwijzing digitaledienstencoördinator en andere bevoegde autoriteiten*

5.2.1 Inhoud verordening

Artikel 49, eerste lid, van de verordening schrijft voor dat de lidstaten een of meer bevoegde autoriteiten aanwijzen voor het toezicht op aanbieders van tussenhandeldiensten en de uitvoering van de verordening. Eén van die autoriteiten dient te worden aangewezen als zogenaamde digitaledienstencoördinator (artikel 49, tweede lid, van de verordening). De digitaledienstencoördinator is verantwoordelijk voor het toezicht en de handhaving van de verordening in die lidstaat, tenzij er andere bevoegde autoriteiten worden aangewezen voor delen van het toezicht en de handhaving. De digitaledienstencoördinator is bovendien verantwoordelijk voor de coördinatie van het toezicht en handhaving op nationaal niveau en draagt bij aan samenwerking op dit terrein op EU-niveau, samen met andere digitaledienstencoördinatoren, andere nationale bevoegde autoriteiten, de digitaledienstenraad en de Commissie. Als een lidstaat naast de digitaledienstencoördinator ook andere bevoegde autoriteiten aanwijst, dan moeten hun taken duidelijk afgebakend zijn en moeten zij nauw en doeltreffend samenwerken. Lidstaten kunnen voorts voorzien in samenwerking en regelmatige gedachtewisselingen tussen de digitaledienstencoördinator en andere nationale autoriteiten, die geen formele rol hebben bij de uitvoering van de verordening.

Artikel 50 van de verordening bevat de vereisten waaraan een autoriteit moet voldoen om te kunnen worden aangewezen als digitaledienstencoördinator. Op grond van artikel 49, vierde lid, van de verordening zijn deze vereisten ook van toepassing op de aanwijzing van andere bevoegde autoriteiten dan de digitaledienstencoördinator. Op grond van het eerste lid van artikel 50 moeten de aangewezen autoriteiten hun taken op een onpartijdige, transparante en tijdige wijze uitvoeren. Zij moeten over alle nodige middelen beschikken om hun taken uit te voeren, waaronder technische, financiële en personele middelen. De autoriteiten moeten voorts voldoende autonomie hebben bij het beheer van hun begroting, om hun onafhankelijkheid niet in het geding te brengen. In artikel 50, tweede lid, van de verordening wordt tot uitdrukking gebracht dat de autoriteiten volledig

onafhankelijk moeten kunnen handelen en dat zij vrij dienen te blijven van directe of indirecte externe beïnvloeding. Zij mogen ook geen instructies van enige andere overheidsinstantie of andere partij aanvaarden. Deze eisen doen geen afbreuk aan de mogelijkheden van rechterlijke toetsing en de algemene verantwoordingverplichtingen die op de autoriteiten rusten (artikel 50, derde lid, van de verordening).

5.2.2 Uitvoering in Nederland

5.2.2.1 Algemeen

De verordening stelt hoge eisen aan de onafhankelijkheid van de digitaledienstencoördinator en eventueel andere aan te wijzen bevoegde autoriteiten. Naar Nederlands recht ligt het in de rede dat de aan te wijzen autoriteiten zelfstandige bestuursorganen (zbo's) moeten zijn en dat voorts verschillende sturingsinstrumenten buiten toepassing verklaard moeten worden, die de verantwoordelijke minister ten aanzien van het door een zbo gevoerde beleid heeft op grond van de Kaderwet zelfstandige bestuursorganen. Het gaat met betrekking tot de uitvoering van de verordening en dit wetsvoorstel om het opstellen van beleidsregels, het vernietigen van een besluit van het zbo en het treffen van voorzieningen bij ernstige taakverwaarlozing. Dit laat onverlet dat de uitvoering van de taken op grond van dit wetsvoorstel in algemene zin onder de verantwoordelijkheid van de minister van Economische Zaken en Klimaat valt. Ook laten de bepalingen uit de verordening onverlet dat de leden van het bestuur van de zbo door de verantwoordelijke minister worden benoemd en dat de zbo's zich in algemene zin moeten verantwoorden over het gevoerde beleid en de besteding van de daarvoor toegekende middelen.

5.2.2.2 Aanwijzing ACM als digitaledienstencoördinator

Voorgesteld wordt om de ACM aan te wijzen als digitaledienstencoördinator (artikel 2.1, eerste lid, van het wetsvoorstel), belast met de uitvoering van de taken van de digitaledienstencoördinator op grond van de verordening en voor het toezicht op het grootste deel van de verplichtingen in de verordening.

De ACM is een zbo wier werkzaamheden tot doel hebben het bevorderen van goed functionerende markten, van ordelijke en transparante marktprocessen en van een zorgvuldige behandeling van consumenten (artikel 2, vijfde lid, van de Instellingswet Autoriteit Consument en Markt (hierna: Instellingswet ACM). 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 en de bepalingen in het BW ter implementatie van de richtlijn elektronische handel.[81] Voorts is de ACM de beoogde toezichthouder voor de *Platform-to-Business* (P2B-)verordening (zie hierover paragraaf 7.1.7) en de digitalemarktenverordening (zie hierover paragraaf 7.1.1).

Het thema "digitale economie" is voorts één van de drie thema's die de ACM tot prioriteit heeft bestempeld in haar meest recente uitvoeringsagenda.[82] Opdat alle mensen en bedrijven met vertrouwen gebruik kunnen maken van online markten, treedt de ACM in dat kader op tegen marktmacht (bijvoorbeeld van grote technologische bedrijven) en misleiding en manipulatie van consumenten. Hieronder valt bijvoorbeeld het gebruik van oneerlijke voorwaarden of algoritmes die

[81] De artikelen 15d en 15e van boek 3 en afdeling 2B van titel 5 van Boek 6 van het BW.
[82] "Focus Werkzaamheden ACM 2023", Acm.nl.

mensen sturen en beïnvloeden. Dit sluit aan bij het doel en de inhoud van de verordening. De ACM heeft in het kader van de Wet handhaving consumentenbescherming bovendien al de nodige ervaring met de uitvoering van een coördinerende rol in het kader van toezicht en handhaving. Om deze redenen acht het kabinet de ACM het meest geschikt om de rol van digitaledienstencoördinator uit te voeren onder de verordening.

Andere zbo's waarvan overwogen is om ze te belasten met de taken van de digitaledienstencoördinator zijn de AP en het Commissariaat voor de Media (hierna: CvdM). Zowel de AP als CvdM hebben expertise die relevant is voor de verordening, respectievelijk wat betreft de bescherming van persoonsgegevens en de vrijheid van meningsuiting en de pluriformiteit van de media. Het CvdM houdt bovendien toezicht op videoplatformdiensten in het kader van de uitvoering van de Mediawet 2008, die ook normadressaat zijn van de verordening. De reden om niet deze zbo's aan te wijzen als digitaledienstencoördinator is dat hun bestaande werkzaamheden en expertise slechts aansluiten op enkele onderdelen van de verordening. Om die reden sluiten, zoals hiervoor beschreven, de bestaande werkzaamheden en expertise van de ACM het beste aan op de verordening als geheel.

Op grond van het eerste lid van artikel 50 moeten de aangewezen autoriteiten over alle nodige middelen beschikken om hun taken uit te voeren, waaronder technische, financiële en personele middelen. In artikel 5, eerste lid, van de Instellingswet ACM is bepaald dat de minister van Economische Zaken en Klimaat voldoende personeel ter beschikking stelt aan de ACM voor de uitvoering van haar wettelijke taken. Op de financiële middelen die nodig zijn voor de uitvoering van taken op grond van dit wetsvoorstel door de ACM wordt nader ingegaan in paragraaf 8.2.4 van deze memorie van toelichting.

5.2.2.3 Aanwijzing AP als andere bevoegde autoriteit

De verordening streeft een hoog niveau van bescherming van grondrechten na, waaronder ook de bescherming van persoonsgegevens. Het gebruik en de bescherming van persoonsgegevens is derhalve onderdeel van een aantal bepalingen in de verordening. In een aantal gevallen verwijst de verordening nadrukkelijk naar begrippen die gedefinieerd zijn in de AVG. Waar de verordening regels stelt voor "profilering" of het gebruik respectievelijk het verwerken van bijzondere persoonsgegevens, is de AP de toezichthouder met de meest relevante inhoudelijk expertise en ervaring. Deze normen zijn bovendien verbijzonderingen van bestaande regels uit de AVG omtrent profilering en het gebruik van persoonsgegevens daarbij. Het toezicht op deze bepalingen ligt dus in het verlengde van de regels waar de AP reeds op toeziet. Om die reden wordt voorgesteld om de AP de bevoegde autoriteit te maken voor het toezicht op en de handhaving van de twee verboden in de verordening die betrekking hebben op het gebruik van profilering bij het tonen van reclames op online-interfaces van online platforms: de artikelen 26, derde lid, en 28, tweede lid, van de verordening (zie artikel 3.2, eerste lid, van het wetsvoorstel).

De AP voldoet als zbo ook aan de eisen die artikel 50 van de verordening aan bevoegde autoriteiten stelt. De betreffende vereisten komen ook grotendeels overeen met de eisen die op grond van artikel 52 van de AVG aan de nationale gegevensbeschermingsautoriteit worden gesteld, waaronder de eis dat de betreffende autoriteit haar taak in volledige onafhankelijkheid moet kunnen uitvoeren.

5.3 ***Toezicht en handhaving***

5.3.1 Afbakening bevoegdheid tot toezicht en handhaving

5.3.1.1 Inhoud verordening

Op grond van artikel 49, tweede lid, van de verordening is de door de lidstaat aangewezen digitaledienstencoördinator, samen met eventueel andere aangewezen bevoegde autoriteiten, verantwoordelijk voor alle kwesties die verband houden met het toezicht op e n de handhaving van de verordening in die lidstaat. Het toezicht en de handhaving richten zich op de verplichtingen die krachtens de verordening rechtstreeks rusten op de normadressaat van de verplichting. Dit zijn in hoofdzaak de aanbieders van tussenhandeldiensten. Het gaat hierbij om de verplichtingen zoals opgenomen in hoofdstuk III van de verordening (zie hoofdstuk 4 van deze memorie van toelichting) en enkele verplichtingen over de omgang met bevelen van bevoegde autoriteiten (artikelen 9 en 10 van de verordening; zie paragraaf 3.4 van deze memorie van toelichting). Als er meer autoriteiten bevoegd zijn voor het toezicht en de handhaving, dan moeten hun respectieve lijke taken duidelijk afgebakend zijn.

Artikel 56 van de verordening verduidelijkt hoe de bevoegdheid tot toezicht en handhaving is verdeeld tussen de verschillende lidstaten en tussen de lidstaten en de Commissie. Wat betreft de afbakening van bevoegdheden tussen de verschillende lidstaten is gekozen voor het zogenoemde "land-van-oorsprongsbeginsel", dat wil zeggen dat de lidstaat waar een aanbieder van tussenhandeldiensten zijn hoofdvestiging heeft, exclusief bevoegd is (artikel 56, eerste lid, van de verordening). In overweging 123 bij de verordening wordt verduidelijkt dat het gaat om de lidstaat waar de aanbieder zijn hoofdkantoor of wettelijke zetel heeft en waar de belangrijkste financiële en operationele controle wordt uitgeoefend. Indien een aanbieder van een tussenhandeldienst geen vestiging in de Unie heeft, dan is de lidstaat bevoegd waar de overeenkomstig artikel 13 van de verordening aangewezen wettelijke vertegenwoordiger verblijft of is gevestigd (artikel 56, zesde lid, van de verordening). Heeft een dergelijke aanbieder geen wettelijke vertegenwoordiger aangewezen, dan zijn alle lidstaten bevoegd (artikel 56, zevende lid, van de verordening).

Voor het toezicht op en de handhaving ten aanzien van aanbieders van zeer grote online platforms en zeer grote online zoekmachines is de Commissie bevoegd. Voor deze aanbieders is de Commissie *exclusief* bevoegd voor het toezicht op en de handhaving van de verplichtingen die uitsluitend voor deze aanbieders gelden, oftewel afdeling 5 van hoofdstuk III (artikel 56, tweede lid, van de verordening). De lidstaten hebben dus geen bevoegdheid tot toezicht en handhaving ten aanzien van deze verplichtingen. Ten aanzien van de overige verplichtingen waaraan ook zeer grote online platforms en zeer grote online zoekmachines moeten voldoen is zowel de lidstaat van de hoofdvestiging als de Commissie bevoegd tot toezicht en handhaving (artikel 56, derde en vierde lid, van de verordening). Daarbij geldt echter dat lidstaten deze bevoegdheid enkel hebben als de Commissie nog geen procedure heeft ingeleid voor dezelfde inbreuk. Overweging 125 bij de verordening stelt in dit verband dat de Commissie in veel gevallen beter in staat is om systemische inbreuken aan te pakken, zoals inbreuken die meerdere lidstaten treffen, ernstige herhaalde inbreuken of het niet instellen van doeltreffende mechanismen zoals de verordening vereist. De lidstaten worden geacht beter op te kunnen treden ten aanzien van individuele inbreuken, die geen aanleiding geven tot systemische of grensoverschrijdende problemen.

5.3.1.2 Uitvoering in Nederland en inhoud wetsvoorstel

In de artikelen 2.2 en 3.2 van het wetsvoorstel worden de bepalingen uit de verordening opgesomd ten aanzien waarvan de ACM respectievelijk de AP worden aangewezen als toezichthouder. Artikel 56 van de verordening heeft rechtstreekse werking en is dus van rechtswege van toepassing op de uitoefening van het toezicht en de handhaving door de ACM en de AP op grond van dit wetsvoorstel. Uit de toepassing van het land-van-oorsprongsbeginsel volgt dat de ACM en de AP bevoegd zullen zijn tot het houden van toezicht op en de handhaving ten aanzien van aanbieders van tussenhandeldiensten die hun hoofdvestiging in Nederland hebben, of aanbieders van

tussenhandeldiensten waarvan de wettelijke vertegenwoordiger in Nederland verblijft of is gevestigd. Hieruit volgt enerzijds dat de ACM en de AP bevoegd zullen zijn ten aanzien van overtredingen van de verordening die buiten Nederland worden begaan door in Nederland gevestigde aanbieders. Anderzijds zijn de ACM en de AP dus niet bevoegd ten aanzien van overtredingen die in Nederland worden begaan door in een andere lidstaat gevestigde aanbieders. Nederlandse afnemers van de tussenhandeldiensten van dergelijke aanbieders zijn in dat laatste geval dus aangewezen op de bevoegde autoriteiten in die andere lidstaten. Wat betreft de zeer grote online platforms en zeer grote online zoekmachines, die in sommige gevallen actief zijn in alle lidstaten van de EU, zijn de ACM en de AP dus bevoegd tot toezicht en handhaving als de aanbieders ervan hun hoofdvestiging of wettelijke vertegenwoordiger in Nederland hebben, behoudens de verordeningsbepalingen ten aanzien waarvan het toezicht en de handhaving exclusief bij de Commissie is belegd. Op het moment van schrijven van deze memorie van toelichting heeft de Commissie in elk geval één aanbieder van een zeer groot online platform aangewezen met een hoofdvestiging in Nederland.

Een deel van de verplichtingen waarvan wordt voorgesteld dat de ACM daar toezicht op zal houden, heeft betrekking op hoe een aanbieder op een zorgvuldige manier moet handelen als hij op de hoogte raakt van op zijn dienst aanwezige illegale inhoud of inhoud in strijd met zijn algemene voorwaarden. Zoals toegelicht in paragraaf 4.1 van deze memorie van toelichting, dient de beoordeling van de vraag of informatie illegaal is of in strijd met de algemene voorwaarden te geschieden op basis van het toepasselijke nationale of Unierecht of de toepasselijke algemene voorwaarden, en niet op basis van de verordening. Uit de afbakening van de bevoegdheden tussen de lidstaten volgt dat de ACM toezicht moet houden op de wijze waarop een in Nederland gevestigde aanbieder, als die in een andere lidstaat zijn diensten aanbiedt, omgaat met inhoud op zijn dienst die illegaal is volgens het recht van die lidstaat. Uit deze systematiek van de verordening volgt dan ook dat de toezichthoudende autoriteit bij de uitvoering van het toezicht niet hoeft, en ook niet kan, beoordelen of online inhoud illegaal is of in strijd met de algemene voorwaarden. Dat is aan de betrokkenen zelf en uiteindelijk aan de ter zake bevoegde rechter. De toezichthouder moet enkel toezien op naleving van de zorgvuldigheidsverplichtingen uit de verordening.

Bij het toezicht op en de handhaving van artikel 18 van de verordening is de situatie ingewikkelder. Op grond van dat artikel moeten aanbieders van tussenhandeldiensten strafbare feiten, waarbij het leven of veiligheid van personen wordt bedreigd, melden bij de rechtshandhavings- of gerechtelijke autoriteiten van de betrokken lidstaat of lidstaten. De verordening laat in het midden wat onder de "rechtshandhavings- of gerechtelijke autoriteit" moet worden verstaan. In Nederland worden dergelijke meldingen bij de politie gedaan. De ACM wordt verantwoordelijk voor het toezicht op de naleving van deze verplichting ten aanzien van in Nederland gevestigde aanbieders. De informatie dat deze verplichting is overtreden, zal over het algemeen komen van de rechtshandhavings- en gerechtelijke autoriteiten in kwestie. Dit kunnen dus ook autoriteiten in andere lidstaten zijn. De ACM zal immers doorgaans zelf niet (kunnen) vaststellen of een aanbieder van hostingdiensten kennis heeft of had van informatie die aanleiding geeft tot een vermoeden dat een strafbaar feit waarbij het leven of de veiligheid wordt bedreigd is, wordt of waarschijnlijk zal worden gepleegd. De bepalingen uit de verordening inzake samenwerking tussen autoriteiten (zie nader paragraaf 6.1 van deze memorie van toelichting), zullen in dat geval uitkomst moeten bieden. In het geval de ACM op andere wijze kennis krijgt van informatie die erop duidt dat een aanbieder deze verplichting heeft overtreden, dan zal de ACM ook een beroep moeten kunnen doen op de betreffende rechtshandhavings- en gerechtelijke autoriteiten om te beoordelen of inderdaad sprak is van een strafbaar feit waarbij het leven of veiligheid van personen wordt bedreigd dat niet is gemeld bij die autoriteiten. De ACM is immers niet in staat om zelf die beoordeling te maken.

Gelet op de aard van de meldplicht van artikel 18 van de verordening, zal het toezicht op de naleving van dit artikel in de praktijk vooral reactief van aard zijn. De ACM zal immers doorgaans zelf niet kunnen vaststellen of een aanbieder van hostingdiensten kennis heeft of had van informatie die aanleiding geeft tot een vermoeden dat een strafbaar feit waarbij het leven of veiligheid wordt bedreigd is, wordt of waarschijnlijk zal worden gepleegd. Informatie hierover zal de ACM in de praktijk achteraf krijgen van de bevoegde rechtshandhavings- en gerechtelijke autoriteiten, die in het kader van een strafrechtelijk onderzoek vaststelt dat de hostingaanbieder beschikte over relevante informatie die hij niet heeft gemeld. Die autoriteiten zijn ook het beste in staat om te beoordelen of bepaalde informatie duidt op een strafbaar feit waarbij het leven of de veiligheid van een persoon of personen wordt bedreigd. Voor handhaving van en toezicht op de meldplicht zal de ACM dus in elk geval nauw moeten samenwerken en gegevens moeten uitwisselen met de politie en het openbaar ministerie (hierna: OM) om te kunnen vaststellen of een aanbieder van hostingdiensten aan deze plicht voldoet.

5.3.2 Onderzoeksbevoegdheden

5.3.2.1 Inhoud verordening

De digitaledienstencoördinator en andere bevoegde autoriteiten moeten op basis van de verordening beschikken over drie onderzoeksbevoegdheden met betrekking tot het gedrag van aanbieders van tussenhandeldiensten (artikel 51, eerste lid, van de verordening). In de eerste plaats gaat het om de bevoegdheid om personen te verzoeken om informatie over een vermeende inbreuk te verstrekken (onderdeel a). In de tweede plaats gaat het om de bevoegdheid om inspecties uit te voeren in bedrijfsruimten van aanbieders van tussenhandeldiensten, met het doel om informatie over een vermeende inbreuk te onderzoeken of in beslag te nemen (onderdeel b). In de derde plaats gaat het om de bevoegdheid om werknemers of vertegenwoordigers van aanbieders van tussenhandeldiensten te verzoeken om uitleg te geven over informatie over een vermeende inbreuk (onderdeel c). Uit de formulering van artikel 51, eerste lid, van de verordening volgt dat deze opsomming van bevoegdheden limitatief van aard is; dat wil zeggen dat lidstaten in hun nationale recht geen andere bevoegdheden kunnen toekennen aan hun bevoegde autoriteiten dan de hier genoemde. Lidstaten zijn wel gehouden om specifieke regels, procedures en waarborgen vast te leggen voor de uitoefening van deze bevoegdheden (artikel 51, zesde lid, van de verordening).

5.3.2.2 Uitvoering in Nederland en inhoud wetsvoorstel

De toezichthoudende ambtenaren van de ACM en de AP beschikken op grond van titel 5.2 van de Algemene wet bestuursrecht (Awb) over een aantal standaard onderzoeksbevoegdheden die zij kunnen inzetten bij het uitoefenen van hun toezichtstaak op grond van dit wetsvoorstel. Deze standaard onderzoeksbevoegdheden komen grotendeels overeen met de bevoegdheden waarover zij op grond van artikel 51, eerste lid, van de verordening dienen te beschikken. De bevoegdheid tot het vorderen van informatie (artikel 51, eerste lid, onderdelen a en c van de verordening) komt overeen met de bevoegdheid tot het vorderen van inlichtingen (artikel 5:16 van de Awb). Het vorderen van inzage van een identiteitsbewijs (artikel 5:16a van de Awb) ligt in het verlengde van deze bevoegdheid. De bevoegdheid om inspecties uit te voeren in bedrijfsruimten van aanbieders van tussenhandeldiensten, met het doel om informatie over een vermeende inbreuk te onderzoeken of in beslag te nemen (onderdeel b van artikel 51, eerste lid, van de verordening) komt overeen met de bevoegdheid om inzage te vorderen in zakelijke gegevens en bescheiden, daarvan kopieën te maken en deze korte tijd mee te nemen (artikel 5:17 van de Awb), de bevoegdheid om zaken te onderzoeken (artikel 5:18 van de Awb) en de bevoegdheid om plaatsen, anders dan woningen

zonder toestemming van de bewoner, te betreden, zo nodig met behulp van de sterke arm (artikel 5:15 Awb).

De bevoegdheid om inspecties uit te voeren heeft betrekking op gebouwen die "aanbieders van tussenhandeldiensten of andere personen gebruiken voor met hun handel, bedrijf, ambacht of beroep verband houdende doeleinden" (artikel 51, eerste lid, onderdeel b, van de verordening), kort gezegd bedrijfsruimten. Uit de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) over het in artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) vervatte recht op respect voor de woning volgt evenwel dat ook bedrijfsruimten onder het begrip "woning" in de zin van artikel 8 van het EVRM kunnen vallen.[83] De ACM en de AP dienen dus ook over de bevoegdheid te beschikken om woningen te betreden, als dat nodig is om de onderzoeksbevoegdheid genoemd in artikel 51, eerste lid, onderdeel b, van de verordening uit te oefenen. De toezichthoudende ambtenaren van de ACM beschikken op grond van artikel 12c van de Instellingswet ACM reeds over de bevoegdheid tot het binnentreden van woningen zonder toestemming van de bewoner. Voor de toezichthoudende ambtenaren van de AP is die bevoegdheid opgenomen in artikel 3.2, derde lid, van dit wetsvoorstel.

Artikel 5:19 van de Awb kent aan toezichthoudende ambtenaren de bevoegdheid toe om vervoermiddelen te onderzoeken, bijvoorbeeld omdat hij met betrekking tot deze vervoermiddelen een toezichthoudende taak heeft of daarmee zaken worden vervoerd met betrekking waartoe hij een toezichthoudende taak heeft. Deze bevoegdheid komt niet terug in artikel 51, eerste lid, van de verordening. Dit is, gelet op het feit dat de verordening online tussenhandeldiensten reguleert, ook niet vreemd. Omdat de in de verordening opgenomen opsomming van onderzoeksbevoegdheden limitatief van aard is, is de bevoegdheid tot het onderzoeken van vervoermiddelen uitgesloten in de artikelen 2.2, tweede lid, en 3.2, tweede lid, van dit wetsvoorstel.

5.3.3 Verbindendverklaring toezeggingen en bindende aanwijzingen

5.3.3.1 Inhoud verordening

Het tweede lid van artikel 51 van de verordening bevat de handhavingsbevoegdheden waar de bevoegde autoriteiten over dienen te beschikken. Net als bij de onderzoeksbevoegdheden in het eerste lid van dat artikel, betreft het een opsomming die limitatief van aard is. Uit de aanhef van het artikel volgt dat de handhavingsbevoegdheden enkel kunnen worden toegepast met betrekking tot aanbieders van tussenhandeldiensten die onder de bevoegdheid van de betreffende lidstaat vallen.

Ingevolge artikel 51, tweede lid, onderdeel a, van de verordening moeten de bevoegde autoriteiten beschikken over de bevoegdheid om door aanbieders gedane toezeggingen over de naleving van de verordening te aanvaarden en om die toezeggingen verbindend te maken. Op grond van artikel 51, tweede lid, onderdeel b, van de verordening moeten de bevoegde autoriteiten over de bevoegdheid beschikken om de stopzetting van inbreuken te bevelen en passende, proportionele en noodzakelijke remedies op te leggen om de inbreuk daadwerkelijk te beëindigen.

5.3.3.2 Uitvoering in Nederland en inhoud wetsvoorstel

De Instellingswet ACM kent de ACM een aantal handhavingsbevoegdheden toe in het kader van het toezicht op en de handhaving van de wettelijke voorschriften waarmee de ACM is belast. Het betreft onder meer de bevoegdheid tot het bindend verklaren van een toezegging (artikel 12h van de

[83] EHRM 16 april 2002, ECLI:CE:ECHR:2002:0416JUD003797197 (Colas Est) en HvJ EG 22 oktober 2002, zaak C-94/00, ECLI:EU:C:2002:603 (Roquette Frères). Zie ook: EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800 en (Niemetz) en EHRM 30 maart 1989, ECLI:NL:XX:1989:AD0700 (Chapell).

Instellingswet ACM) en het opleggen van een bindende aanwijzing (artikel 12j van de Instellingswet ACM). De ACM zal deze bevoegdheden ook kunnen inzetten ten behoeve van de uitvoering van haar taken op grond van dit wetsvoorstel, wanneer dat verheven is tot wet. De bevoegdheid daartoe vloeit rechtstreeks voort uit de Instellingswet ACM en er bestaat derhalve geen noodzaak om daarover iets te regelen in onderhavig wetsvoorstel. De AP beschikt op basis van bestaande wetgeving niet over een grondslag om de hierboven genoemde bevoegdheden bij de uitvoering van dit wetsvoorstel toe te passen. Om die reden kennen de artikelen 3.5 en 3.6, eerste lid, van dit wetsvoorstel de AP die bevoegdheden toe.

5.3.4 Voorlopige maatregelen bij ernstige schade

5.3.4.1 Inhoud verordening

Artikel 51, tweede lid, onderdeel e, van de verordening bepaalt dat de bevoegde autoriteiten bevoegd moeten zijn om voorlopige maatregelen te nemen om het gevaar van ernstige schade te voorkomen. Uit de aanhef van het artikellid volgt dat de voorlopige maatregel moet worden genomen met betrekking tot aanbieders van tussenhandeldiensten. Blijkens overweging 114 bij de verordening kunnen dergelijke voorlopige maatregelen de vorm hebben van bevelen om een bepaalde vermeende inbreuk te beëindigen of te verhelpen. Deze bevelen mogen niet verder gaan dan wat nodig is om ernstige schade te voorkomen in afwachting van een definitieve beslissing. Het gaat bij deze maatregelen dus om situaties waarin nog niet definitief is vastgesteld dat er een inbreuk op een verplichting uit de verordening heeft plaatsgevonden. Onderdeel e zou zo kunnen worden gelezen dat de bevoegde autoriteit zelf de voorlopige maatregel moet uitvoeren, maar uit de voornoemde overweging bij de verordening kan worden afgeleid dat dit niet de bedoeling van de Uniewetgever is. Een dergelijke lezing zou ook niet passen bij de aard van de verplichtingen van de verordening, waarvan het niet goed voorstelbaar is dat de bevoegde autoriteit zelf een maatregel zou uitvoeren om een dreigende inbreuk ongedaan te maken.

5.3.4.2 Uitvoering in Nederland en inhoud wetsvoorstel

Het instrument van de voorlopige maatregel is als volgt in het wetsvoorstel verankerd. In de artikelen 2.5, eerste lid, onderdeel a, en 3.6, tweede lid, onderdeel a, van het wetsvoorstel is bepaald dat de ACM en de AP bevoegd zijn om een voorlopige maatregel in de zin van de verordening op te leggen. Hiervoor wordt gebruik gemaakt van de figuur van de zelfstandige last (artikel 5:2, tweede lid, Awb). In het geval deze last niet wordt nageleefd, kunnen de ACM en de AP een last onder dwangsom of bestuurlijke boete opleggen (artikel 12m van de Instellingswet ACM in samenhang met artikel 2.3 van het wetsvoorstel en artikel 3.3 van het wetsvoorstel).

5.3.5 Maatregelen bij ernstige en aanhoudende inbreuken

5.3.5.1 Inhoud verordening

Artikel 51, derde lid, van de verordening voorziet in de bevoegdheid om maatregelen op te leggen in het geval alle handhavingsbevoegdheden uit het tweede lid van dat artikel zijn uitgeput en de inbreuk niet is verholpen of blijft bestaan. Ook moet de inbreuk ernstige schade veroorzaken die niet kan worden vermeden door de uitoefening van andere bevoegdheden die beschikbaar zijn uit hoofde van het Unierecht en het nationale recht. Blijkens overweging 119 bij de verordening gaat het om bijzonder ernstige en aanhoudende inbreuken op de verordening. Als voorbeelden van bevoegdheden die beschikbaar zijn op grond van ander recht worden daar genoemd maatregelen om de collectieve belangen van consumenten te beschermen, om webpagina's die kinderpornografie bevatten of verspreiden snel te laten verwijderen of om diensten ontoegankelijk te maken die door

een derde worden gebruikt om inbreuk te maken op intellectuele eigendomsrechten. Artikel 51, derde lid, van de verordening heeft dus betrekking op de situatie dat de dienst van een aanbieder wordt gebruikt voor het opslaan of verspreiden van illegale inhoud die ernstige schade veroorzaakt en waarin de aanbieder, door de verplichtingen uit de verordening aanhoudend niet na te komen, bijdraagt aan het voortbestaan van die situatie.

De maatregelen die in dat geval kunnen worden opgelegd zijn de volgende. In de eerste plaats kan de digitaledienstencoördinator een maatregel opleggen aan de aanbieder van een tussenhandeldienst waarmee van het leidinggevende orgaan van de aanbieder wordt geëist dat zij de situatie onverwijld onderzoekt, een actieplan met de nodige maatregelen vaststelt en indient, ervoor zorgt dat die maatregelen worden genomen en rapporteert over de genomen maatregelen (artikel 51, derde lid, onderdeel a, van de verordening). Wanneer de aanbieder van de tussenhandeldienst ook een dergelijke opgelegde maatregel niet voldoende naleeft, de inbreuk blijft bestaan en ernstige schade blijft veroorzaken, en de inbreuk bovendien neerkomt op een strafbaar feit waarbij het leven of de veiligheid van personen wordt bedreigd, dan is de digitaledienstencoördinator bevoegd om de "bevoegde gerechtelijke autoriteit" te verzoeken om de maatregel genoemd in onderdeel b van artikel 51, derde lid, van de verordening op te leggen in de vorm van een tijdelijke beperking van de toegang tot de dienst. De verordening laat in het midden wat onder de "bevoegde gerechtelijke autoriteit" moet worden verstaan; het is dus aan de lidstaten om hier in hun nationale recht invulling aan te geven.[84]

Het begrip "strafbaar feit waarbij het leven of de veiligheid van personen wordt bedreigd" lijkt te verwijzen naar zware, strafrechtelijk gesanctioneerde misdrijven. Daarnaast verwijst overweging 56 bij de verordening naar de strafbare feiten genoemd in Richtlijn 2011/36/EU[85], Richtlijn 2011/93/EU[86] of Richtlijn (EU) 2017/541[87]. Een logische lezing van deze bepaling is dat de inbreuk op de verordening door een aanbieder verband moet houden met dergelijke zware delicten, in de vorm van illegale inhoud die via de dienst in kwestie wordt verspreid of opgeslagen. Te denken valt aan kinderpornografie die doorlopend via een platform beschikbaar blijft. De verordening geeft niet aan volgens welk recht er sprake moet zijn van een strafbaar feit: het recht van de lidstaat van vestiging van de aanbieder, het recht van de staat waar het strafbare feit is gepleegd of beide.

De maatregel in artikel 51, derde lid, onderdeel b, van de verordening houdt in dat de toegang van afnemers tot de betrokken dienst tijdelijk wordt beperkt. Als dat technisch niet haalbaar is, dan kan de bevoegde autoriteit verzoeken om de toegang tot de online-interface van de dienst tijdelijk te beperken. Het gaat dus om het tijdelijk beperken van de toegang tot de gehele dienst die bij de inbreuk is betrokken, of de online-interface daarvan. Bij dit laatste kan worden gedacht aan het laten blokkeren van de website die toegang biedt tot de betreffende tussenhandeldienst. Een dergelijk bevel moet gericht worden tot de aanbieder van tussenhandeldiensten die in een redelijke positie

---

[84] Zie ook artikel 51, zesde lid, van de verordening, op grond waarvan lidstaten specifieke regels en procedures moeten vastleggen voor de uitoefening van de bevoegdheden krachtens het eerste, tweede en derde lid van dat artikel.

[85] Richtlijn 2011/36/EU van het Europees Parlement en de Raad van 5 april 2011 inzake de voorkoming en bestrijding van mensenhandel en de bescherming van slachtoffers daarvan, en ter vervanging van Kaderbesluit 2002/629/JBZ van de Raad (PbEU 2011, L 101).

[86] Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PbEU 2011, L 335).

[87] Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad (PbEU 2017, L 88).

verkeert om die doelstelling te verwezenlijken zonder de toegang tot wettige informatie onnodig te beperken, zoals de berokken aanbieder van de hostingdienst, de internetdienst, het domeinregister of een registrerende instantie (overweging 120).

Deze maatregel moet dus worden onderscheiden van maatregelen die betrekking hebben op de toegang tot specifieke illegale inhoud. De verordening bepaalt niet aan wie de maatregel moet worden opgelegd. Dat betekent dat de maatregel niet enkel kan worden opgelegd aan de aanbieder van de tussenhandeldienst, 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, of andere dienstaanbieder in de keten zijn.

De maatregel kan worden opgelegd voor een termijn van vier weken. De gerechtelijke autoriteit kan bepalen dat de digitaledienstencoördinator de duur van de maatregel een bepaald aantal malen met vier weken kan verlengen, als de aanbieder heeft nagelaten om de nodige maatregelen ter beëindiging van de inbreuk te nemen en als dit geen onevenredige nadelige gevolgen heeft voor de afnemers van de dienst. Indien de digitaledienstencoördinator de termijn niet verder kan verlengen, dient hij een nieuw verzoek in bij de gerechtelijke autoriteit.

Zoals ook in overweging 119 van de verordening wordt opgemerkt, heeft deze maatregel nadelige gevolgen voor de rechten en belangen van derden. Ook de inhoud van derden die geen verband houdt met een strafbaar feit waarbij het leven of de veiligheid van personen wordt bedreigd wordt immers geraakt door de tijdelijke toegangsbeperking. Dit heeft onder meer gevolgen voor de vrijheid van meningsuiting en de vrijheid van informatie. Artikel 51, derde lid, van de verordening bevat daarom een aantal procedurele voorschriften voor het toepassen van de maatregel. Zo moeten belanghebbenden in de gelegenheid worden gesteld om voorafgaand schriftelijke opmerkingen te maken. De aanbieder van de tussenhandeldienst, de geadresseerden van de maatregel en derden met een legitiem belang mogen verder deelnemen aan de procedure bij de bevoegde gerechtelijke autoriteit. De opgelegde maatregelen moeten in verhouding staan tot de aard, de ernst, de herhaling en de duur van de inbreuk, zonder onnodige beperking van toegang tot wettelijke informatie door afnemers van de betrokken dienst.

5.3.5.2 Uitvoering in Nederland en inhoud wetsvoorstel

De bevoegdheid voor de ACM en de AP als bedoeld in artikel 51, derde lid, onderdeel a, van de verordening is in het wetsvoorstel op dezelfde wijze vormgegeven als de bevoegdheid om een voorlopige maatregel op te leggen, dus in de vorm van de bevoegdheid tot het opleggen van een zelfstandige last in de zin van artikel 5:2, tweede lid, van de Awb (de artikelen 2.5, eerste lid, onderdeel b, en 3.6, tweede lid, onderdeel b, van het wetsvoorstel). In het geval de last niet wordt nageleefd, kunnen de ACM en de AP een last onder dwangsom of bestuurlijke boete opleggen (artikel 12m van de Instellingswet ACM in samenhang met artikel 2.3 van het wetsvoorstel en artikel 3.3 van het wetsvoorstel), waarover hieronder in paragraaf 5.3.6 van deze memorie van toelichting meer.

Voorgesteld wordt om de procedure voor het opleggen van een maatregel als bedoeld in artikel 51, derde lid, onderdeel b, van de verordening bestuursrechtelijk vorm te geven. In de artikelen 2.5 en 2.6 van het wetsvoorstel is daartoe bepaald dat de ACM bevoegd zal zijn tot het opleggen van deze maatregel, na machtiging daartoe van de rechter-commissaris. Voor deze bestuursrechtelijke vormgeving is gekozen omdat deze maatregel het sluitstuk is van een bestuursrechtelijk handhavingstraject. De maatregel wordt immers opgelegd bij ernstige en herhaalde overtredingen waarbij de inzet van andere bestuursrechtelijke sancties onvoldoende effectief is gebleken. In het Nederlandse bestuursrecht is het evenwel altijd het bestuursorgaan dat dergelijke maatregelen

oplegt, niet een gerechtelijke autoriteit. Om invulling te geven aan de verplichting uit de verordening dat de maatregel voorafgaand wordt beoordeeld door een gerechtelijke autoriteit, is voorzien in voorafgaande machtiging van de rechter-commissaris, belast met de behandeling van strafzaken bij de rechtbank Rotterdam (artikel 2.6, eerste lid, van het wetsvoorstel). Deze machtiging is een rechtsfiguur die ook in andere wetgeving wordt voorgeschreven bij het nemen van dit soort bestuursrechtelijke maatregelen, vanwege de ingrijpende gevolgen van de maatregel voor de grondrechten van betrokkenen en vanwege de samenhang met het strafrecht.[88]

Een alternatieve vormgeving van deze maatregel die bij het opstellen van onderhavig wetsvoorstel is overwogen, is om de officier van justitie bevoegd te maken tot het opleggen ervan. De officier van justitie is immers te beschouwen als een gerechtelijke autoriteit en de betrokkenheid van het OM ligt hoe dan ook in de rede vanwege de relatie tussen deze maatregel en strafbare feiten die het leven of de veiligheid van personen bedreigen. Er is niet gekozen voor deze optie, omdat de maatregel niet wordt opgelegd in het kader van een strafvorderlijk onderzoek naar strafbare feiten, waar de officier van justitie een centrale rol heeft, maar in het kader van een bestuursrechtelijk handhavingstraject, waar de ACM als digitaledienstencoördinator de bevoegde autoriteit is. Voorts past de positie van belanghebbenden in het totstandkomingsproces van de maatregel beter in het bestuursrecht dan in het strafrecht. Gezien de raakvlakken die de maatregel heeft met het bestuursrecht en het strafrecht, ligt het eveneens niet in de rede om de civiele rechter een rol te geven bij het nemen van deze maatregel.

De maatregel genoemd in artikel 51, derde lid, onderdeel b, van de verordening is een ultimum remedium. Pas als de uitoefening van andere (bestuursrechtelijke en strafrechtelijke) bevoegdheden geen soelaas biedt, komt deze maatregel aan bod. Gelet op de sterke relatie van deze bevoegdheid met strafvorderlijk optreden, kan de ACM op grond van artikel 2.5, derde lid, van het wetsvoorstel advies vragen aan het OM. Ten eerste kan de ACM aan het OM vragen of het OM door uitoefening van andere bevoegdheden de schade kan vermijden. Ten tweede is het, gezien haar expertise, passend dat het OM adviseert of sprake is van een strafbaar feit waarbij het leven of de veiligheid van personen wordt bedreigd. Het ligt in de rede dat deze advisering het sluitstuk is van een samenwerkingstraject tussen de ACM en het OM met betrekking tot dit soort gevallen.

Voordat de ACM een verzoek om afgifte van de machtiging indient, verzoekt zij de belanghebbenden om schriftelijke opmerkingen in te dienen (artikel 51, derde lid, tweede alinea, van de verordening).[89] In dit verzoek omschrijft de ACM de voorgenomen maatregel en de geadresseerden van de maatregel. De aanbieder van tussenhandeldiensten, de geadresseerden van de maatregel en eventuele derden met een legitiem belang dienen op grond artikel 51, derde lid, tweede alinea, van de verordening voorts deel te kunnen nemen aan de procedures voor de bevoegde gerechtelijke autoriteit. Daartoe is in artikel 2.6, tweede lid, van het wetsvoorstel bepaald dat de rechter-commissaris bovengenoemde partijen kan horen alvorens te beslissen. De ACM heeft de mogelijkheid om tegen de beslissing van de rechter-commissaris om het verzoek niet toe te wijzen beroep in te stellen bij de rechtbank Rotterdam, sector strafrecht (artikel 2.6, vijfde lid, van het wetsvoorstel). Belanghebbenden kunnen bezwaar en beroep instellen tegen oplegging van de maatregel zelf. De machtiging van de rechter-commissaris kan in deze procedure betrokken worden. Nadat de machtiging is afgegeven door de rechter-commissaris, legt de ACM de maatregel op in de

[88] Zie onder meer artikel 2.7 van de Wet handhaving consumentenbescherming en artikel 15.7c van de Telecommunicatiewet.
[89] Dit geldt niet als de ACM handelt op verzoek van de Commissie. Zie hierover paragraaf 5.3.10.1.

vorm van een zelfstandige last. Indien de geadresseerde niet overeenkomstig die last handelt, kan de ACM een bestuurlijke boete of een last onder dwangsom opleggen.

Het wetsvoorstel voorziet niet in de bevoegdheid voor de AP tot het opleggen van een maatregel als bedoeld in artikel 51, derde lid, onderdeel b, van de verordening. Gelet op het feit dat de AP alleen toeziet op de naleving van bepalingen van de verordening die betrekking hebben op een verbod op het gebruik van profileringstechnieken bij het tonen van reclames op online-interfaces, zal de AP deze bevoegdheid niet nodig hebben om haar taak uit hoofde van de verordening uit te voeren. Bij overtredingen van die bepalingen zal immers nooit sprake zijn van een verband met strafbare feiten waarbij het leven of de veiligheid van personen wordt bedreigd.

5.3.6 Boete en dwangsom

5.3.6.1 Inhoud verordening

In artikel 51, tweede lid, onderdelen c en d, van de verordening worden de boete en de dwangsom genoemd als handhavingsmaatregelen die de bevoegde autoriteiten moeten kunnen opleggen aan aanbieders van tussenhandeldiensten. Een dwangsom moet kunnen worden opgelegd om ervoor te zorgen dat een inbreuk wordt beëindigd in overeenstemming met een bevel daartoe op grond van artikel 51, tweede lid, onderdeel b, van de verordening. De boete en de dwangsom moeten ook kunnen worden opgelegd wegens niet-naleving van krachtens het eerste lid van artikel 51 verstrekte onderzoeksbevelen en in dat geval kan de boete of dwangsom ook worden gericht aan de personen tot wie het bevel is gericht. Dit kan iemand anders zijn dan de aanbieder van de tussenhandeldienst (zie de laatste alinea van artikel 51, tweede lid, van de verordening).

Op grond van artikel 52, eerste lid, van de verordening moeten de lidstaten voorzien in voorschriften inzake de sancties die gelden voor inbreuken op de verordening door aanbieders van tussenhandeldiensten en moeten zij ervoor zorgen dat die sancties in overeenstemming met artikel 51 worden toegepast. De sancties moeten doeltreffend, evenredig en afschrikkend zijn (artikel 52, tweede lid, van de verordening). De maximale hoogte van de boete en de dwangsom worden bepaald in artikel 52, derde en vierde lid, van de verordening, en zijn voor de boete bepaald op een percentage van de wereldwijde jaaromzet van de aanbieder van de tussenhandeldienst, waarbij gedifferentieerd is naar type inbreuk, en voor de dwangsom op een percentage van de wereldwijde gemiddelde dagomzet van de aanbieder.

Blijkens artikel 51, vijfde lid, van de verordening en overweging 117 vindt de Uniewetgever het van belang dat bij het opleggen van sancties rekening wordt gehouden met de aard, de ernst, het herhaaldelijke karakter en de duur van de inbreuk, in relatie tot het algemeen belang dat wordt nagestreefd, de omvang en het soort activiteiten dat wordt uitgevoerd, en met de economische capaciteit van de inbreukmaker. Bij de vaststelling van de sancties moet volgens de overweging met name rekening worden gehouden met de systematische of herhaaldelijke aard van de inbreuk en verder met het aantal getroffen afnemers van de dienst, de opzettelijke of nalatige aard van de inbreuk en of de aanbieder in verschillende lidstaten actief is.

5.3.6.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel

De artikelen 2.3 en 2.4 van het wetsvoorstel voorzien in de bevoegdheid voor de ACM om een bestuurlijke boete en een last onder dwangsom op te leggen wegens overtreding van de verordening en de artikelen 3.3 en 3.4 van het wetsvoorstel voorzien in dezelfde bevoegdheid voor de AP. Een bestuurlijke boete of een last onder dwangsom kan ook worden opgelegd wegens overtreding van de medewerkingsplicht aan toezichtsmaatregelen (artikel 5:20 van de Awb) en het niet voldoen aan de

zelfstandige last (artikel 12m van de Instellingswet ACM en artikel 3.3 van dit wetsvoorstel). Voor de maximale hoogte van de bestuurlijke boete en de last onder dwangsom wordt in de betreffende bepalingen verwezen naar de bepalingen daarover in de verordening (artikel 51, derde en vierde lid, van de verordening). De bestuurlijke boete en de last onder dwangsom die overeenkomstig dit wetsvoorstel kunnen worden opgelegd, vormen doeltreffende, evenredige en afschrikkende sancties, zoals wordt vereist in artikel 52, tweede lid, van de verordening.

Zoals in paragraaf 4.3.1 van deze memorie van toelichting is toegelicht, hebben verschillende zorgvuldigheidsverplichtingen in de verordening het karakter van een open norm of doelvoorschrift. Dat is van belang in verband met het legaliteitsbeginsel, dat onder meer voortvloeit uit artikel 7 van het EVRM en artikel 49 van het Handvest. Dat beginsel houdt in dat, als er sprake is van een bestraffende sanctie, er sprake moet zijn van een kenbare, nauwkeurige, duidelijke en ondubbelzinnig geformuleerde delictsomschrijving op basis waarvan personen hun gedrag kunnen afstemmen. Om bij het opleggen van een bestuurlijke boete of last onder dwangsom voor overtreding van dit soort open normen aan het legaliteitsbeginsel te voldoen, zal er ofwel sprake moeten zijn van een evidente schending van de norm, of de norm moet zijn geconcretiseerd. Dit kan door de ACM zelf gebeuren, bijvoorbeeld in de vorm van een bindende aanwijzing, waarbij concreet wordt aangegeven wat er van de normadressaat wordt gevraagd ter nakoming van de open norm. Daarnaast voorziet de verordening in verschillende grondslagen voor de Commissie om richtsnoeren op te stellen, bijvoorbeeld waar het gaat om de verplichting voor aanbieders van online platforms om maatregelen te nemen ter bescherming van minderjarigen (artikel 28, vierde lid, van de verordening). Ook de digitaledienstenraad kan hierin een rol spelen (zie hierna paragraaf 5.4.5 van deze memorie van toelichting).

Een bijzonder geval vormen de zorgvuldigheidsverplichtingen die het karakter hebben van een open norm en die zien op de wijze waarop een aanbieder moet handelen bij de aanwezigheid op zijn dienst van illegale inhoud of inhoud in strijd met zijn algemene voorwaarden. Het gaat dan concreet om de verplichting voor alle aanbieders van tussenhandeldiensten om zorgvuldig te handelen bij de toepassing van inhoudsmoderatie met gepaste aandacht voor de rechten en legitieme belangen van alle betrokkenen (artikel 14, vierde lid, van de verordening) en de verplichting voor aanbieders van hostingdiensten om meldingen van illegale inhoud op een tijdige, zorgvuldige, niet-willekeurige en objectieve wijze te beoordelen (artikel 16, zesde lid, van de verordening). Deze bepalingen reguleren hoe een besluit tot inhoudsmoderatie moet worden genomen, terwijl de vraag of de betreffende inhoud illegaal of in strijd met algemene voorwaarden is wordt gereguleerd door een kader dat buiten de verordening ligt, namelijk het toepasselijke Unierecht of nationale recht of de algemene voorwaarden van de aanbieder. Het toezicht op deze normen vergt dan ook geen beoordeling van de illegaliteit van de informatie. Het gaat daarentegen om de wijze waarop het besluit tot inhoudsmoderatie tot stand komt.

Het bijzondere karakter van deze bepalingen heeft gevolgen voor de wijze waarop deze bepalingen op de meest doeltreffende en evenredige manier kunnen worden gehandhaafd. De aard van beide bepalingen sluit namelijk het beste aan bij het civiele recht. Besluiten over inhoudsmoderatie vinden immers plaats in het kader van de contractuele verhouding tussen aanbieder en gebruiker. Voor 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. Blijkens overweging 45 bij de verordening heeft de Uniewetgever het desondanks nodig geacht om regels te stellen over deze contractuele verhouding in het belang van de transparantie, de bescherming van de afnemers en het voorkomen van oneerlijke of willekeurige resultaten.

De inhoud van deze verplichtingen sluit ook aan bij het civiele recht, bij contractuele relaties in de vorm van de eisen van redelijkheid en billijkheid en daarbuiten in de vorm van de vereiste maatschappelijke zorgvuldigheid bij de onrechtmatige daad (zie nader paragraaf 5.3.8 van deze memorie van toelichting). De civiele rechter is ook bij uitstek in staat om in het concrete geval de vereiste belangenafweging te verrichten, waaronder de afweging tussen de verschillende aan de orde zijnde grondrechten. Dit laatste volgt uit jurisprudentie het HvJ EU, waarin de horizontale werking van de rechten in het Handvest is vastgesteld.[90] Ook door de Nederlandse rechter wordt de horizontale werking van grondrechten geaccepteerd. Met publiekrechtelijk toezicht op de horizontale werking van grondrechten moet dan ook terughoudend worden omgegaan.

Ook het feit dat de toezichthouder op grond van de verordening niet over de inhoud van de informatie kan oordelen, pleit ervoor om de handhaving van deze bepalingen primair civielrechtelijk vorm te geven. De overtreding van deze zorgvuldigheidsnormen zal in het concrete geval immers vaak samenhangen met de beoordeling of de inhoud zelf illegaal is of in strijd met de algemene voorwaarden. Een afnemer die vindt dat zijn inhoud ten onrechte is verwijderd, zal naar verwachting immers sneller vinden dat de aanbieder onzorgvuldig heeft gehandeld of zijn belangen onvoldoende gewicht heeft toegekend bij het verwijderingsbesluit. Tot slot voorziet het civiele recht in remedies die publiekrechtelijke handhaving niet als zodanig kent, met name de mogelijkheid om een vordering tot schadevergoeding in te stellen.

In het licht van het voorgaande kan de handhaving van de artikelen 14, vierde lid, en 16, zesde lid, van de verordening in een concreet geschil tussen betrokken partijen het beste geschieden door de civiele rechter, of in voorkomend geval het buitengerechtelijke geschillenbeslechtingsorgaan. De rol van publiekrechtelijke handhaving dient – in lijn met wat in overweging 117 bij de verordening wordt genoemd – beperkt te worden tot overtredingen die aanmerkelijk negatieve gevolgen hebben voor de veiligheid, voorspelbaarheid of betrouwbaarheid van de onlineomgeving (de artikelen 2.3, tweede lid, en 2.4, tweede lid, van dit wetsvoorstel). Het begrip “de veiligheid, voorspelbaarheid of betrouwbaarheid van de onlineomgeving” is onderdeel van de doelomschrijving in artikel 1, eerste lid, van de verordening. Van een aanmerkelijke negatieve invloed op de veiligheid, voorspelbaarheid of betrouwbaarheid van de onlineomgeving is sprake bij systematische of herhaaldelijke overtredingen van deze bepalingen, dat wil zeggen overtredingen die een groot aantal afnemers van de dienst treffen, die opzettelijk of nalatig van aard zijn of die grensoverschrijdend zijn doordat de betreffende aanbieder in verschillende lidstaten actief is.

Met deze aanvullende voorwaarde voor het opleggen van een bestuurlijke boete of een last onder dwangsom wordt invulling gegeven aan de ruimte die de verordening biedt om te voorzien in voorschriften inzake de sancties die gelden voor inbreuken van de verordening (artikel 52, eerste lid, van de verordening) en aan de eis dat de sancties doeltreffende, evenredig en afschrikkend moeten zijn (artikel 52, tweede lid, van de verordening). Het is namelijk niet doeltreffend en evenredig als elke overtreding van deze bepalingen publiekrechtelijk gehandhaafd zou kunnen worden. Het stellen van deze aanvullende voorwaarde laat overigens onverlet dat de ACM ten aanzien van overtredingen van de andere bepalingen van de verordening handhavingsbeleid kan voeren en daarbij rekening kan houden met de aard, de ernst, de herhaling en de duur van de inbreuk. Dit volgt ook uit artikel 51, vijfde lid, van de verordening.

[90] HvJ EU 6 november 2018, zaken C-569/16 en C-570/16, ECLI:EU:C:2018:871 (Bauer en Broßonn), HvJ EU 6 november 2018, zaak C-619/16, ECLI:EU:C:2018:872 (Kreuziger) en HvJ EU 6 november 2018, zaak C-684/16, ECLI:EU:C:2018:874 (Max-Planck-Gesellschaft).

De aanvullende voorwaarde voor het opleggen van een bestuurlijke boete of een last onder dwangsom geldt ook voor overtredingen van de verplichting voor aanbieders om onverwijld te reageren op een bevel van een bevoegde autoriteit (de artikelen 9, eerste lid, en 10, eerste lid, van de verordening). Het is immers, zoals ook toegelicht in paragraaf 3.4.2 van deze memorie van toelichting, aan de bevoegde autoriteit in kwestie om op te treden tegen de niet-naleving, of niet tijdige naleving van een dergelijk bevel. Handhaving van deze artikelen uit de verordening door de ACM is pas aan de orde als er sprake is van systematische of herhaaldelijke overtredingen. Hetzelfde geldt voor de verplichting om te goeder trouw mee te werken met een buitengerechtelijk geschillenbeslechtingsorgaan (artikel 21, tweede lid, van de verordening). Overtreding van die bepaling kan het beste in het kader van dat geschil worden opgelost en publiekrechtelijke handhaving is enkel aan de orde als sprake is van systematische of herhaaldelijke overtredingen.

5.3.7 Klachtrecht

5.3.7.1 Inhoud verordening

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. Tijdens de klachtenprocedure hebben beide partijen het recht om te worden gehoord en passende informatie te ontvangen over de stand van zaken in verband met de klacht. Hoewel het niet expliciet wordt genoemd, ligt het in de rede dat ook het informeren over de uitkomst van de klacht onder het begrip “informatie over de stand van zaken in verband met de klacht” valt.

5.3.7.2 Uitvoeringswijze in Nederland

Artikel 53 van de verordening werkt rechtstreeks en behoeft geen uitvoering in onderhavig wetsvoorstel. Het begrip “klacht” heeft in de verordening een autonome betekenis, die moet worden onderscheiden van het begrip “klacht” in de Awb. In de verordening heeft een klacht betrekking op een vermeende inbreuk op de verordening door een aanbieder van een tussenhandeldienst. In de Awb heeft het woord klacht betrekking op de wijze waarop een bestuursorgaan zich in een bepaalde aangelegenheid heeft gedragen.

Het is afhankelijk van de formulering en de inhoud van de klacht of de klacht naar Nederlands recht beschouwd moet worden als een verzoek van een belanghebbende om een handhavingsbesluit te nemen (artikel 1:3, derde lid, van de Awb) en daarmee als een handhavingsverzoek. Hierbij dient de ACM onder andere te toetsen of het verzoek voldoende concreet is en of de afnemer (of zijn gemachtigde) de ACM enig aanknopingspunt biedt voor onderzoek naar de vraag of de aanbieder van een tussenhandeldienst een overtreding begaat of heeft begaan.[91] Daarnaast dient de afnemer (of zijn gemachtigde) een belanghebbende in de zin van artikel 1:2, eerste lid, van de Awb te zijn om de klacht als handhavingsverzoek te kunnen beschouwen. Als sprake is van een handhavingsverzoek, heeft de ACM een beginselplicht tot handhaving. De beginselplicht tot handhaving geldt enkel voor herstelsancties (zoals de last onder dwangsom); en dus niet voor punitieve sancties.[92] Als de klacht beschouwd wordt als handhavingsverzoek, is de schriftelijke reactie van de ACM op de klacht een besluit in de zin van artikel 1:3, eerste lid, van de Awb. Hiertegen staat bezwaar en beroep open.

[91] CBb 18 april 2018, ECLI:NL:CBB:2018:128, r.o. 4.2.1.
[92] ABRvS 30 juni 2021, ECLI:NL:RVS:2021:1407, r.o. 5.1.

Deze kwalificatie naar nationaal recht heeft geen gevolgen voor het recht van partijen om te worden gehoord en passende informatie te ontvangen over de stand van zaken in verband met de klacht, dat op grond van de verordening geldt voor alle klachten.

Uit artikel 53 van de verordening volgt tevens dat elke klacht moet worden beoordeeld door de digitaledienstencoördinator. Dat betekent echter niet dat elke klacht hoeft te leiden tot een formeel onderzoek. Uit artikel 55 in samenhang met overweging 122 van de verordening kan evenwel worden afgeleid dat het jaarverslag van de digitaledienstencoördinator onder meer een overzicht moet bevatten van ontvangen klachten en het vervolg dat daaraan is gegeven, "met vermelding van onder meer het totale aantal ontvangen klachten en het aantal klachten dat heeft geleid tot een formeel onderzoek of tot doorgifte aan andere digitaledienstencoördinatoren".

5.3.8 Schadevergoeding

5.3.8.1 Inhoud verordening

Artikel 54 van de verordening bepaalt dat afnemers op grond van het Unierecht en het nationale recht het recht hebben om aanbieders van tussenhandeldiensten te verzoeken om schadevergoeding te betalen voor alle schade of verliezen die zij lijden als gevolg van een schending door die aanbieder van de verplichtingen uit de verordening. Als een aanbieder de verordening overtreedt en iemand lijdt daar schade door, dan kan diegene dus een schadevergoedingsvordering instellen.

5.3.8.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel

De grondslag voor schadevergoeding in het Nederlandse recht is de onrechtmatige daad, meer specifiek een doen of nalaten in strijd met een wettelijke plicht. De beperkte aansprakelijkheidsvrijstellingen voor aanbieders van tussenhandeldiensten (artikelen 4 tot en met 6 van de verordening) zijn hier niet van toepassing, omdat het hier gaat om schade als gevolg van een inbreuk op de verplichtingen uit de verordening door de aanbieder. Overigens kan ook een collectieve schadevergoedingsvordering worden ingesteld wegens overtreding van de verordening. Dat volgt uit artikel 90 van de verordening, waarmee de verordening wordt toegevoegd aan de lijst met Unierechtelijke bepalingen die door middel van representatieve vorderingen voor het beschermen van de collectieve belangen van consumenten kunnen worden gehandhaafd.

5.3.9 Wederzijdse bijstand, samenwerking en bijstand aan de Commissie

5.3.9.1 Inhoud verordening

Op grond van artikel 49, tweede lid, van de verordening moeten de digitaledienstencoördinatoren samenwerken met elkaar, met andere bevoegde nationale autoriteiten, met de digitaledienstenraad en met de Commissie met het oog op het doeltreffend en consistent toezicht houden op en handhaven van de verordening binnen de hele Unie. De lidstaten en de Commissie moeten op grond van artikel 56, vijfde lid, nauw samenwerken bij het toezicht op en handhaving van de verordening. De samenwerking tussen de digitaledienstencoördinatoren onderling en met de Commissie zijn verder uitgewerkt in de artikelen 57 tot en met 60 van de verordening.

Artikel 57 van de verordening heeft betrekking op wederzijdse bijstand. Op grond van het eerste lid van dat artikel moet de digitaledienstencoördinator van de plaats van vestiging de digitaledienstencoördinator van de plaats van bestemming[93], de digitaledienstenraad en de Commissie in kennis stellen van het instellen van een onderzoek en het voornemen om een definitief

[93] Dit is de digitaledienstencoördinator van de lidstaat waar de tussenhandeldienst wordt verstrekt (artikel 3, onderdeel o, van de verordening).

handhavingsbesluit te nemen. Op grond van het tweede en derde lid kan de digitaledienstencoördinator van de plaats van vestiging aan een andere digitaledienstencoördinator verzoeken om specifieke informatie over een specifieke aanbieder van tussenhandeldiensten te verstrekken als dat nodig is voor een onderzoek. Het gaat dan om informatie waarover de andere digitaledienstencoördinator al beschikt, of die hij met behulp van de onderzoeksbevoegdheden (artikel 51, eerste lid, van de verordening) kan verkrijgen. Waar passend kan de andere digitaledienstencoördinator andere bevoegde autoriteiten of andere overheidsinstellingen betrekken. De andere digitaledienstencoördinator geeft binnen twee maanden gevolg aan een dergelijk verzoek, tenzij één van de uitzonderingsgronden genoemd in het derde lid van toepassing is.

Artikel 58, eerste en tweede lid, van de verordening voorzien in de mogelijkheid voor de digitaledienstencoördinator van de plaats van bestemming of de digitaledienstenraad om de digitaledienstencoördinator van de plaats van vestiging gemotiveerd te verzoeken om een zaak te beoordelen en de nodige onderzoeks- en handhavingsmaatregelen te nemen. Ingevolge het vierde en vijfde lid van artikel 58 van de verordening houdt de digitaledienstencoördinator van de plaats van vestiging zoveel mogelijk rekening met een dergelijk verzoek en moet hij uiterlijk binnen twee maanden de beoordeling van de vermeende inbreuk meedelen aan de betreffende digitaledienstencoördinator en de digitaledienstenraad. Als de digitaledienstenraad het niet eens is met die beoordeling, dan kan zij de zaak verwijzen naar de Commissie, die de digitaledienstencoördinator van de plaats van vestiging kan verzoeken de beoordeling van de inbreuk te herzien (artikel 59 van de verordening).

De mogelijkheid van gezamenlijke onderzoeken is geregeld in artikel 60 van de verordening. Dergelijke gezamenlijke onderzoeken vinden plaats onder leiding van de digitaledienstencoördinator van de plaats van vestiging, op zijn initiatief of die van de digitaledienstenraad. Andere digitaledienstencoördinatoren met een legitiem belang kunnen deelnemen. De digitaledienstencoördinatoren werken te goeder trouw samen bij dit soort onderzoeken. De digitaledienstencoördinator van de plaats van vestiging deelt de uitkomst van het onderzoek mee aan de andere digitaledienstencoördinatoren, de digitaledienstenraad en de Commissie. Als de digitaledienstenraad het niet eens is met die beoordeling, dan kan zij de zaak verwijzen naar de Commissie, die de digitaledienstencoördinator van de plaats van vestiging kan verzoeken de beoordeling van de inbreuk te herzien.

5.3.9.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel

Artikel 57 van de verordening bepaalt dat dat de digitaledienstencoördinator bijstand moet verlenen op verzoek van andere digitaledienstencoördinatoren of de digitaledienstenraad. Dit kan onder meer inhouden dat hij inspecties uitvoert met betrekking tot specifieke informatie die zich in zijn lidstaat bevindt. De nationale ambtenaren oefenen daarbij hun bevoegdheden uit overeenkomstig het nationale recht. Artikel 2.7 van het wetsvoorstel bepaalt dat de toezichthoudende ambtenaren van de ACM daartoe bevoegd zijn. Zij beschikken daarbij over dezelfde bevoegdheden als die waarover zij beschikken bij de handhaving van de verordening. De overige artikelen inzake samenwerking werken rechtstreeks en behoeven geen uitvoering in onderhavig wetsvoorstel.

5.3.10 Toezicht en handhaving door de Commissie

5.3.10.1 Inhoud verordening

De Commissie is de enige handhaver van de verplichtingen die uitsluitend gelden voor aanbieders van zeer grote online platforms en zeer grote online zoekmachines (afdeling 5 van hoofdstuk III, zie

paragraaf 4.3.6 van deze memorie van toelichting). De Commissie is bovendien bevoegd om de overige verplichtingen van de verordening te handhaven ten aanzien van aanbieders van zeer grote online platforms en zeer grote online zoekmachines. De verordening geeft de Commissie verschillende onderzoeksbevoegdheden om te controleren of aanbieders van zeer grote online platforms en zeer grote online zoekmachines voldoen aan de verplichtingen uit de verordening. Daarbij gaat het respectievelijk om het verzoeken om inlichtingen (artikel 67 van de verordening), het horen en afnemen van verklaringen (artikel 68 van de verordening) en het verrichten van inspecties bij een onderneming of een ondernemersvereniging (artikel 69 van de verordening). De Commissie heeft de bevoegdheid om de nodige toezichtsmaatregelen te nemen. Zo kan zij onder meer gelasten dat zeer grote online platforms en zeer grote online zoekmachines toegang verlenen tot en uitleg geven over hun databanken en algoritmen (artikel 72 van de verordening). Ook kan de Commissie voorlopige maatregelen opleggen in gevallen waarin ernstig schade voor afnemers dreigt (artikel 70 van de verordening). Tot slot kan de Commissie toezeggingen bindend maken (artikel 71 van de verordening).

Indien de Commissie constateert dat een aanbieder van een zeer groot online platform of een zeer grote online zoekmachine een verplichting uit de verordening heeft overtreden, dan stelt zij een niet-nalevingsbesluit vast (artikel 73, eerste lid, van de verordening). In dit besluit geeft de Commissie de aanbieder van het zeer grote online platform of de zeer grote online zoekmachine de opdracht om de niet-naleving te beëindigen en daarover te rapporteren (artikel 73, vierde en vijfde lid, van de verordening). In het niet-nalevingsbesluit kan de Commissie ingeval van opzet of nalatigheid ook een boete opleggen, ter hoogte van maximaal zes procent van de totale wereldwijde omzet van het zeer grote online platform of de zeer grote online zoekmachine uit het vorige boekjaar (artikel 74, eerste lid, van de verordening). Naast een boete kan de Commissie ook een dwangsom opleggen ter hoogte van maximaal vijf procent van de gemiddelde dagelijkse inkomsten of de wereldwijde jaaromzet (artikel 76 van de verordening). Hiermee heeft de Commissie de mogelijkheid om een onderneming te dwingen om bepaalde verplichtingen, die zijn opgesomd in artikel 76, eerste lid, van de verordening, na te komen. Als een niet-nalevingsbesluit betrekking heeft op een inbreuk van een bepaling uit afdeling 5 van hoofdstuk III van de verordening, dan eist zij dat de betrokken aanbieder een actieplan opstelt met maatregelen om de inbreuk te beëindigen (artikel 75 van de verordening). Dit actieplan wordt meegedeeld aan de digitaledienstencoördinator, de digitaledienstenraad en de Commissie.

De digitaledienstencoördinatoren hebben verschillende taken ter ondersteuning van de Commissie bij de uitvoering van de verordening. Zo dienen ze informatie te verstrekken aan de Commissie (artikel 66, tweede lid, van de verordening). Ook kan de Commissie één of meer digitaledienstencoördinatoren verzoeken om steun bij de uitoefening van haar onderzoeksbevoegdheden (artikel 66, derde lid, van de verordening). De betrokken digitaledienstencoördinator en de eventueel betrokken bevoegde autoriteit en moeten loyaal en tijdig met de Commissie samenwerken na een dergelijk verzoek en hun onderzoeksbevoegdheden kunnen inzetten (artikel 51, eerste lid, van de verordening).

De digitaledienstencoördinatoren moeten voorts op verzoek van de Commissie actief bijstand verlenen bij inspecties op basis van artikel 69, zevende lid, van de verordening. Indien een aanbieder medewerking aan een inspectie weigert, moet daarbij ook de politie of een gelijkwaardige handhavingsautoriteit kunnen worden ingeschakeld (artikel 69, achtste lid, van de verordening). In het nationale recht kan aan deze laatste vorm van actieve bijstand de eis worden gesteld van een voorafgaande machtiging van een rechterlijke instantie (artikel 69, negende en tiende lid, van de verordening). De Commissie kan tot slot de digitaledienstencoördinator van de plaats van vestiging

bij ernstige en herhaalde overtredingen vragen om op treden overeenkomstig artikel 51, derde lid, van de verordening (zie nader paragraaf 5.3.5 van deze memorie van toelichting).

Overtreding van de verplichtingen van de verordening kan ook leiden tot civielrechtelijke handhaving door personen wier rechten zijn geschonden. Zij kunnen dan een civiele rechtsvordering instellen bij de nationale rechter. Artikel 82, derde lid, van de verordening bepaalt voor dit soort gevallen dat de nationale rechterlijke instanties geen uitspraken mogen doen die in strijd zijn met besluiten van de Commissie en dat zij strijdigheid met mogelijke besluiten van de Commissie in lopende procedures moeten vermijden.

5.3.10.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel

De uitvoering van de toezichts- en handhavingstaken van de Commissie behoeven geen voorziening in de nationale wetgeving. De ondersteunende taken die de nationale bevoegde autoriteiten daarbij hebben, zijn als volgt vormgegeven in dit wetsvoorstel. De informatie-uitwisseling tussen de digitaledienstencoördinator en de Commissie wordt beheerst door de verordening en vereist geen nadere nationale regelgeving. Wat betreft de steun bij de uitoefening van haar onderzoeksbevoegdheden van de Commissie bepaalt artikel 2.7 van het wetsvoorstel dat de toezichthoudende ambtenaren van de ACM bevoegd zijn die steun te verlenen. Zij beschikken daarbij over dezelfde bevoegdheden als die waarover zij beschikken bij de handhaving van de verordening.

Artikel 69, zevende lid, van de verordening vereist voorzieningen voor het verlenen van bijstand door ambtenaren van de nationale bevoegde autoriteit bij inspecties door de Commissie naar mogelijke overtreding van de verordening. De ambtenaren van de autoriteit handelen in het laatste geval onder de verantwoordelijkheid en het gezag van de Commissie en beschikken over dezelfde bevoegdheden als ambtenaren van de Commissie. Artikel 2.8, eerste lid, van het wetsvoorstel bepaalt dat de toezichthoudende ambtenaren van de ACM belast zijn met het verlenen van deze bijstand. Artikel 69, achtste lid, van de verordening schrijft voor dat deze ambtenaren de nodige bijstand moeten verlenen om de Commissie in staat te stellen haar inspectie te verrichten, in het geval dat een aanbieder zich tegen een inspectie door de Commissie verzet. Daarbij moet zo nodig een beroep gedaan kunnen worden op de politie of een andere handhavingsautoriteit. Dit is vastgelegd in artikel 2.8, derde lid, van het wetsvoorstel.

De relevante inspectiebevoegdheden zijn in dit verband het betreden van alle ruimten, terreinen en vervoersmiddelen van aanbieders (artikel 69, tweede lid, onderdeel a, van de verordening) en het controleren van de boeken en andere bescheiden betreffende de onderneming (artikel 69, tweede lid, onderdeel b, van de verordening). De Commissie is uit hoofde van de verordening dus wel bevoegd tot het betreden van vervoersmiddelen, terwijl in artikel 51 van de verordening die onderzoeksbevoegdheid niet aan de nationale bevoegde autoriteiten wordt toegekend. De uitoefening van onderzoeksbevoegdheden wordt in het Unierecht beperkt door de eis van noodzakelijkheid en evenredigheid. Artikel 82, derde lid, van de verordening vergt tot slot geen uitvoering in het nationale recht.

Het verlenen van bijstand aan de Commissie bij de uitvoering van diens inspecties wordt uitgevoerd door de ACM. De AP heeft hier geen rol bij. Dat is anders waar het gaat om het toepassen van onderzoeksbevoegdheden op verzoek van een andere digitaledienstencoördinator of de Commissie. De verzoeken daartoe worden door de ACM ontvangen. De ACM voert die uit waar het haar toezichtstaak betreft (artikel 2.7 van het wetsvoorstel) en zendt het verzoek door naar de AP waar het verzoek de toezichtstaken van de AP betreft (artikel 3.7 van het wetsvoorstel).

5.4 *Overige taken digitaledienstencoördinator*

5.4.1 Inleiding

De digitaledienstencoördinator is op grond van de verordening niet alleen verantwoordelijk voor de uitvoering van taken op het gebied van toezicht en handhaving (zie paragraaf 5.3 van deze memorie van toelichting), maar zij heeft ook andere uitvoeringstaken op grond van de verordening: de certificering van buitengerechtelijke geschillenbeslechtingsorganen (artikel 21, derde lid, van de verordening), de toekenning van de status van "betrouwbare flagger" (artikel 22, tweede lid, van de verordening) en de toekenning van de status van "erkende onderzoeker" (artikel 40, achtste lid, van de verordening). Daarnaast nemen de digitaledienstencoördinatoren deel aan de Europese Raad voor digitale diensten (digitaledienstenraad). In deze paragraaf wordt beschreven hoe de uitvoering van deze taken zal geschieden door de ACM in haar hoedanigheid als voorgestelde digitaledienstencoördinator in Nederland. Bovendien wordt beschreven welke rol de AP heeft bij de uitvoering van deze taken als voorgestelde andere bevoegde autoriteit voor het toezicht op en de handhaving van de verordening.

5.4.2 Ontvangen en doorzenden van afschriften van bevelen aan aanbieders

Op grond van de artikelen 9, derde en vierde lid, en 10, derde en vierde lid, van de verordening dient de ACM een afschrift te ontvangen van bevelen die in Nederland zijn uitgegeven aan aanbieders van tussenhandeldiensten en dient de ACM deze door te sturen naar de andere digitaledienstencoördinatoren. Op deze bevelen is nader ingegaan in paragraaf 3.4 van deze memorie van toelichting. Het is aan de bevoegde autoriteit die het bevel uitgeeft om een afschrift aan de ACM te zenden. Voor bevelen die worden uitgegeven door de civiele rechter wordt door middel van dit wetsvoorstel in het Rv geregeld dat het verzenden van afschriften geschiedt door tussenkomst van de Raad voor de rechtspraak (artikel 5.6 van dit wetsvoorstel).

5.4.3 Certificering en toekenning formele statussen

5.4.3.1 Inhoud verordening

De verordeningsbepalingen over buitengerechtelijke geschillenbeslechting, de behandeling van meldingen van betrouwbare flaggers en de toegang tot gegevens van zeer grote online platforms en zeer grote online zoekmachines voor erkende onderzoekers zijn toegelicht in hoofdstuk 4 van deze memorie van toelichting.[94] Deze bepalingen schrijven tussenkomst van de digitaledienstencoördinator voor, die de buitengerechtelijke geschillenbeslechtingsorganisaties moet certificeren en betrouwbare flaggers en onderzoekers de status van "betrouwbare flagger" respectievelijk "erkend onderzoeker" moet toekennen.

5.4.3.2 Uitvoeringswijze in Nederland en inhoud wetsvoorstel

De besluiten tot het certificeren van buitengerechtelijke geschillenbeslechtingsorganen, het toekennen van de status van "betrouwbare flagger" en het toekennen van de status van "erkende onderzoeker" door de ACM, in haar hoedanigheid als voorgestelde digitaledienstencoördinator, worden rechtstreeks genomen op grond van de verordening. Deze besluiten zijn te beschouwen als besluiten in de zin van artikel 1:3, eerste lid, van de Awb, waardoor de bepalingen van de Awb over besluiten van rechtswege van toepassing zullen zijn op de besluiten die de ACM in het kader van deze taken zal nemen. Daarvoor is in beginsel geen nadere uitwerking nodig in dit wetsvoorstel, tenzij er bijzondere aspecten aan het nemen van deze besluiten zijn die bijzondere regels vergen in

[94] Zie paragrafen 4.3.4.2, 4.3.4.3 en 4.3.6.7 van deze memorie van toelichting.

aanvulling op de bepalingen van de Awb. Hierna wordt per besluit toegelicht in hoeverre dat nodig is en hoe de uitvoeringswijze in Nederland er uit zal zien.

De certificering van buitengerechtelijke geschillenbeslechtingsorganen vergt geen aanvullende bepalingen in dit wetsvoorstel. Op grond van het zesde lid van artikel 21 van de verordening kunnen lidstaten zelf buitengerechtelijke geschillenbeslechtingsorganen oprichten of de activiteiten van gecertificeerde organen ondersteunen. Van deze mogelijkheid wordt op dit moment geen gebruik gemaakt, omdat het kabinet erop vertrouwt dat er in Nederland voldoende gekwalificeerde organisaties zullen zijn die in aanmerking komen voor de rol van gecertificeerd buitengerechtelijke geschillenbeslechtingsorgaan om een goede uitvoering van dit onderdeel van de verordening mogelijk te maken.

Ook de toekenning van de status van "betrouwbare flagger" behoeft geen nadere regeling in onderhavig wetsvoorstel. Opgemerkt zij wel dat het kabinet de status van "betrouwbare flagger" als iets beschouwt dat met name geschikt is voor private handhaving door private organisaties. Het kabinet is dan ook van oordeel dat het in beginsel onwenselijk is dat overheidsorganisaties en toezichthouders de status van betrouwbare flagger onder de verordening aanvragen. In plaats daarvan zouden zij gebruik moeten maken van hun wettelijke bevoegdheden om bevelen uit te vaardigen teneinde illegale inhoud onverwijld verwijderd te krijgen, of tot vrijwillige afspraken met online platforms of tussenhandeldiensten moeten komen of die in stand houden. 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.

In het wetsvoorstel zijn wel aanvullende regels opgenomen over de toekenning van de status van "erkend onderzoeker". Erkende onderzoekers krijgen toegang tot de gegevens van aanbieders van zeer grote online platforms en zeer grote online zoekmachines, met als doel het onderzoeken van systeemrisico's van deze diensten en de effectiviteit van risicobeperkende maatregelen die deze aanbieders nemen. Deze toegang zelf brengt de nodige risico's met zich mee, onder meer op het gebied van de bescherming van persoonsgegevens van gebruikers van die diensten en van de niet-openbare bedrijfsgegevens van de aanbieder. Om die reden worden in artikel 40, achtste lid, van de verordening strenge voorwaarden gesteld aan de toekenning van de status van "erkend onderzoeker". Een van die voorwaarden (onderdeel d) is dat de onderzoekers aantoonbaar in staat zijn om specifieke gegevensbeveiligings- en vertrouwelijkheidsvereisten in acht te nemen en persoonsgegevens te beschermen. Om die reden schrijft artikel 2.9 van het wetsvoorstel voor dat de AP advies uitbrengt aan de ACM bij de beoordeling van dit criterium. In verband met dit advies, en de complexiteit van de beoordeling in zijn geheel, is bepaald dat de beslistermijn van dit besluit wordt gesteld op twaalf weken en dat die termijn eenmalig kan worden verlengd met acht werken. De termijn om advies uit te brengen is gesteld op zeven weken; die termijn is twaalf weken als de beslistermijn wordt verlengd. Een eventueel bezwaar en beroep tegen een besluit tot toekenning van de status van "erkend onderzoeker" kan betrekking hebben op het aspect waar de AP over heeft geadviseerd. Het ligt in de rede dat de AP ook in die fase zo nodig adviseert; afdeling 3.3 van de Awb biedt daar het kader voor.

5.4.4 Activiteitenverslag

5.4.4.1 Inhoud verordening

Artikel 55, eerste lid, van de verordening schrijft voor dat de digitaledienstencoördinatoren jaarverslagen opstellen over hun activiteiten uit hoofde van de verordening. In het bijzonder wordt genoemd een overzicht van het aantal klachten dat op grond van artikel 53 van de verordening is

ingediend en welk gevolg aan die klachten is gegeven. Ingevolge het tweede lid van artikel 55 van de verordening moet het verslag ook inzicht bieden in de bevelen voor het verwijderen van informatie en het verstrekken van informatie die overeenkomstig de artikelen 9 en 10 van de verordening zijn uitgevaardigd en welk gevolg daaraan is gegeven. Als een lidstaat ook andere bevoegde autoriteiten aanwijst, dan moet het verslag ook betrekking hebben op de activiteiten van die andere autoriteiten; de lidstaten moeten ervoor zorgen dat de digitaledienstencoördinator van die andere autoriteiten alle relevante informatie en ondersteuning ontvangt.

5.4.4.2 Uitvoeringswijze in Nederland

Artikel 55, eerste en tweede lid, van de verordening werkt rechtstreeks en behoeft geen nadere regeling in onderhavig wetsvoorstel. Ter uitvoering van artikel 55, derde lid, van de verordening is in artikel 4.1, tweede lid, van het wetsvoorstel bepaald dat de AP alle relevante informatie en ondersteuning aan de ACM verstrekt die nodig is om het jaarlijkse activiteitenverslag op te stellen.

5.4.5 Deelname digitaledienstenraad

5.4.5.1 Inhoud verordening

De Europese Raad voor digitale diensten, ofwel de "digitaledienstenraad", is de onafhankelijke adviesgroep van digitaledienstencoördinatoren (artikel 61, eerste lid, van de verordening). De digitaledienstenraad adviseert de digitaledienstencoördinatoren en de Commissie over een consistente toepassing van de verordening en effectieve samenwerking, de door de Commissie op te stellen richtsnoeren en verleent de Commissie bijstand bij het toezicht op de zeer grote online platforms (artikel 61, tweede lid, van de verordening). Deze taken zijn nader uitgewerkt in artikel 63 van de verordening. De digitaledienstenraad bestaat uit de digitaledienstencoördinatoren en, als het recht van de lidstaat in kwestie dat bepaalt, andere bevoegde autoriteiten van de lidstaten (artikel 62, eerste lid, van de verordening). De Commissie zit de raad voor en biedt administratieve ondersteuning. Elke lidstaat heeft één stem bij de besluitvorming door de digitaledienstenraad, ongeacht het aantal autoriteiten dat namens de lidstaat deelneemt (artikel 62, derde lid, van de verordening). Ook andere nationale autoriteiten kunnen worden uitgenodigd om deel te nemen. De raad kan ook samenwerken met andere organen van de Unie en kan belanghebbende raadplegen (artikel 62, vijfde en zesde lid, van de verordening).

5.4.5.2 Uitvoeringswijze in Nederland

De ACM zal, als voorgestelde digitaledienstencoördinator voor Nederland, deel uitmaken van de digitaledienstenraad. Voor de uitvoering van de taken van de AP als andere bevoegde autoriteit voor toezicht en handhaving, is het ook van belang dat de AP kan deelnemen aan de digitaledienstenraad. Dit is geregeld in artikel 3.1, vierde lid, van het wetsvoorstel, zoals artikel 62, eerste lid, van de verordening voorschrijft. Het ligt in de rede dat de ACM en de AP over hun gezamenlijke deelname aan de digitaledienstenraad afspraken maken in hun samenwerkingsprotocol.

6 Samenwerking en gegevensuitwisseling tussen autoriteiten

6.1 *Samenwerking tussen de bevoegde autoriteiten en met andere autoriteiten*

Als een lidstaat naast de digitaledienstencoördinator ook andere bevoegde autoriteiten aanwijst, dan moeten hun taken duidelijk afgebakend zijn en moeten zij nauw en doeltreffend samenwerken (artikel 49, tweede lid, van de verordening). In onderhavig wetsvoorstel worden de onderscheiden taken van de ACM en de AP duidelijk afgebakend, door in de artikelen 2.2 en 3.2 van het wetsvoorstel duidelijk te bepalen voor welke bepalingen welke autoriteit bevoegd is toezicht te

houden. Deze bevoegdheden overlappen elkaar niet, in de zin dat voor elke verplichting in de verordening maar één autoriteit bevoegd zal zijn voor toezicht en handhaving.

Artikel 4.2 van het wetsvoorstel schrijft voorts voor dat de ACM en de AP een samenwerkingsprotocol opstellen, waarin zij in elk geval afspraken dienen te maken over een nauwe en doeltreffende samenwerking bij de uitvoering van hun respectievelijke taken ter uitvoering van de verordening. Dit samenwerkingsprotocol is het instrument waarmee zij invulling geven aan de op hen op grond van artikel 49, tweede lid, van de verordening rustende verplichting om nauw en doeltreffend samen te werken. Het wetsvoorstel bevat ook voorzieningen voor de samenwerking tussen de ACM en de AP bij de toekenning van de status van "erkend onderzoeker" en bij het verlenen van de nodige bijstand bij onderzoeken van de Commissie. Deze voorzieningen worden nader toegelicht in de paragrafen 4.3.6.7 en 5.3.9 van deze memorie van toelichting. Het wetsvoorstel voorziet tot slot ook in een grondslag voor gegevensverstrekking van de AP aan de ACM (artikel 4.1 van het wetsvoorstel), in aanvulling op de gegevensverstrekking van de ACM aan de AP die al mogelijk is op grond van de Instellingswet ACM. Hierop wordt nader ingegaan in paragraaf 6.2.1 van deze memorie van toelichting.

De ACM en de AP kunnen met andere autoriteiten samenwerken als dat nodig of wenselijk is voor de uitvoering van hun taken onder de verordening. Die samenwerking kan op informele basis plaatsvinden, maar kan ook een formele status krijgen in de vorm van een samenwerkingsovereenkomst. In het bijzonder kan gewezen worden op het Samenwerkingsplatform Digitale Toezichthouders (hierna: SDT), dat gericht is op het bevorderen van een coherente en gecoördineerde aanpak van het toezicht op digitale activiteiten en waar de ACM, de AP, de Autoriteit Financiële Markten en het CvdM bijvoorbeeld deel van uitmaken. Binnen dit SDT werken de toezichthouders samen door het uitwisselen van kennis en ervaringen uit de toezichtspraktijk op verschillende thema's in het digitale domein, zoals kunstmatige intelligentie, algoritmes en dataverwerking, online design, personalisering, manipulatie en misleiding. Ook investeren ze gezamenlijk in kennis, expertise en competenties. Verder kijken de toezichthouders waar ze elkaar in handhavingstrajecten kunnen versterken, onder meer door gezamenlijk digitale marktproblemen aan te pakken. Recent werd bekend dat het SDT twee extra zogeheten Kamers zal oprichten voor het afstemmen van toezicht op online platforms en op kunstmatige intelligentie, namelijk een DSA-Kamer (die ziet op digitale diensten, waaronder online platforms) en een Algoritme- & AI-kamer.[95]

Het brede, open karakter van de norm neergelegd in artikel 28, eerste lid, van de verordening (zie paragraaf 4.3.4.9 van deze memorie van toelichting) brengt mee dat die aan de taken, kennis en expertise van meerdere toezichthouders kan raken. Naast de ACM valt met name te denken aan de AP en het CvdM. Het ligt daarom voor de hand dat de ACM die andere toezichthouders in voorkomende gevallen raadpleegt of op een andere wijze betrekt bij het toezicht op en de handhaving van het artikel. De bestaande samenwerkingsprotocollen bieden daarvoor de mogelijkheden.

6.2 *Gegevensuitwisseling*

6.2.1 Gegevensuitwisseling tussen de AP en de ACM

Voor een nauwe en doeltreffende samenwerking bij de uitvoering van de verschillende onderdelen van de verordening is het nodig dat de ACM en AP gegevens of inlichtingen kunnen uitwisselen die zij in het kader van de uitoefening van hun taken op grond van dit wetsvoorstel verkrijgen. Vanwege de

[95] Zie het bericht dat de ACM hierover op zijn website heeft geplaats: https://www.acm.nl/nl/publicaties/toezichthouders-van-sdt-breiden-samenwerking-digitaal-toezicht-uit.

geheimhoudingsplicht op grond van artikel 2:5, tweede lid, van de Awb kunnen de ACM en de AP vertrouwelijke gegevens of inlichtingen in beginsel niet verstrekken aan andere overheidsinstanties. Bij wettelijk voorschrift kan van deze geheimhoudingsplicht worden afgeweken. Voor het verstrekken van gegevens door de ACM aan de AP vormen artikel 7, derde en vierde lid, van de Instellingswet ACM en de Regeling gegevensverstrekking ACM 2019[96] het betreffende wettelijke voorschrift. Voor het verstrekken van gegevens door de AP aan de ACM voorziet artikel 4.1 van dit wetsvoorstel in een dergelijke grondslag.

De uitwisseling van inlichtingen en gegevens tussen de ACM en de AP heeft twee functies. In de eerste plaats draagt de uitwisseling bij aan een nauwe en doeltreffende samenwerking bij het uitoefenen van hun toezichtstaken. De toezichtstaken van de ACM en de AP in onderhavig wetsvoorstel zijn weliswaar duidelijk afgebakend, maar voor de doeltreffendheid van het toezicht is het wel van belang dat de ACM en de AP hun toezichtsactiviteiten op elkaar afstemmen. Het toezicht van de ACM en de AP is immers gericht op dezelfde normadressaten en er bestaat een inhoudelijke samenhang tussen de bepalingen waar de ACM en de AP op toezien. Ook is het denkbaar dat de ACM en de AP gezamenlijk onderzoek doen naar de naleving van de verordening door een aanbieder van tussenhandeldiensten. De uitwisseling van inlichtingen en gegevens zal in dit kader betrekking hebben op informatie die in het kader van het toezicht wordt verkregen en informatie over opgelegde sancties.

In de tweede plaats is de uitwisseling van gegevens en inlichtingen nodig voor de uitvoering van de andere taken op grond van de verordening door de ACM en de AP. Zo voorziet artikel 2.9, derde lid, van het wetsvoorstel in een adviestaak van AP bij de verlening van de status van "erkende onderzoeker" door de ACM (zie paragraaf 5.4.3.2 van deze memorie van toelichting). Hiervoor is het noodzakelijk dat de ACM de onderzoeksaanvraag aan de AP kan sturen en dat de AP in voorkomend geval vertrouwelijke gegevens of inlichtingen in zijn advies aan de ACM kan opnemen. Voorts kunnen digitaledienstencoördinatoren en de Commissie een informatieverzoek indienen bij de ACM in het kader van wederzijdse bijstand (zie artikel 57 van de verordening). Als het informatie betreft waar de AP over beschikt, dan moet de AP die informatie aan de ACM verstrekken, zodat de ACM het informatieverzoek kan beantwoorden. Ook bij grensoverschrijdende samenwerking tussen digitaledienstencoördinatoren (artikel 58 van de verordening) kan informatie relevant zijn waar AP over beschikt. Tot slot is het van belang dat de ACM en de AP informatie uitwisselen ten behoeve van de deelname aan de digitaledienstenraad en het jaarverslag dat de ACM als digitaledienstencoördinator moet opstellen over de uitvoering van de verordening in Nederland. De verwachting is echter niet dat voor die laatste twee doeleinden vertrouwelijke gegevens of inlichtingen hoeven te worden uitgewisseld.

De verstrekking van inlichtingen en gegevens door de AP aan de ACM op grond van artikel 4.1 van het wetsvoorstel kan betrekking hebben op persoonsgegevens. Als het gaat om gegevens verkregen bij toezichtsactiviteiten, kan er sprake zijn van persoonsgegevens als het online platform waar de AP toezicht op houdt wordt aangeboden door een natuurlijke persoon. In de praktijk zullen de meeste aanbieders van online platforms rechtspersonen zijn, maar gezien de grote verscheidenheid aan online platforms is het niet uitgesloten dat het platform wordt aangeboden door een natuurlijke persoon. Bij het adviseren over de verlening van de status van "erkende onderzoeker" zal in beginsel ook sprake zijn van persoonsgegevens van de betreffende onderzoekers.

De verwerking van persoonsgegevens is alleen toegestaan voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5, eerste lid, onderdeel b, van de AVG). Het

[96] Deze regeling zal worden gewijzigd ten behoeve van gegevensverstrekking in het kader van dit wetsvoorstel.

doel van de uitwisseling van persoonsgegevens op grond van dit wetsvoorstel is om een goede uitoefening van de taken van de ACM en de AP op grond van dit wetsvoorstel mogelijk te maken. De verwerking moet ingevolge artikel 6, eerste lid, van de AVG gebaseerd zijn op één van de daar genoemde rechtsgronden. In onderhavig geval is de rechtsgrond dat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (artikel 6, eerste lid, onderdeel c, van de AVG). De doelbinding is geborgd doordat is bepaald dat de ACM, als ontvanger, de gegevens enkel kan verwerken voor het doel waarvoor ze worden verstrekt, dat wil zeggen een goede uitoefening van de taken van de ACM op grond van dit wetsvoorstel (artikel 4.1, eerste lid, van het wetsvoorstel).

De noodzaak van de gegevensverstrekking van de AP aan de ACM is erin gelegen dat een nauwe en doeltreffende samenwerking tussen de ACM en de AP bij hun toezichtstaken, zoals voorgeschreven door de digitaledienstenverordening, niet mogelijk is zonder adequate uitwisseling van inlichtingen en gegevens. De noodzaak van de gegevensverstrekking vloeit voorts voort uit de adviestaak van de AP op grond van artikel 2.9, derde lid, van het wetsvoorstel en uit de verschillende coördinerende taken van de ACM onder de verordening; zonder gegevensverstrekking van de AP aan de ACM is de uitvoering van die taken niet mogelijk.

6.2.2 Gegevensuitwisseling tussen de ACM, de politie en het OM

De politie en het OM zijn voor Nederland de rechtshandhavingsautoriteit en gerechtelijke autoriteit waar aanbieders van hostingdiensten meldingen moeten doen van strafbare feiten waarbij het leven of de veiligheid van personen wordt bedreigd (artikel 18 van de verordening; zie hierover nader paragraaf 4.3.3.3 van deze memorie van toelichting). De ACM, als digitaledienstencoördinator, zal toezicht houden op deze verplichting. In het kader daarvan is het nodig dat de politie en het OM gegevens en inlichtingen aan de ACM kunnen verstrekken over de meldingen die zij uit hoofde van artikel 18 van de verordening hebben ontvangen en welk gevolg daaraan is gegeven. Ook zullen de politie en het OM in voorkomende gevallen kunnen vaststellen of een hostingaanbieder beschikte over relevante informatie die hij had moeten melden op grond van artikel 18 van de verordening, maar niet heeft gemeld. Gegevens en inlichtingen daarover zullen eveneens aan de ACM moeten worden verstrekt, teneinde de ACM in staat te stellen artikel 18 van de verordening te handhaven.

De ACM kan het OM voorts verzoeken om advies bij het nemen van een maatregel die neerkomt op een tijdelijke toegangsbeperking voor aanbieders van tussenhandeldiensten bij ernstige overtredingen van de verordening die samenhangen met strafbare feiten waarbij het leven of de veiligheid van personen wordt bedreigd (artikel 51, derde lid, onderdeel b, van de verordening; zie hierover nader paragraaf 5.3.5 van deze memorie van toelichting). Dit advies heeft betrekking op de vraag of in het concrete geval sprake is van ernstige schade die niet kan worden vermeden door de uitoefening van strafvorderlijke bevoegdheden en de vraag of sprake is van een strafbaar feit of strafbare feiten waarbij het leven of de veiligheid van personen wordt bedreigd (artikel 2.5, derde lid, van het wetsvoorstel). Om deze adviestaak te kunnen vervullen, is het noodzakelijk dat de ACM vertrouwelijke gegevens kan verstrekken aan het OM en het OM aan de ACM.

De verstrekking van politiegegevens door de politie geschiedt op grond van de Wet politiegegevens. Voor het verstrekken van politiegegevens in het kader van dit wetsvoorstel zal een grondslag worden opgenomen in het Besluit politiegegevens krachtens die wet. De verstrekking van justitiële en strafvorderlijke gegevens door het OM zal geschieden op grond van artikel 39, eerste lid, onderdeel d, van de Wet justitiële en strafvorderlijke gegevens.

7 Verhouding tot ander EU-recht

De verordening voert een horizontaal en algemeen kader in voor tussenhandeldiensten, terwijl andere EU-instrumenten regels bevatten die specifiek zijn toegesneden op bepaalde specifieke soorten inhoud, onderwerpen of rechtsgebieden. De verordening is niet van invloed op de toepassing van dergelijke Unierechtshandelingen, die bepaalde andere aspecten van de levering van diensten van de informatiemaatschappij regelen. Dit volgt uit artikel 2, vierde lid, en overweging 10 en 11 van de verordening. De verordening noemt in dit verband met name de volgende niet-uitputtende voorbeelden van Unierechtelijke handelingen:

- de (herziene) Richtlijn audiovisuele mediadiensten;[97]
- het Unierecht inzake auteursrechten en verwante rechten, waaronder de Richtlijn auteursrecht in de informatiemaatschappij[98], de Handhavingsrichtlijn[99] en de Richtlijn inzake auteursrecht in de digitale eengemaakte markt;[100]
- de Verordening ter bestrijding van terroristische online-inhoud;[101]
- de Verordening over het op de markt brengen en het gebruik van precursoren voor explosieven;[102]
- de *Platform-to-business* verordening (hierna: P2B-verordening);[103]
- het Unierecht betreffende consumentenbescherming en productveiligheid, waaronder de CPC-Verordening[104], de Markttoezichtverordening[105], de Richtlijn Algemene

[97] Richtlijn 2010/13/EU van het Europees Parlement en de Raad van 10 maart 2010 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten), zoals gewijzigd bij Richtlijn (EU) 2018/1808 van het Europees Parlement en de Raad van 14 november 2018 tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten) in het licht van een veranderende marktsituatie (PbEU 2010, L 95).
[98] Richtlijn 2001/29/EG van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij (PbEG 2011, L 167).
[99] Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (PbEU 2004, L 157).
[100] Richtlijn (EU) 2019/790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG (PbEU 2019, L 130).
[101] Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud (PbEU 2021, L 172).
[102] Verordening (EU) 2019/1148 van het Europees Parlement en de Raad van 20 juni 2019 over het op de markt brengen en het gebruik van precursoren voor explosieven, tot wijziging van Verordening (EG) nr. 1907/2006 en tot intrekking van Verordening (EU) nr. 98/2013 (PbEU 2019, L 186).
[103] Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van online tussenhandeldiensten (PbEU 2019, L 186).
[104] Verordening (EU) 2017/2394 van het Europees Parlement en de Raad van 12 december 2017 betreffende samenwerking tussen de nationale autoriteiten die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en tot intrekking van Verordening (EG) nr. 2006/2004 (PbEU 2017, L 345).
[105] Verordening (EU) 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van producten en tot wijziging van Richtlijn 2004/42/EG en de Verordeningen (EG) nr. 765/2008 en (EU) nr. 305/2011 (PbEU 2019, L 169).

Productveiligheid[106], de richtlijn OHP, de Richtlijn consumentenrechten[107], de Richtlijn oneerlijke bedingen in consumentenovereenkomsten[108] en de Richtlijn ADR consumenten;[109]

- het Unierecht betreffende de bescherming van persoonsgegevens, met name de AVG[110] en de ePrivacy richtlijn;[111]
- het Unierecht op het gebied van internationaal privaatrecht, waaronder de EEX-verordening[112] en de regels betreffende het recht dat van toepassing is op contractuele[113] en niet-contractuele verbintenissen;[114]
- Unierechtelijke bepalingen vastgelegd in een verordening betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken[115] en in een richtlijn tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures.[116]

Voor zover dergelijke andere Unierechtshandelingen dezelfde doelstellingen nastreven als die van de verordening, zijn de regels van de verordening echter wel van toepassing op aangelegenheden die niet, of niet volledig, door die andere rechtshandelingen worden aangepakt. Dit geldt ook voor aangelegenheden waarvoor die andere rechtshandelingen de lidstaten de mogelijkheid laten om bepaalde maatregelen op nationaal niveau vast te stellen. Dit volgt uit overweging 10. De horizontale regels uit de verordening zijn dus van toepassing, tenzij een andere Unierechtshandeling een bepaald onderwerp uitputtend regelt. Dit volgt ook uit artikel 2, vierde lid, van de verordening, waarin wordt verwezen naar de andere Unierechtshandelingen "die deze verordening specificeren en aanvullen".

---

[106] Richtlijn 2001/95/EG van het Europees Parlement en de Raad van 3 december 2001 inzake algemene productveiligheid (PbEG 2011, L 11).

[107] Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad (PbEU 2011, L 304).

[108] Richtlijn 93/13/EEG van de Raad van 5 april 1993 betreffende oneerlijke bedingen in consumentenovereenkomsten (PbEG 1993, L 95).

[109] Richtlijn 2013/11/EU van het Europees Parlement en de Raad van 21 mei 2013 betreffende alternatieve beslechting van consumentengeschillen en tot wijziging van Verordening (EG) nr. 2006/2004 en Richtlijn 2009/22/EG (PbEU 2013, L 165).

[110] 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).

[111] 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).

[112] Verordening (EU) nr. 1215/2012 van het Europees Parlement en de Raad van 12 december 2012 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken (herschikking) (PbEU 2012, L 351).

[113] Verordening (EG) nr. 593/2008 van het Europees Parlement en de Raad van 17 juni 2008 inzake het recht dat van toepassing is op verbintenissen uit overeenkomst (Rome I) (PbEU 2008, L 177).

[114] Verordening (EG) nr. 864/2007 van het Europees Parlement en de Raad van 11 juli 2007 betreffende het recht dat van toepassing is op niet-contractuele verbintenissen (Rome II) (PbEU 2007, L 199).

[115] Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken, COM (2018) 225.

[116] Voorstel voor een Richtlijn van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures, COM/2018/226 final.

Ten behoeve van de duidelijkheid wordt hieronder kort ingegaan op de verhouding tussen de verordening en een aantal specifieke EU-wetgevingsinstrumenten die bepaalde aspecten van de aanbieding van tussenhandeldiensten regelen.

7.1.1 Digitalemarktenverordening

De digtalemarktenverordening[117] bevat regels voor de grootste online platforms die door hun aanzienlijke marktpositie binnen de sector als zogenaamde "poortwachters" kwalificeren. Het betreft veelal platforms die zo machtig zijn dat zij zelfstandig de voorwaarden kunnen bepalen waaronder zij bedrijven en consumenten toegang verlenen tot een bepaalde digitale markt. De verordening legt verplichtingen op aan deze platforms en voorziet in de handhaving van die verplichtingen. Doel van de digitalemarktenverordening is bij te dragen aan een goed functionerende interne markt door geharmoniseerde regels vast te stellen die in de gehele Unie ten aanzien van alle ondernemingen zorgen voor betwistbare en eerlijke markten in de digitale sector waarop poortwachters aanwezig zijn, een en ander ten behoeve van zowel zakelijke gebruikers als eindgebruikers.

De doelstellingen van de digitalemarktenverordening liggen in het verlengde van de digitaledienstenverordening. Beide verordeningen zijn onderdeel van samenhangende inspanningen van de Commissie om belangrijke online diensten, en de aanbieders daarvan, te reguleren op basis van Europese waarden. Daarbij ziet de digitalemarktenverordening voornamelijk op marktordening. De digitalemarktenverordening richt zich op poortwachters, waarvoor andere criteria en definities gebruikt worden (zie artikel 3 en Bijlage A van de verordening) dan voor de zeer grote online platforms en zeer grote online zoekmachines onder de verordening (zie paragraaf 4.3.6.2). Poortwachters onder de digitalemarktenverordening zijn dus niet per definitie ook aanbieders van zeer grote online platforms of zeer grote online zoekmachines in de zin van de verordening, en andersom. Het is echter wel waarschijnlijk dat er in de praktijk overlap zal zijn, waardoor sommige ondernemingen onder de reikwijdte van beide verordeningen vallen.

7.1.2 Richtlijn audiovisuele mediadiensten

De gewijzigde richtlijn audiovisuele mediadiensten[118], zoals geïmplementeerd in de Mediawet 2008, bevat verplichtingen voor aanbieders van "videoplatformdiensten" die in een EU-lidstaat zijn gevestigd. Het is aannemelijk dat een aantal online platforms of zeer grote online platforms onder de verordening ook aanbieders van videoplatformdiensten zullen zijn in de zin van artikel 1, onder a bis, van die richtlijn. Artikel 28ter van die richtlijn verplicht aanbieders van videoplatformdiensten onder meer om minderjarigen te beschermen tegen programma's die hun lichamelijke, geestelijke of morele ontwikkeling kunnen aantasten en om het publiek in zijn algemeenheid te beschermen tegen terroristische content of content dan wel commerciële inhoud die aanzet tot geweld of haat. Videoplatforms moeten ook transparant zijn jegens hun gebruikers over audiovisuele commerciële communicatie die via hun videoplatformdienst wordt verspreid. De digitaledienstenverordening bevat diverse verplichtingen die gedeeltelijk overlappen met deze verplichtingen voor videoplatformdiensten, zoals artikel 26 van de verordening (reclame op online platforms, zie

[117] Verordening (EU) 2022/1925 over betwistbare en eerlijke markten in de digitale sector (de digitalemarktenverordening) (PbEU 2022, L 265).

[118] Richtlijn 2010/13/EU van het Europees Parlement en de Raad van 10 maart 2010 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten), zoals gewijzigd bij Richtlijn (EU) 2018/1808 van het Europees Parlement en de Raad van 14 november 2018 tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten) in het licht van een veranderende marktsituatie (PbEU 2010, L 95).

paragraaf 4.3.4.7) en artikel 28 van de verordening (de bescherming van minderjarigen, zie paragraaf 4.3.4.9). De richtlijn en de verordening kennen dus raakvlakken, zowel waar het gaat om de vraag welke dienstaanbieders onder de reikwijdte vallen als inhoudelijk. Daarbij geldt dat de verordening, conform artikel 2, vierde lid en overweging 10, geen afbreuk mag doen aan de regels in de richtlijn audiovisuele mediadiensten.

7.1.3 Verordening terroristische online-inhoud

De Verordening terroristische online-inhoud (hierna: TOI-verordening) heeft tot doel om misbruik van hostingdiensten voor terroristische doeleinden tegen te gaan. Voor dat doel bevat de verordening onder meer verschillende zorgplichten die door aanbieders van hostingdiensten moeten worden nagekomen om de verspreiding van terroristische online-inhoud tegen te gaan en, zo nodig, de snelle verwijdering of blokkering van dergelijke inhoud te garanderen. De verordening schrijft ook voor welke maatregelen de lidstaten moeten invoeren om terroristische inhoud te identificeren en de snelle verwijdering ervan te garanderen en om samenwerking tussen de bevoegde autoriteiten van lidstaten, aanbieders van hostingdiensten en, waar passend, Europol te faciliteren. De TOI-verordening verplicht tot het aanwijzen van een autoriteit die verwijderingsbevelen kan uitvaardigen om terroristische online-inhoud ontoegankelijk te doen maken. In Nederland wordt dat de Autoriteit Online Terroristisch en Kinderpornografisch Materiaal.[119]

De Verordening terroristische online-inhoud richt zich dus op een subtype tussenhandeldienst, namelijk de hostingdienst, en een subtype van illegale inhoud, namelijk terroristische online-inhoud. Waar het om terroristische online-inhoud gaat heeft de TOI-verordening als *lex specialis* dus voorrang en is de digitaledienstenverordening, als *lex generalis*, aanvullend.

7.1.4 Auteursrecht in de digitale eengemaakte markt

De richtlijn inzake auteursrechten en naburige rechten in de digitale eengemaakte markt[120] (hierna: DSM-richtlijn) stelt voorschriften vast met het oog op verdere harmonisatie van het Unierecht met betrekking tot het auteursrecht en naburige rechten in het kader van de interne markt, met name rekening houdend met digitaal en grensoverschrijdend gebruik van beschermde content.

Zowel de digitaledienstenverordening als de DSM-richtlijn leggen verplichtingen op met betrekking tot de wijze waarop (bepaalde) online platforms omgaan met illegale informatie. De verordening doet dat voor illegale inhoud in het algemeen, artikel 17 DSM-richtlijn doet dat specifiek voor inhoud die inbreuk maakt op het auteursrecht. Artikel 17 van de DSM-richtlijn introduceert een speciaal aansprakelijkheidsregime voor zogenaamde "aanbieders van onlinediensten voor het delen van inhoud", dat afwijkt van het regime voor hostingdiensten in de richtlijn elektronische handel (vervangen door de verordening).

Sommige partijen die kwalificeren als "online platform" of soms zelfs als "zeer groot online platform" in de zin van de verordening zullen tevens kwalificeren als "aanbieder van onlinediensten voor het delen van inhoud" in de zin van artikel 17 DSM-richtlijn. In dat laatste geval zal de aanbieder in ieder geval aan het *lex specialis* regime van artikel 17 DSM-richtlijn moeten voldoen en is de aansprakelijkheidsvrijwaring voor hostingdiensten niet van toepassing. Dat laat onverlet dat de

[119] Zie Stb. 2023, 122.
[120] Richtlijn (EU) 2019/790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG (PbEU 2019, L130).

verordening van toepassing is waar het aangelegenheden betreft die niet of niet volledig door artikel 17 DSM-richtlijn worden aangepakt, of waar artikel 17 DSM-richtlijn de lidstaten ruimte laat.

7.1.5 Consumentenrecht

Eén van de doeleinden van de digitaledienstenverordening is het bereiken van een hoog niveau van consumentenbescherming. Dat streven komt onder meer naar voren in de speciale regel voor de consumentenrechtelijke aansprakelijkheid van online platforms die consumenten de mogelijkheid bieden overeenkomsten op afstand te sluiten met handelaren (artikel 6, derde lid, van de verordening, zie paragraaf 3.2.1.2). Daarnaast bevat de verordening een specifieke regeling voor dergelijke B2C online marktplaatsen in afdeling 4 van hoofdstuk III. Die regeling moet in essentie waarborgen dat B2C online marktplaatsen bijdragen aan de goede naleving van de verplichtingen die onder het Europese consumentenrecht al gelden voor handelaren. De *know-your-business customer*- en *compliance by design*-verplichtingen moeten handelaren in staat stellen om aan hun verplichtingen onder het Europese consumentenrecht te voldoen. De verordening bevat zelf dus geen nieuwe verplichtingen die direct worden opgelegd aan handelaren.

7.1.6 Algemene verordening gegevensbescherming

De verordening doet geen afbreuk aan de AVG, die het algemene kader voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens biedt.

De regels in de verordening over reclame gaan op sommige punten verder dan wat de AVG vereist. Zo mogen aanbieders van online platforms op grond van artikel 26, derde lid, van de verordening geen reclame tonen gebaseerd op profilering met gebruikmaking van zogenaamde bijzondere categorieën persoonsgegevens. Voor de definitie van de begrippen “profilering” en “bijzondere categorieën persoonsgegevens” wordt in de verordening verwezen naar de AVG. Voor platforms die toegankelijk zijn voor minderjarigen geldt bovendien een verbod op het tonen van reclame op basis van profilering (artikel 28, tweede lid, van de verordening). Dit zijn categorale verboden, die de AVG niet kent. Dit vanwege de potentieel bijzonder ernstige negatieve gevolgen van online reclame. Ten slotte geldt voor aanbieders van zeer grote online platforms en zeer grote online zoekmachines dat zij in ieder geval moeten voorzien in een optie voor een aanbevelingssysteem dat niet gebaseerd is op profilering in de zin van de AVG (artikel 38 van de verordening). De AVG kent een vergelijkbare bepaling niet.

7.1.7 Platform-to-business verordening

De P2B-verordening[121] legt transparantievereisten op aan platforms in hun relatie met zakelijke gebruikers die goederen of diensten via die platforms aanbieden aan consumenten en bevat bepalingen over geschillenbeslechting tussen deze partijen. Voorbeelden van online platforms die onder de P2B-verordening vallen zijn online marktplaatsen waarop ondernemers goederen of diensten aanbieden, reserveringsplatforms, vergelijkingssites en appstores.[122]

De P2B-verordening heeft tot doel te zorgen voor een eerlijke en voorspelbare bedrijfsomgeving voor zakelijke gebruikers die platforms gebruiken om hun goederen of diensten aan te bieden op de

[121] Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van online tussenhandeldiensten (PBEU 2019, L 186). Het voorstel voor de Uitvoeringswet P2B-verordening belast de ACM met het toezicht op naleving en de handhaving van de P2B-verordening. Dit wetsvoorstel is thans aanhangig bij de Tweede Kamer (Kamerstukken II, 2022/23, 36 285, nr. 2).
[122] Overweging 11 van de P2B-verordening.

Europese interne markt. Het doel en de reikwijdte van de P2B-verordening en de digitaledienstenverordening komen dus deels overeen. Beide beogen bij te dragen aan een voorspelbare en betrouwbare online omgeving. Belangrijkste verschil is dat de P2B-verordening dat uitsluitend doet voor zakelijke gebruikers van platforms, terwijl de digitaledienstenverordening ook andere afnemers beoogt te beschermen. De digitaledienstenverordening is verder van toepassing op een bredere groep tussenhandeldiensten dan de P2B-verordening, die enkel geldt voor, kort gezegd, online platforms die zakelijke gebruikers de mogelijkheid geven om goederen of diensten aan te bieden aan consumenten, met het oog op het faciliteren van directe transacties tussen die zakelijke gebruikers en consumenten.

De beide verordeningen hebben deels betrekking op dezelfde onderwerpen. Zo hebben beide verordeningen bijvoorbeeld betrekking op de algemene voorwaarden[123] en de opzegging van de dienstverlening aan de (zakelijke) gebruiker.[124] Ook bevatten beide verordeningen voorschriften over de rangschikking van inhoud.[125] Belangrijk verschil is dat de digitaledienstenverordening, anders dan de P2B-verordening, verder gaat dan enkel het voorschrijven van transparantie, maar ook inhoudelijke verplichtingen over die onderwerpen bevat.

7.1.8 De verordening inzake algemene productveiligheid

Op 23 mei 2023 is de nieuwe verordening inzake algemene productveiligheid[126] in het Publicatieblad gepubliceerd. De verordening wordt van toepassing met ingang van 13 december 2024. Zoals toegelicht in paragraaf 4.3.5.3 van deze memorie van toelichting, bevat de verordening inzake algemene productveiligheid specifieke voorschriften voor aanbieders van B2C online marktplaatsen die, wat betreft productveiligheid, voortbouwen op de verplichtingen uit de digitaledienstenverordening of deze verplichtingen aanvullen.

De verordening inzake algemene productveiligheid kwalificeert als *lex specialis* ten opzichte van de verordening. Zo bevat artikel 22 van de verordening inzake algemene productveiligheid specifieke met productveiligheid verband houdende verplichtingen voor aanbieders van online marktplaatsen. De bepaling verwijst onder meer naar de artikelen 11, 12, 16 en 23 van de digitaledienstenverordening en bevat concrete voorschriften die gelden “met het oog op de naleving van artikel 31, derde lid,” van de digitaledienstenverordening. Die voorschriften houden onder meer in dat aanbieders van online marktplaatsen, wat productveiligheid betreft, gebruik dienen te maken van het Safety Gate Portal en dat zij voor elk aangeboden product bepaalde informatie dienen te verstrekken.

8 Gevolgen

8.1 *Regeldruk en nalevingslasten van de Uitvoeringswet*

Met de concept Uitvoeringswet wordt uitvoering gegeven aan de verordening. Omdat de verordening rechtstreeks doorwerkt in de nationale rechtsorde, heeft het voorliggende wetsvoorstel geen directe gevolgen voor bedrijfsleven en burgers. Die gevolgen volgen immers uit de verordening zelf. Aanbieders van tussenhandeldiensten moeten zich houden aan de verplichtingen die vanuit de

[123] Artikel 3 van de P2B-verordening en artikel 14 van de digitaledienstenverordening.
[124] Artikel 4 van de P2B-verordening en artikel 17 van de digitaledienstenverordening.
[125] Artikel 5 van de P2B-verordening en artikel 27 van de digitaledienstenverordening.
[126] Verordening (EU) 2023/988 van het Europees Parlement en de Raad van 10 mei 2023 inzake algemene productveiligheid, tot wijziging van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad en Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad, en tot intrekking van Richtlijn 2001/95/EG van het Europees Parlement en de Raad en Richtlijn 87/357/EEG van de Raad (PbEU 2023, L 135).

verordening op hen rusten. Op de administratieve lasten en nalevingskosten die rechtstreeks uit de verordening volgen, kan nationale wetgeving geen invloed uitoefenen.

De verordening verplicht lidstaten om nationale bevoegde autoriteiten aan te wijzen die verantwoordelijk zijn voor het toezicht op en de handhaving van de verordening. In Nederland worden in dit verband de ACM en de AP als bevoegde autoriteiten aangewezen. Door het toezicht kunnen regeldrukkosten ontstaan voor het bedrijfsleven. Aanbieders van tussenhandeldiensten met hun hoofdvestiging in Nederland zijn immers onderworpen aan het toezicht en handhaving door de ACM en de AP op de naleving van de verordening. Dit kan regeldrukeffecten hebben voor die tussenhandeldiensten. De uitoefening van onderzoeks- of handhavingsbevoegdheden door de ACM of AP kan het bijvoorbeeld noodzakelijk maken om kosten te maken, zoals het verzamelen en aanleveren van informatie als die wordt gevorderd of het wijzigen van processen of diensten om een overtreding weg te nemen.

8.2 *Uitvoeringslasten direct voortvloeiend uit de verordening*

De Commissie heeft in 2020 een impactanalyse (*impact assessment*) uitgevoerd naar de gevolgen van drie verschillende beleidsopties die voorafgingen aan het uiteindelijke voorstel voor de verordening.[127] Daarbij heeft de Commissie niet alleen gekeken naar de economische gevolgen van de verschillende opties, maar ook naar de gevolgen voor internationale handel, sociale gevolgen en de gevolgen voor de bescherming van grondrechten. De drie opties die zijn onderzocht zijn (1) het opleggen van een beperkt aantal nieuwe verplichtingen aan tussenhandeldiensten ten behoeve van de bestrijding van illegale inhoud (“*limited measures against illegal activity*”), (2) volledige harmonisatie van de verplichtingen voor aanbieders van tussenhandeldiensten binnen de EU (“*full harmonisation*”), en (3) de maatregelen uit optie 2 gecombineerd met asymmetrische maatregelen met strengere verplichtingen voor zeer grote online platforms, en een systeem voor vergaande samenwerking tussen toezichthouders op EU-niveau (“*asymmetric measures and EU governance*”).

Uit de analyse blijkt dat de kans dat de beleidsdoelstellingen worden bereikt zonder buitensporige kosten het grootst is bij de derde optie. Deze optie, waarbij de zorgvuldigheidsverplichtingen proportioneel zijn aan de grootte en het bereik van een tussenhandeldienst, is inderdaad de optie die ook terug te zien is in de verordening (en het eerste voorstel daarvoor).

De Commissie concludeert in de impactanalyse dat de grensoverschrijdende digitale handel met 1% tot 1,8% zal toenemen bij deze derde, uiteindelijk gekozen, optie. Dit komt naar schatting overeen met een toename van de grensoverschrijdende omzet tussen de 8,6 miljard euro en 15,5 miljard euro. Kleine, opkomende tussenhandeldiensten krijgen volgens de impact analyse verder de kans om toe te treden tot de markt zonder dat zij gebukt gaan onder te zware zorgvuldigheidsverplichtingen, terwijl de risico’s van de grotere tussenhandeldiensten adequaat geadresseerd worden door die diensten juist aan zwaarder verplichtingen te onderwerpen. De impactanalyse concludeert verder dat transparantie, online veiligheid en de bescherming van grondrechten zal toenemen, wat zowel bedrijven als consumenten ten goede komt.

De directe kosten voor aanbieders van tussenhandeldiensten staan volgens de impactanalyse verder in verhouding tot de omvang en het bereik van de tussenhandeldienst. Dit komt onder meer door de brede uitzonderingen van de verplichtingen voor het micro- en kleinbedrijf en het feit dat de zwaarste verplichtingen beperkt blijven tot de allergrootste online platforms en online zoekmachines in de EU. Zij beschikken over de financiële mogelijkheden om deze kosten te dragen. De uitzonderingen voor het micro- en kleinbedrijf voorkomen verder dat de verordening hoge

[127] Commission Staff working document, Impact Assessment, COM (2020) 825 final, met name hoofdstuk 6.

toetredingsdrempels creëert waardoor de bestaande marktpartijen indirect beschermd zouden worden tegen nieuwe concurrenten.

8.2.1 Gevolgen voor aanbieders van tussenhandeldiensten

Alle drie de onderzochte opties brengen volgens de impactanalyse kosten met zich mee voor aanbieders van tussenhandeldiensten. Deze kosten zijn volgens de Commissie echter aanzienlijk lager dan de kosten die voortvloeien uit het bestaande en zich ontwikkelende, versnipperde samenspel van nationale regels. Voor een middelgroot bedrijf dat actief is in drie lidstaten leidt de harmonisatie van zorgvuldigheidsverplichtingen door de verordening volgens de Commissie tot een kostenreductie van zo'n € 400.000 per jaar. Voor middelgrote bedrijven die hun dienst aanbieden in 10 lidstaten zou dit oplopen naar tenminste € 4 miljoen per jaar, en zelfs € 11 miljoen in een extreem scenario met versnipperde regels voor aanbieders van tussenhandeldiensten in elk van de 27 lidstaten van de Unie. De kostenbesparingen zijn het grootst voor micro- en kleine ondernemingen, waar de huidige versnippering het aanbieden van diensten in meer dan twee lidstaten praktisch onmogelijk maakt.[128]

De directe kosten die voortvloeien uit de belangrijkste zorgvuldigheidsverplichtingen (die van alle onderzochte opties deel uitmaken) hangen volgens de impactanalyse in grote mate af van het aantal door een aanbieder van een tussenhandeldienst ontvangen meldingen en het aantal zaken dat escaleert naar buitengerechtelijke geschillenbeslechting. De impactanalyse noemt bedragen variërend van een eenmalige investering van € 15.000 voor het inrichten van het kennisgevings- en actiemechanisme tot kosten van € 1 miljoen voor een volume van 200 meldingen per dag.[129] Voor een gemiddelde onderneming die 50 meldingen per jaar ontvangt, waarvan 5% leidt tot discussie, kost naleving ongeveer € 15.000 per jaar.[130]

Aanbieders van tussenhandeldiensten moeten ook kosten maken voor de naleving van de verplichtingen inzake het (technisch) ontwerp van hun diensten, onderhoud en transparantieverplichtingen. Volgens de impactanalyse zullen deze kosten naar verwachting echter marginaal zijn en opgaan in de reguliere exploitatie- en ontwerpkosten die aanbieders van tussenhandeldiensten maken ten behoeve van hun bedrijfsvoering en de ontwikkeling van hun diensten. De kosten voor naleving van de rapportageverplichtingen gaan volgens de impactanalyse door stroomlijning en harmonisatie van deze verplichtingen op EU-niveau eerder dalen dan stijgen.

De potentiële kosten voor de aanbieders van zeer grote online platforms zijn volgens de impactanalyse omvangrijker. Deze kosten vloeien onder meer voort uit vaste kosten die deze platforms moeten maken om jaarlijks risicobeoordelingen en audits uit te (laten) voeren, de benoeming van een compliancefunctie en rapportages aan de toezichthouder(s). De risicobeoordelingen kunnen bovendien nopen tot het nemen van risicobeperkende maatregelen. De kosten daarvan hangen volgens de impactanalyse in hoge mate af van het oorspronkelijke ontwerp van de systemen en de ernst van de risico's. In totaal variëren de extra kosten voor dergelijke, zeer grote online platforms tussen de € 300.000 en € 3.500.000 per jaar. Als er aanvullende risicobeperkende maatregelen moeten worden getroffen dan komen hier extra variabele kosten bovenop.[131]

---

[128] Commission Staff working document, Impact Assessment, COM (2020) 825 final, p. 53, 55.
[129] Commission Staff working document, Impact Assessment, COM (2020) 825 final, p. 54.
[130] Commission Staff working document, Impact Assessment, COM (2020) 825 final, p. 55.
[131] Commission Staff working document, Impact Assessment, COM (2020) 825 final, p. 53-54.

8.2.2 Gevolgen voor het mkb

Voor het midden- en kleinbedrijf (mkb) nemen de kosten volgens de impactanalyse af. Volgens de Commissie zijn de kosten die de juridische versnippering van regels voor tussenhandeldiensten creëren onbetaalbaar voor het micro- en kleinbedrijf. De verordening maakt het voor veel kleine en middelgrote bedrijven haalbaarder om de interne markt te betreden en op te schalen. De introductie van geharmoniseerde standaarden voor bijvoorbeeld meldingen zou de verwachte kosten voor kleine ondernemingen verder moeten verlagen.[132] Voor het mkb is ook van belang dat de verordening ruime uitzonderingen bevat voor micro- en kleine ondernemingen.

8.2.3 Gevolgen voor afnemers

De verordening zal positieve effecten hebben voor afnemers. In de impactanalyse concludeert de Commissie dat de verordening zal bijdragen aan een toename van de online veiligheid en de bescherming van consumenten. De verordening heeft bovendien een positieve impact op de (uitoefening en bescherming van) grondrechten, waaronder met name de vrijheid van meningsuiting, het recht op non-discriminatie, het recht op privacy en de bescherming van persoonsgegevens, het recht op eigendom en de rechten van het kind.[133]

Onder de verordening (artikel 53) wordt het voor afnemers verder mogelijk om een klacht in te dienen bij de ACM over de naleving van de verordening door een aanbieder van een tussenhandeldienst. De ACM kan naar aanleiding van die klacht een onderzoek starten naar de vermeende niet-naleving van de verordening door een aanbieder van een tussenhandeldienst. Deze mogelijkheid vormt een ondersteunende en laagdrempelige manier voor afnemers om op te komen tegen niet-naleving van de verordening door aanbieders van tussenhandeldiensten.

Afnemers profiteren verder van de in de verordening voorgeschreven transparantie, onder andere met betrekking tot inhoudsmoderatie en aanbevelingssystemen, en de verhaalsmogelijkheden waarin de verordening voorziet.

8.2.4 Gevolgen voor toezichthouders

Dat de inwerkingtreding van de verordening leidt tot extra taken en noodzakelijke inzet van de ACM en de AP is evident. Dat geldt met name voor de ACM, die de taak krijgt van digitaledienstencoördinator en toezicht zal houden op de meeste bepalingen neergelegd in de verordening. Digitaledienstencoördinatoren zullen volgens de impactanalyse kosten moeten maken. Daar staat volgens de impactanalyse echter tegenover dat de kosten als gevolg van de inefficiënties en doublures in de bestaande opzet voor de samenwerking tussen lidstatelijke autoriteiten aanzienlijk zullen verminderen.

De impactanalyse gaat uit van kosten variërend tussen de 0,5 FTE en 25 FTE's – afhankelijk van het aantal aanbieders van tussenhandeldiensten dat gevestigd is in de lidstaat in kwestie – voor het houden van toezicht op de zorgvuldigheidsverplichtingen die gelden voor alle aanbieders van tussenhandeldiensten.

Het toezicht op de aanvullende verplichtingen voor online platforms hangt volgens de impactanalyse af van het aantal onderzoeken/inspecties dat uitgevoerd zal worden. De kosten voor één inspectie

[132] Commission Staff working document, Annex 3 accompanying the Impact Assessment, COM (2020) 825 final, p. 49.
[133] Commission Staff working document, Impact Assessment, COM (2020) 825 final, p. 60-66.

worden geschat tussen de
€ 50.000 en € 300.000.[134]

9 Adviezen en consultatie

Zowel de ACM als de AP hebben een toets uitgevoerd op de uitvoerbaarheid en handhaafbaarheid van het wetsvoorstel ("UHT").

9.1 *ACM*

[Invullen op basis van UHT door de ACM]

[+ toezichtkosten en handhavingskosten]

9.2 *AP*

[Invullen op basis van UHT door de ACM]

[+ toezichtkosten en handhavingskosten]

9.3 *Internetconsultatie*

Het wetsvoorstel is in internetconsultatie gegeven van [datum] tot [datum].

[134] Commission Staff working document, Impact Assessment, COM (2020) 825 final, p. 56-57.

B. ARTIKELSGEWIJZE TOELICHTING

Artikel 1.1

In dit voorgestelde artikel worden enkele begrippen die in het wetsvoorstel worden gebruikt van een definitie voorzien. De definities van “Autoriteit Consument en Markt”, “Autoriteit persoonsgegevens” en “digitaledienstenverordening” behoeven geen nadere toelichting. De begrippen “aanbieder van een tussenhandeldienst” en “digitaledienstenraad” worden gebruikt in de digitaledienstenverordening en in onderhavig wetsvoorstel. Voor de definitie van deze begrippen wordt verwezen naar de verordening.

De ACM en de AP kunnen op grond van de artikelen 2.5 en 3.6 van het wetsvoorstel een zelfstandige last opleggen ter uitvoering van de verordening. Dit is nader toegelicht in de paragrafen 5.3.4.2 en 5.3.5.2 van het algemene deel van deze memorie van toelichting. In de definitie van het begrip “zelfstandige last” wordt verwezen naar artikel 5:2, tweede lid, van de Awb, waarin is bepaald dat de enkele last tot het verrichten van bepaalde handelingen geen bestuurlijke sanctie is. Een dergelijke last is gericht op naleving van de betreffende wettelijke bepalingen en heeft als zodanig geen sanctionerend karakter. Een dergelijke last kan ook worden opgelegd als er (nog) geen sprake van een overtreding van een wettelijke bepaling.

Artikel 2.1

In het eerste lid van dit voorgestelde artikel wordt de ACM als digitaledienstencoördinator aangewezen. Zie voor een toelichting hierop nader paragraaf 5.2.2.2 van het algemene deel van deze memorie van toelichting. In het tweede lid is bepaald dat de ACM bevoegd zal zijn om de taken uit te voeren en de bevoegdheden uit te oefenen die in de digitaledienstenverordening zijn opgedragen aan de digitaledienstencoördinator. Deze taken en bevoegdheden zijn toegelicht in paragraaf 5.3 en 5.4 van het algemene deel van deze memorie van toelichting. Met de bewoording “krachtens de verordening” wordt rekening gehouden met de mogelijkheid dat er in de door de Commissie vast te stellen uitvoeringsverordeningen taken of bevoegdheden bij de digitaledienstencoördinator worden belegd.

Het derde en vierde lid van het voorgestelde artikel zien tot slot op de uitsluiting en de beperking van enkele bevoegdheden van de minister van EZK op grond van de Kaderwet ZBO’s, vanwege de door de verordening vereiste volledige onafhankelijkheid van de digitaledienstencoördinator. Dit is nader toegelicht in paragraaf 5.2.2.1 van het algemene deel van deze memorie van toelichting.

Artikel 2.2

In dit voorgestelde artikel wordt de ACM belast met het toezicht op de naleving van het grootste deel van de verplichtingen in de verordening. Artikel 12a van de Instellingswet ACM bevat de grondslag voor de ACM om bij besluit de ambtenaren aan te wijzen die belast zijn met de uitvoering van het toezicht van op de naleving van wettelijke voorschriften dat is opgedragen aan de ACM. Om die reden wordt in onderhavig artikel de ACM aangewezen als toezichthouder, terwijl in artikel 3.2 van het wetsvoorstel bepaalde ambtenaren van de AP worden aangewezen als toezichthoudende ambtenaren.

Artikelen 2.3 en 2.4

De voorgestelde artikelen zien op de bevoegdheid van de ACM om ter handhaving van de bepalingen waar zij toezicht op houden, een bestuurlijke boete of een last onder dwangsom op te leggen. Op grond van artikel 12m, eerste lid, van de Instellingswet ACM beschikt de ACM in aanvulling daarop

over de bevoegdheid om een bestuurlijke boete op te leggen, onder meer wegens overtreding van een zelfstandige last en de plicht om medewerking te verlenen aan toezichthouders (artikel 5:20 Awb). Op grond van het derde lid van dat artikel van de Instellingswet kan de ACM ook een last onder dwangsom opleggen bij de overtreding van een zelfstandige last. De bevoegdheid om een bestuurlijke boete of een last onder dwangsom op te leggen is bij de overtreding van bepaalde artikelen van de verordening beperkt tot gevallen waarin er aanmerkelijke negatieve gevolgen zijn voor de veiligheid, voorspelbaarheid of betrouwbaarheid van de onlineomgeving (artikelen 2.3, tweede lid, en 2.4, tweede lid, van dit wetsvoorstel). Dit is toegelicht in paragraaf 5.3.6.2 van deze memorie van toelichting.

Het derde en vierde lid van artikel 52 van de verordening schrijft gedetailleerd voor wat de maximale hoogte van de bestuurlijke boete en de last onder dwangsom is. Naar deze maximale hoogte wordt verwezen in onderhavige artikelen van het wetsvoorstel. Ook de bestuurlijke boete en de last onder dwangsom die de ACM kan opleggen op grond van artikel 12m van de Instellingswet ACM zijn gemaximeerd overeenkomstig de verordening (zie artikel 2.3, derde lid, en artikel 2.4, derde lid, van het wetsvoorstel). De verordening maakt het op dit punt noodzakelijk om af te wijken van het kabinetsbeleid dat bij vaststellen van een maximale bestuurlijke boetehoogte wordt verwezen naar een van de boetecategorieën in het Wetboek van Strafrecht.[135]

Naast de algemene bepalingen over de last onder dwangsom uit de Awb, voorziet artikel 12r van de Instellingswet ACM in aanvullende regels voor de gevallen waarin de ACM bevoegd is tot het opleggen van een last onder dwangsom. Die regels zijn dat een last onder dwangsom ten hoogste twee jaar kan gelden, dat de bevoegdheid tot het opleggen van een last onder dwangsom na vijf jaar vervalt, gerekend vanaf het plaatsvinden van de overtreding, en dat de ACM aan een last onder dwangsom voorschriften kan verbinden inzake het verstrekken van gegevens aan de ACM. Indien de opgelegde last onder dwangsom of bestuurlijke boete verplicht tot betaling van een geldsom, komt deze geldsom toe aan de Staat (artikel 12t van de Instellingswet ACM).

Artikel 2.5

Het voorgestelde artikel 2.5, eerste lid, van het wetsvoorstel biedt de grondslag voor de ACM om een zelfstandige last op te leggen, in de vorm van een voorlopige maatregel (artikel 51, tweede lid, onderdeel e, van de verordening), een maatregel om het leidinggevende orgaan van een aanbieder te verplichten een actieplan op te stellen en uit te voeren (artikel 51, derde lid, onderdeel a, van de verordening) en een maatregel om de toegang van afnemers tot de dienst van een aanbieder tijdelijk te beperken (artikel 51, derde lid, onderdeel a, van de verordening). Zie voor een toelichting hierop nader paragrafen 5.3.4 en 5.3.5 van het algemene deel van deze memorie van toelichting.

Op grond van het tweede lid van artikel 2.5 van het wetsvoorstel is het verboden in strijd te handelen met een zelfstandige last als bedoeld in het eerste lid van het artikel. Bij overtreding van dit verbod is de ACM op grond van artikel 12m, eerste lid, van de Instellingswet ACM bevoegd tot het opleggen van een bestuurlijke boete of een last onder dwangsom. Een last onder dwangsom kan ook gelijktijdig met de zelfstandige last worden opgelegd, als de omstandigheden van het geval daar aanleiding toe geven.

Het derde en vierde lid van dit artikel hebben betrekking op de mogelijkheid van de ACM om advies te vragen aan het OM over strafvorderlijke aspecten bij de voorbereiding van een besluit tot het

[135] Zie Aanwijzing 5.43 van de Aanwijzingen voor de regelgeving.

opleggen van de zelfstandige last, bedoeld in het eerste lid, onderdeel c, van dit artikel. Zie voor een toelichting hierop nader paragraaf 5.3.5.2 van het algemene deel van deze memorie van toelichting.

Artikel 2.6

Artikel 2.6 van het wetsvoorstel bevat nadere voorschriften over de voorafgaande machtiging van de rechter-commissaris die vereist is voordat de ACM een zelfstandige last als bedoeld in artikel 2.5, eerste lid, onderdeel c, van het wetsvoorstel kan opleggen. Zie voor een nadere toelichting op deze zelfstandige last paragraaf 5.3.5.2 van het algemene deel van deze memorie van toelichting.

De machtiging wordt verleend door de rechter-commissaris, belast met de behandeling van strafzaken bij de rechtbank Rotterdam. Daar is voor gekozen vanwege de rol die het strafrecht speelt bij het opleggen van de zelfstandige last en omdat de beroepen tegen besluiten van de ACM zijn geconcentreerd bij de rechtbank Rotterdam. De rechter-commissaris dient de voorgenomen maatregel te toetsen op proportionaliteit, ook in het licht van de betrokken grondrechten zoals de vrijheid van meningsuiting en de vrijheid van informatie. Dit vloeit voort uit de verordening, namelijk dat een opgelegde maatregel in verhouding moet staan tot de aard, de ernst, de herhaling en de duur van de inbreuk, zonder onnodige beperking van de toegang tot wettelijke informatie door afnemers van de dienst (artikel 51, derde lid, onderdeel b, tweede alinea, laatste volzin, van de verordening). In het voorgestelde eerste lid van onderhavig artikel wordt bepaald dat de ACM dit aspect moet motiveren in haar verzoek om afgifte van de machtiging.

De Commissie kan de ACM ook verzoeken om een zelfstandige last als bedoeld in artikel 2.5, eerste lid, onderdelen b en c, van het wetsvoorstel op te leggen (artikel 82, eerste lid, van de verordening). Ook in de gevallen dat de Commissie de ACM verzoekt om een zelfstandige last als bedoeld in artikel 2.5, eerste lid, onderdeel c, van het wetsvoorstel, is een machtiging van de rechter-commissaris vereist. In het derde lid van het voorgestelde artikel 2.6 is bepaald dat de Commissie schriftelijke, en met toestemming van de rechter-commissaris mondelinge, opmerkingen kan maken. De rechter-commissaris verstrekt voorts de documenten aan de Commissie waar die om verzoekt, om de Commissie in staat te stellen de zaak te beoordelen (artikel 2.6, vierde lid, van het wetsvoorstel).

Artikel 2.7

Artikel 57, tweede lid, van de verordening schrijft voor dat de digitale dienstencoördinator van de lidstaat onderzoeksbevoegdheden uitoefent op verzoek van een andere digitale dienstencoördinator. Op grond van artikel 66, derde lid, van de verordening geldt hetzelfde op verzoek van de Commissie. De nationale ambtenaren oefenen daarbij hun bevoegdheden uit overeenkomstig het nationale recht. Het voorgestelde artikel bepaalt dat de toezichthoudende ambtenaren van de ACM zijn belast met de uitoefening van de onderzoeksbevoegdheden en dat zij daarbij beschikken over dezelfde bevoegdheden als bij het toezicht in het kader van artikel 2.2 van het wetsvoorstel.

Artikel 2.8

In het voorgestelde eerste lid van artikel 2.8 van het wetsvoorstel worden de ambtenaren van de ACM belast met het verlenen van bijstand bij inspecties door de Commissie in het kader van het toezicht door de Commissie op de naleving van de verordening door aanbieders van zeer grote online platforms en zeer grote online zoekmachines die in Nederland zijn gevestigd. Deze bepalingen zijn toegelicht in paragraaf 5.3.9 van deze memorie van toelichting.

De functionarissen van de Commissie hebben op grond van interne regels van de Commissie een legitimatieplicht. Er is echter niet voorzien in een legitimatieplicht voor de nationale ambtenaren die bijstand verlenen. In artikel 5:12 van de Awb is bepaald dat toezichthouders bij de uitoefening van

hun taak een legitimatiebewijs bij zich dienen te dragen, dat is uitgegeven door het desbetreffende bestuursorgaan. Omdat de bepalingen inzake het toezicht op de naleving van de Awb niet van toepassing zijn in het geval de ambtenaren van de ACM bijstand verlenen aan de Commissie, wordt artikel 5:12 van de Awb van overeenkomstige toepassing verklaard in het voorgestelde tweede lid.

In het voorgestelde derde lid worden de ambtenaren van de ACM belast met het verlenen van bijstand bij inspecties door de Commissie, in het geval de onderneming in kwestie zich tegen de inspectie verzet. De verleende bijstand moet de Commissie in staat stellen om alsnog de inspectie uit te voeren. De ambtenaren van de ACM zijn daarbij bevoegd om zo nodig de hulp van de sterke arm in te roepen. Het begrip 'sterke arm' omvat de ambtenaren van politie die zijn aangesteld voor de uitvoering van de politietaak (zie artikel 2, onderdelen a, c en d, van de Politiewet 2012), alsmede militairen van de Koninklijke marechaussee voor zover deze politietaken uitvoeren (zie artikel 4, eerste lid, van de Politiewet 2012). Het gebruik van dit begrip wordt voorgeschreven bij het regelen van de mogelijkheid om bij de uitoefening van een bevoegdheid de assistentie van de politie in te roepen.

Artikel 2.9

In het voorgestelde eerste en tweede lid van artikel 2.9 van het wetsvoorstel wordt de termijn bepaald waarbinnen de ACM een beslissing op een aanvraag tot toekenning van de status "erkend onderzoeker" dient te nemen. Deze beslistermijn is ingegeven door de complexiteit van de beoordeling van de aanvraag en het feit dat voorgesteld wordt dat de AP een advies uitbrengt aan de ACM ter voorbereiding van het besluit. Voor de overige besluiten die de ACM dient te nemen op grond van de verordening, zoals de toekenning van de status van "trusted flagger", zijn de regels inzake de beslistermijn van artikel 4:13 van de Awb afdoende. Zie voor een nadere toelichting op de toekenning van de status "erkend onderzoeker" paragraaf 4.3.6.7 van deze memorie van toelichting.

Het voorgestelde derde lid ziet op de advisering door de AP aan de ACM over het criterium "bescherming van persoonsgegevens". Het voorgestelde vierde lid bepaalt de adviestermijn, namelijk zeven weken. Afdeling 3.3 van de Awb is van toepassing op dit advies. Dit betekent onder meer dat het ontbreken van een advies, als dat niet tijdig wordt uitgebracht, niet in de weg staat aan het nemen van een besluit (artikel 3:6, tweede lid, van de Awb). Ook kan ter motivering worden volstaan met een verwijzing naar het uitgebrachte advies van de AP (artikel 3:49 Awb) en dient de ACM, indien zij afwijkt van het uitgebrachte advies, de redenen voor deze afwijking te vermelden (artikel 3:50 Awb). Op grond van de Awb kan de aanvrager tegen dit besluit bezwaar en beroep aantekenen en daarbij mede de inhoud van het advies aan de orde stellen.

Artikel 3.1

In artikel 3.1, eerste lid, van het wetsvoorstel wordt de AP aangewezen als bevoegde autoriteit in de zin van artikel 49, eerste lid, van de verordening, omdat zij samen met de ACM verantwoordelijk zal zijn voor het toezicht op de naleving van de verordening door aanbieders van tussenhandeldiensten. Zie voor een toelichting hierop nader paragraaf 5.2.2.3 van het algemene deel van deze memorie van toelichting. Het tweede en derde lid van onderhavig artikel zien op de uitsluiting en de beperking van enkele bevoegdheden van de minister van EZK op grond van de Kaderwet ZBO's, vanwege de door de verordening vereiste volledige onafhankelijkheid van de bevoegde autoriteiten (artikel 50 jo. artikel 49, vierde lid, van de verordening). Dit is nader toegelicht in paragraaf 5.2.2.1 van het algemene deel van deze memorie van toelichting.

Artikel 3.2

In artikel 3.2, eerste lid, van het wetsvoorstel worden de daar genoemde ambtenaren van de AP belast met het toezicht op de naleving van de artikelen 26, derde lid, en 28, tweede lid van de verordening. Zie voor een toelichting hierop nader paragraaf 5.2.2.3 van het algemene deel van deze memorie van toelichting. De genoemde ambtenaren zijn dezelfde als die op grond van artikel 15 van de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG) zijn belast met het toezicht op de naleving van de AVG en die wet.

Het tweede, derde en vierde lid van onderhavig artikel hebben betrekking op de toezichtsbevoegdheden van de toezichthoudende ambtenaren van AP. Op grond van het tweede lid beschikken zij niet over de bevoegdheid om vervoermiddelen te onderzoeken. Dit is nader toegelicht in paragraaf 5.3.2.2 van het algemene deel van deze memorie van toelichting. Op grond van het derde lid kunnen zij woningen betreden zonder toestemming van de bewoner. Op deze bevoegdheid is de Algemene wet op het binnentreden van toepassing, waaruit onder meer volgt dat voor het toepassen van deze bevoegdheid een voorafgaande machtiging van de burgemeester is vereist (artikelen 2 en 3 van de Algemene wet op het binnentreden).

De procedure voor deze bevoegdheid voor de AP wijkt daarmee af van de procedure die voor toepassing van deze bevoegdheid geldt voor de ACM op grond van de Instellingswet ACM, die onder meer voorziet in voorafgaande machtiging door de rechter-commissaris. Het kabinet acht het van belang dat de procedures voor de toepassing van dit soort bevoegdheden voor een toezichthouder zo veel mogelijk uniform is voor zijn verschillende wettelijke toezichtstaken. Daarom is gekozen om aan te sluiten bij de huidige procedure voor de AP.

De in het vierde lid opgenomen extra waarborg inhoudende dat de toezichthouder voor de uitoefening van de bevoegdheid van het tweede lid de uitdrukkelijke en bijzondere volmacht van de AP behoeft, bestaat eveneens reeds op grond van artikel 15 van de UAVG. Vanwege het belang van de uniformiteit van procedurele voorschriften is deze waarborg ook in onderhavig wetsvoorstel opgenomen.

Artikelen 3.3 en 3.4

De voorgestelde onderhavige artikelen zien op de bevoegdheid van de AP om een bestuurlijke boete of een last onder dwangsom op te leggen. Dit kan zij doen bij overtreding van de verordeningsbepalingen waar zij toezicht op houdt, de niet-naleving van een toezegging of een zelfstandige last of een overtreding van de plicht om medewerking te verlenen aan toezichthouders (artikel 5:20 Awb). Ingeval een overtreding ook strafbaar is gesteld in het Wetboek van Strafrecht, zijn de desbetreffende bepalingen van het Wetboek van Strafrecht buiten toepassing verklaard. Het derde en vierde lid van artikel 52 van de verordening schrijven gedetailleerd voor wat de maximale hoogte van de bestuurlijke boete en de last onder dwangsom is. Naar deze maximale hoogte wordt verwezen in onderhavige artikelen van het wetsvoorstel.

Artikel 3.5

Op grond van artikel 51, tweede lid, onderdeel a, van de verordening moeten de bevoegde autoriteiten over de bevoegdheid beschikken om toezeggingen door aanbieders van tussenhandeldiensten te aanvaarden en verbindend te maken. Onderhavig voorgesteld artikel voorziet in die bevoegdheid voor de AP. Zoals toegelicht in paragraaf 5.3.3.2 van deze memorie van toelichting, beschikt de ACM op grond van artikel 12h van de Instellingswet ACM al over deze bevoegdheid in het kader van al haar wettelijke toezichtstaken en dient daarvoor niets geregeld te

worden in het wetsvoorstel. De bevoegdheid van de AP om een toezegging te aanvaarden en verbindend te maken is in onderhavig artikel op dezelfde wijze vormgegeven als onder artikel 12h van de Instellingswet ACM.

De procedure om deze bevoegdheid toe te passen is als volgt. De desbetreffende aanbieder kan een aanvraag doen bij de AP voor het bindend verklaren van een toezegging en dient daarbij de noodzakelijke gegevens en bescheiden te voegen (artikel 3.5, eerste lid, van het wetsvoorstel). De aanvraag kan gedaan worden zolang de AP nog geen besluit omtrent het opleggen van een bestuurlijke boete of last onder dwangsom heeft genomen (artikel 3.5, derde lid, van het wetsvoorstel). Dat kan dus ook in de fase zijn dat het toezichtsonderzoek nog loopt en er nog geen overtreding is vastgesteld. De vervaltermijn voor het opleggen van een bestuurlijke boete, bedoeld in artikel 5:45, eerste lid, van de Awb, wordt opgeschort tot de AP op de aanvraag heeft beslist (artikel 3.5, vierde lid, van het wetsvoorstel). Indien de aanvrager zou opkomen tegen het besluit tot bindendverklaring, wordt die termijn eveneens opgeschort door de van overeenkomstige toepassing verklaring van artikel 5:45, derde lid, van de Awb.

Het rechtsgevolg van de bindendverklaring is dat de bevoegdheid van de AP vervalt om in de desbetreffende zaak een boete of last onder dwangsom op te leggen. Mocht blijken dat de bindendverklaring is gebaseerd op door de aanbieder verstrekte onvolledige, onjuiste of misleidende gegevens of dat de aanbieder zich niet overeenkomstig het besluit tot bindendverklaring gedraagt, dan kan de AP dit besluit wijzigen of intrekken en herleeft de mogelijkheid tot het nemen van een besluit tot het opleggen van een bestuurlijke boete of last onder dwangsom (artikel 3.5, zevende lid, van het wetsvoorstel). Alsdan is het zinvol om het toezichtsonderzoek voor het opleggen van een dergelijke sanctie te starten. Voor het niet-naleven van het besluit tot bindendverklaring van de toezegging, kan de AP de desbetreffende aanbieder een bestuurlijke boete of een last onder dwangsom opleggen op grond van de artikelen 3.3 en 3.4 van het wetsvoorstel.

Artikel 3.6

Krachtens artikel 51, tweede lid, onderdeel b, van de verordening dienen de bevoegde autoriteiten over de bevoegdheid te beschikken om een bindende aanwijzing op te leggen. Artikel 3.6, eerste lid, voorziet in deze bevoegdheid voor de AP. Een bindende aanwijzing wordt opgelegd als sprake is van een overtreding. De bindende aanwijzing is een zelfstandige last in de zin van artikel 5:2, tweede lid, van de Awb, omdat het gaat om de enkele last tot het verrichten van bepaalde handelingen ter bevordering van de naleving van wettelijke voorschriften.

Het voorgestelde artikel 3.6, tweede lid, van het wetsvoorstel biedt de grondslag voor de AP om een zelfstandige last op te leggen, in de vorm van een voorlopige maatregel (artikel 51, tweede lid, onderdeel e, van de verordening) of een maatregel om het leidinggevende orgaan van een aanbieder te verplichten een actieplan op te stellen en uit te voeren (artikel 51, derde lid, onderdeel a, van de verordening). Zie voor een toelichting hierop nader paragrafen 5.3.4 en 5.3.5 van het algemene deel van deze memorie van toelichting.

Op grond van het derde lid van artikel 3.6 van het wetsvoorstel is het verboden in strijd te handelen met een zelfstandige last als bedoeld in het eerste lid of tweede lid van het artikel. Bij overtreding van dit verbod is de AP op grond van de artikelen 3.3 en 3.4 bevoegd tot het opleggen van een bestuurlijke boete of een last onder dwangsom. Een last onder dwangsom kan ook gelijktijdig met de zelfstandige last worden opgelegd, als de omstandigheden van het geval daar aanleiding toe geven.

Artikel 3.7

Artikel 57, tweede lid, van de verordening schrijft voor dat de digitaledienstencoördinator van de lidstaat onderzoeksbevoegdheden uitoefent op verzoek van een andere digitaledienstencoördinator. Op grond van artikel 66, derde lid, van de verordening geldt hetzelfde op verzoek van de Europese Commissie. De digitaledienstencoördinator kan daarbij andere bevoegde autoriteiten betrekken. De nationale ambtenaren oefenen daarbij hun bevoegdheden uit overeenkomstig het nationale recht. Het voorgestelde artikel bepaalt dat de ACM een dergelijk verzoek doorverwijst naar de AP als het betrekking heeft op het toezicht op de verordening dat door de AP wordt uitgeoefend op grond van artikel 3.2 van het wetsvoorstel (eerste lid). De toezichthoudende ambtenaren van de AP zijn belast met de uitoefening van de onderzoeksbevoegdheden en zij beschikken daarbij over dezelfde bevoegdheden als die waarover zij beschikken bij het toezicht in het kader van artikel 3.2 van het wetsvoorstel.

Artikel 4.1

Het voorgestelde artikel 4.1, eerste lid, voorziet – in aanvulling op artikel 19, tweede lid, van de UAVG (uitwisseling van persoonsgegevens tussen AP en andere toezichthouders) en artikel 7 van de Instellingswet ACM (verstrekking van gegevens door de ACM) – in een grondslag voor het delen gegevens tussen de ACM en de AP. Zie hiervoor nader paragraaf 6.2.1 van het algemene deel van deze memorie van toelichting. In het tweede lid van artikel 4.1 is bepaald welke ondersteuning, informatie en gegevens de AP aan de ACM moet verstrekken ten behoeve van het jaarverslag van de ACM over de uitvoering van de verordening en voor het verstrekken van gegevens in het kader van verzoeken van digitaledienstencoördinatoren van andere lidstaten.

Artikel 4.2

Het voorgestelde artikel 4.2 bepaalt dat de ACM en de AP een samenwerkingsprotocol opstellen, waarvan in de Staatscourant mededeling wordt gedaan. Er kan ook worden gekozen om een bestaand samenwerkingsprotocol aan te passen, bijvoorbeeld het samenwerkingsprotocol tussen de ACM en AP in het kader van artikel 19, eerste lid, van de UAVG.

Artikel 4.3

Om een eenvormige uitleg van begrippen door de ACM en de AP te waarborgen is bepaald dat overeenstemming dient plaats te vinden indien de ACM en de AP dezelfde begrippen toepassen. Het gaat dan om begrippen die zowel worden gebruikt in de artikelen 26, derde lid, en 28, tweede lid, van de verordening, waar de AP toezicht op houdt, als in de bepalingen van de verordening waar de ACM toezicht op houdt. Het gaat van bijvoorbeeld om de begrippen “aanbieders van onlineplatforms”, “reclame”, “afnemers van de diensten” en “online-interface”. Dit voorgestelde artikel verplicht niet tot overeenstemming over de uitleg van begrippen die enkel worden gebruikt in de bepalingen waar de AP toezicht op houdt en die zijn gedefinieerd in de AVG, zoals “profilering” en “persoonsgegevens”.

Artikel 5.1

Vanwege het vervallen van artikel 196c van Boek 6 van het BW, wordt artikel V, derde lid, van de Aanpassingswet richtlijn inzake elektronische handel geschrapt. Zoals toegelicht in paragraaf 3.2.2.1 van deze memorie van toelichting, kan worden volstaan met de rechtstreekse werkende bepalingen uit de verordening.

Artikel 5.2

Voor beroep tegen besluiten van de ACM op grond van dit wetsvoorstel wordt aangesloten bij de gebruikelijke rechtsgang voor wettelijke voorschriften waar de ACM toezicht op houdt, dat wil zeggen dat de rechtsmacht in eerste aanleg toegedeeld wordt aan de rechtbank Rotterdam en in hoger beroep aan het College van Beroep voor het bedrijfsleven. Daartoe voorziet onderhavig artikel in de wijziging van bijlage 2 van de Awb.

Voor beroep tegen besluiten die op grond van dit wetsvoorstel zullen worden genomen door de AP, wordt niet voorzien in een bijzondere rechtsgang. Dat betekent dat beroepen tegen besluiten van de AP op grond van dit wetsvoorstel dienen te worden ingesteld bij de reguliere bestuursrechter en hoger beroep bij de Afdeling Bestuursrecht van de Raad van State.

De reden voor deze vormgeving van de rechtsmacht bij beroepen op grond van dit wetsvoorstel is dat hiermee wordt aangesloten bij de rechtsmachtsverdeling zoals voorzien in andere wetten op grond waarvan de ACM en de AP besluiten nemen. Dit is in het belang van de uniformiteit van de werkwijze van deze toezichthouders en komt de uitvoerbaarheid ten goede. Voor de bepalingen van de verordening waar de AP op toezicht zal houden (de artikelen 26, derde lid, en 28, tweede lid, van de verordening) geldt bovendien dat die inhoudelijk aansluiten op het toezicht dat de AP uitoefent krachtens de UAVG, waardoor het in de rede ligt om ook dezelfde rechters bevoegd te maken bij beroepen op grond van die wet en dit wetsvoorstel.

Artikel 5.3

Vanwege het vervallen van artikel 196c van Boek 6 van het BW, wordt voorgesteld om in artikel 29e van de Auteurswet de verwijzing naar het vierde lid die bepaling te vervangen door een verwijzing naar het direct werkende artikel 6 van de verordening. Artikel 29e van de Auteurswet vormt de implementatie van artikel 17, derde lid, van de richtlijn auteursrecht in de digitale eengemaakte markt[136] en houdt in dat een aanbieder van een onlinedienst voor het delen van inhoud, die een beroep kan doen op het in artikel 29c dan wel artikel 29d van de Auteurswet bepaalde, geen beroep kan doen op de aansprakelijkheidsvrijstelling voor aanbieders van hostingdiensten.

Artikel 5.4

Dit artikel voorziet in het vervallen van artikel 196c van Boek 6 van het BW. Dit is nader toegelicht in paragraaf 3.2.2.1 van het algemene deel van deze memorie van toelichting.

Artikel 5.5

Vanwege het vervallen van artikel 196c van Boek 6 van het BW, wordt de verwijzing naar deze bepaling in 8.2, derde lid, van de Wet handhaving consumentenbescherming geschrapt.

Artikel 5.6

Onderhavig artikel voorziet in het toevoegen van een nieuw negende lid aan artikel 29, achtste lid, van het Wetboek van Burgerlijke Rechtsvordering, waarin is voorzien in de doorzending van civielrechtelijke bevelen in de zin de artikelen 9 en 10 van de verordening aan de ACM. De doorzending geschiedt door de griffier, door tussenkomst van de Raad voor de rechtspraak, behalve

[136] Richtlijn (EU) 2019/790 van het Europees Parlement en van de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG (PbEU 2019, L 130).

als het arresten of beschikkingen van de Hoge Raad betreft. Dit is nader toegelicht in paragraaf 3.4.2.1 van het algemene deel van deze memorie van toelichting.

Artikel 6.1

[PM]

Artikel 6.2

De implementatietermijn van de verordening is vastgesteld op 17 februari 2024. Dit wetsvoorstel dient daarom ook op deze datum in werking te treden, hetgeen vastgesteld wordt in het voorgestelde artikel 6.2. Wordt de wet na die datum gepubliceerd, dan treedt het wetsvoorstel onmiddellijk in werking. Hiermee wordt, overeenkomstig het kabinetsbeleid inzake vaste verandermomenten[137], afgeweken van het uitgangspunt dat wetsvoorstellen op 1 januari of 1 juli in werking treden met een minimuminvoeringstermijn van twee maanden. Deze uitzondering is gerechtvaardigd omdat dit wetsvoorstel de implementatie van een Europese verordening betreft.

Artikel 6.3

Dit artikel bevat de citeertitel van het wetsvoorstel.

[137] Kamerstukken II 2009/10, 29 515, nr. 309.

C. BIJLAGE BIJ DE TOELICHTING

Transponeringstabel

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 (digitaledienstenverordening) (PbEU L 2022, 277)

Bepaling verordening	*Bepaling in wetsvoorstel of bestaande regeling* *Toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie behoeft*	*Omschrijving beleidsruimte*	*Toelichting op de keuze(n) bij de invulling van de beleidsruimte*
Artikel 1 (Onderwerp)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 2 (Toepassingsgebied)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 3 (Definities)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 4 (Mere conduit)	Art. 6:196c BW vervalt (art 5.4 van dit wetsvoorstel) Implementatie door middel van bestaande regeling (art. 54a Sr) Zie § 3.2.2 van deze MvT	Geen	
Artikel 5 (Caching)	Art. 6:196c BW vervalt (art 5.4 van dit wetsvoorstel) Implementatie door middel van bestaande regeling (art. 54a Sr) Zie § 3.2.2 van deze MvT	Geen	
Artikel 6 (Hosting)	Art. 6:196c BW vervalt (art 5.4 van dit wetsvoorstel) Implementatie door middel van bestaande regeling (art. 54a Sr) Zie § 3.2.2 van deze MvT	Geen	
Artikel 7 (Vrijwillige onderzoeken op eigen initiatief en naleving van wetgeving)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 8 (Geen algemene verplichting tot monitoring of actief feitenonderzoek)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 9 (Aanbieders stellen autoriteit onverwijld in kennis van opvolgen bevel om op te treden tegen illegale inhoud)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 9, tweede lid (Eisen aan inhoud bevel)	Implementatie door middel van bestaande	Geen	

	regeling (art. 56 Rv, art. 125p Sv en art. 2:6 Awb); zie § 3.4.2 van deze MvT		
Artikel 9, derde lid (Beveluitvaardigende autoriteit zendt het bevel en ontvangen informatie door aan de digitaledienstencoördinator)	Nieuw art. 29, lid 9, Rv (art. 5.6 van het wetsvoorstel), zie § 3.4.2 van deze MvT	Geen	
Artikel 9, vierde lid (Digitaledienstencoördinator stuurt bevel door aan alle andere digitaledienstencoördinatoren)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 9, vijfde lid (Aanbieders stellen afnemers in kennis van het ontvangen bevel en het daaraan gegeven gevolg)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 9, zesde lid (Dit artikel doet geen afbreuk aan nationaal burgerlijk recht en strafprocesrecht)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 10, eerste lid (Aanbieders stellen autoriteit onverwijld in kennis van opvolgen bevel om informatie te verstrekken)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 10, tweede lid (Eisen aan inhoud bevel)	Implementatie door middel van bestaande regeling (art. 56 BW, artt. 126n/u/zh en 126ng/ug/zl Sv, artt. 2:6, 5:16 en 5:17 Awb); zie § 3.4.2 van deze MvT	Geen	
Artikel 10, derde lid (Beveluitvaardigende autoriteit zendt het bevel en ontvangen informatie door aan de digitaledienstencoördinator)	Nieuw art. 29, lid 9, Rv (art. 5.6 van het wetsvoorstel), zie § 3.4.2 van deze MvT	Geen	
Artikel 10, vierde lid (Digitaledienstencoördinator stuurt bevel door aan alle andere digitaledienstencoördinatoren)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 10, vijfde lid (Aanbieders stellen afnemers in kennis van het ontvangen bevel en het daaraan gegeven gevolg)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 10, zesde lid (Dit artikel doet geen afbreuk aan nationaal burgerlijk recht en strafprocesrecht)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 11 (Contactpunten voor lidstatelijke autoriteiten, de Commissie en de digitaledienstenraad)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 12 (Contactpunten voor afnemers)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 13 (Wettelijke vertegenwoordigers)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 14 (Algemene voorwaarden)	Behoeft naar zijn aard geen implementatie	Geen	

Artikel 15 (Transparantierapportageverplichtingen voor alle aanbieders)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 16 (Kennisgevings- en actiemechanismen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 17 (Motivering)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 18 (Kennisgeving van vermoedens van strafbare feiten)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 19 (Uitsluiting van micro- en kleine ondernemingen voor aanvullende bepalingen online platforms)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 20 (Intern klachtenafhandelingssyteem)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 21 (Buitengerechtelijke geschillenbeslechting)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 22 (Betrouwbare flaggers)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 23 (Maatregelen en bescherming tegen misbruik)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 24 (Aanvullende transparantierapportageverplichtingen voor online platforms)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 25 (Vormgeving en organisatie van online-interfaces)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 26 (Reclame op online platforms)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 27 (Transparantie van aanbevelingssystemen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 28 (Bescherming van minderjarigen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 29 (Uitsluiting van micro- en kleine ondernemingen voor aanvullende bepalingen B2C online marktplaatsen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 30 (Traceerbaarheid van handelaren)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 31 (Op conformiteit gericht ontwerp)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 32 (Recht op informatie)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 33 (Zeer grote online platforms en zeer grote online zoekmachines)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 34 (Risicobeoordeling)	Behoeft naar zijn aard geen implementatie	Geen	

Artikel 35 (Risicobeperking)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 36 (Crisisresponsmechanisme)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 37 (Onafhankelijke controle)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 38 (Aanbevelingssystemen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 39 (Bijkomende transparantie met betrekking tot online reclame)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 40 (Toegang tot gegevens en onderzoek)	Behoeft naar zijn aard geen implementatie Lid 8: art. 2.9 van het wetsvoorstel; zie § 5.4.3 van deze MvT	Geen	
Artikel 41 (Compliancefunctie)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 42 (Aanvullende transparantierapportageverplichtingen voor zeer grote online platforms en zeer grote online zoekmachines)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 43 (Toezichtsvergoeding)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 44 (Normen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 45 (Gedragscodes)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 46 (Gedragscodes voor online reclame)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 47 (Gedragscodes voor toegankelijkheid)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 48 (Crisisprotocollen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 49, eerste lid (Aanwijzing bevoegde autoriteiten) en 49 tweede lid, eerste en tweede alinea (Aanwijzing digitaledienstencoördinator)	Artt. 2.1 en 3.1 van dit wetsvoorstel	Lidstaat heeft de keuze om een of meer bevoegde autoriteiten aan te wijzen	Zie § 5.2.2 van deze MvT
Artikel 49, tweede lid, derde alinea (Nauwe en doeltreffende samenwerking bevoegde autoriteiten)	Hoofdstuk 4 van dit wetsvoorstel	Deze alinea verplicht de lidstaten om voor nauwe en doeltreffende samenwerking van bevoegde autoriteiten te zorgen	Zie hoofdstuk 6 van deze MvT
Artikel 49, derde lid (Mededeling naam en informatie digitaledienstencoördinator)	Behoeft naar zijn aard geen implementatie	Geen	

Artikel 49, vierde lid (Overeenkomstige toepassing bevoegde autoriteiten artikelen 50, 51 en 57 van de verordening)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 50 (Vereisten voor digitaledienstencoordinatoren en bevoegde autoriteiten)	Artt. 2.1, derde en vierde lid, en 3.1, tweede en derde lid, van dit wetsvoorstel. Zie § 5.2.2.1 van deze MvT	Geen	
Artikel 51, eerste lid (Onderzoeksbevoegdheden)	Implementatie door middel van bestaande regeling (artt. 5:15, 5:16, 5:16a, 5:17 en 5:18 Awb; art. 12c Instellingswet ACM) Art. 3.2, derde en vierde lid, van dit wetsvoorstel Zie § 5.3.2 van deze MvT	Geen	
Artikel 51, tweede lid, onderdeel a (Handhavingsbevoegdheid om toezeggingen verbindend te maken)	Implementatie door middel van bestaande regeling (Art. 12h Instellingswet ACM) Art. 3.5 van dit wetsvoorstel Zie § 5.3.3 van deze MvT	Geen	
Artikel 51, tweede lid, onderdeel b (Handhavingsbevoegdheid om stopzetting van inbreuken te bevelen)	Implementatie door middel van bestaande regeling (art. 12j Instellingswet ACM) Art. 3.6, eerste lid, van dit wetsvoorstel Zie § 5.3.3 van deze MvT	Geen	
Artikel 51, tweede lid, onderdeel c (Handhavingsbevoegdheid om geldboeten op te leggen)	Artt. 2.3 en 3.3 van dit wetsvoorstel; zie § 5.3.6 van deze MvT	Geen	
Artikel 51, tweede lid, onderdeel d en (Handhavingsbevoegdheid om dwangsommen op te leggen)	Artt. 2.4 en 3.4 van dit wetsvoorstel; zie § 5.3.6 van deze MvT	Geen	
Artikel 51, tweede lid, onderdeel e (Handhavingsbevoegdheid om voorlopige maatregelen te nemen)	Artt. 2.5, eerste lid, onderdeel a, en 3.6, tweede lid, onderdeel a, van dit wetsvoorstel; zie § 5.3.4 van deze MvT	Geen	
Artikel 51, derde lid, eerste alinea, onderdeel a (Bevoegdheid om aan het leidinggevende orgaan eisen op te leggen bij ernstige inbreuken)	Artt. 2.5, eerste lid, onderdeel b, en 3.6, tweede lid, onderdeel b, van dit wetsvoorstel; zie § 5.3.5 van deze MvT	Geen	

Artikel 51, derde lid, eerste alinea, onderdeel b (Bevoegdheid om te verzoeken toegang online-interface tijdelijk te beperken)	Artt. 2.5, eerste lid, onderdeel c, derde en vierde lid en 2.6 van dit wetsvoorstel, zie § 5.3.5.2 van deze MvT		
Artikel 51, vierde lid (Onverminderde geldigheid bevoegdheden)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 51, vijfde lid (Doeltreffende, ontradende en evenredige maatregelen)	Implementatie door middel van bestaande regeling (hoofdstukken 2, 3, 4 en 5 Awb)	Geen	
Artikel 51, zesde lid (Vastlegging specifieke regels en procedures door lidstaten)	Implementatie door middel van bestaande regeling (hoofdstukken 5 en 6 Awb)	Geen	
Artikel 52, eerste en tweede lid (Lidstaten voorzien in voorschriften inzake sancties; sancties moeten doeltreffend, evenredig en afschrikkend zijn)	Artt. 2.3, 2.4, 3.3 en 3.4 van dit wetsvoorstel	Dit lid geeft de ruimte aan lidstaten om keuzes te maken bij vormgeving sancties.	Zie § 5.3.6.2 van deze MvT
Artikel 52, derde lid (Maximumbedrag geldboeten)	Artt. 2.3, eerste lid, en 3.3, eerste lid van dit wetsvoorstel	Geen	
Artikel 52, vierde lid (Maximumbedrag dwangsommen)	Artt. 2.4, eerste lid, en 3.4, eerste lid van dit wetsvoorstel	Geen	
Artikel 53 (Klachtrecht)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 54 (Schadevergoeding)	Implementatie door middel van bestaande regeling (art. 6:74, 6:96 en 6:162 BW)	Geen	
Artikel 55, eerste en tweede lid (Activiteitenverslagen digitaledienstencoördinator)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 55, derde lid (Relevante informatie andere bevoegde autoriteit voor activiteitenverslag)	Art. 4.1, tweede lid, van dit wetsvoorstel	Geen	
Artikel 56 (Bevoegdheidsverdeling)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 57 (Wederzijdse bijstand)	Artt. 2.7 en 2.8 van dit wetsvoorstel, zie § 5.3.5.29 van deze MvT	Geen	
Artikel 58 (Grensoverschrijdende samenwerking tussen digitaledienstencoördinatoren)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 59 (Verwijzing naar de Commissie)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 60 (Gezamenlijke onderzoeken)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 61 (Digitaledienstenraad)	Behoeft naar zijn aard geen implementatie	Geen	

Artikel 62, eerste lid (Samenstelling digitaledienstenraad)	Art. 3.1, vierde lid, van dit wetsvoorstel,	Het nationale recht kan erin voorzien dat naast de digitaledienstencoördinator ook andere bevoegde autoriteiten kunnen deelnemen aan de raad.	Zie § 5.4.5.2 van deze MvT
Artikel 62, tweede tot en met zevende lid (Structuur digitaledienstenraad)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 63 (Taken digitaledienstenraad)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 64 (Ontwikkelen van deskundigheid en capaciteiten)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 65 (Handhaving van verplichtingen van aanbieders van zeer grote online platforms en zeer grote online zoekmachines)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 66, eerste en tweede lid (Inleiding van procedures door de Commissie)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 66, derde lid (Uitoefening onderzoeksbevoegdheden op verzoek van de Commissie)	Artt. 2.7 en 3.7 van dit wetsvoorstel, zie § 5.3.5.29 van deze MvT	Geen	
Artikel 66, vierde lid (Verstrekking relevante informatie)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 67 (Verzoeken om inlichtingen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 68 (Bevoegdheid van de Commissie om te horen en verklaringen af te nemen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 69, eerste tot en met zesde lid (Bevoegdheid van de Commissie om inspecties uit te voeren)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 69, zevende tot en met tiende lid (bijstand van nationale bevoegde autoriteiten)	Art. 2.8 van dit wetsvoorstel, zie § 5.3.5.29 van deze MvT	Geen	
Artikel 70 (Voorlopige maatregelen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 71 (Toezeggingen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 72 (Toezichtsmaatregelen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 73 (Niet-naleving)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 74 (Geldboeten)	Behoeft naar zijn aard geen implementatie	Geen	

Artikel 75 (Verscherpt toezicht)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 76 (Dwangsommen)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 77 (Verjaringstermijn voor opleggen sancties)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 78 (Verjaringsperiode voor uitvoering van sancties)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 79 (Recht om te worden gehoord en toegang tot het dossier)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 80 (Bekendmaking besluiten)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 81 (Beroep bij het Hof van Justitie van de Europese Unie)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 82, eerste lid (Verzoeken om toegangsbeperking)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 82, tweede lid (Indienen schriftelijke opmerkingen bij gerechtelijke autoriteit en verzoek toezenden relevante documenten)	Art. 2.6, derde en vierde lid, van dit wetsvoorstel, zie § 5.3.5.25 van deze MvT	Geen	
Artikel 82, derde lid (Geen beslissing in strijd met besluit van de Commissie)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 83 (Uitvoeringshandelingen met betrekking tot tussenkomst van de Commissie)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 84 (Beroepsgeheim)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 85 (Informatie-uitwisselingssysteem)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 86 (Vertegenwoordiging)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 87 (Comitéprocedure)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 89 (Wijzigingen richtlijn inzake elektronische handel)	Wijzigingen van verwijzingen in de Aanpassingswet richtlijn inzake elektronische handel, de Auteurswet en de Wet handhaving consumentenbescherming (Artt. 5.1, 5.3 en 5.5 van dit wetsvoorstel)	Geen	
Artikel 90 (Wijziging Richtlijn (EU) 2020/1828)	Behoeft naar zijn aard geen implementatie	Geen	

Artikel 91 (Herziening)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 92 (Vervroegde toepassing op aanbieders van zeer grote online platforms en zeer grote online zoekmachines)	Behoeft naar zijn aard geen implementatie	Geen	
Artikel 93 (Inwerkingtreding en toepassing)	Behoeft naar zijn aard geen implementatie	Geen	