

FACT-CHECKING DESINFORMATIE: MODERATIE OF ONSCHULDIGE CONTEXT?

Alexander de Wit & Michael Klos*

Desinformatie is geen illegale inhoud en hoeft dus niet altijd verwijderd te worden. Maar wat is het dan wel? In deze bijdrage wordt ingegaan op de aanpak van desinformatie onder de digitale dienstenverordening (DSA). De auteurs laten zien dat desinformatie weliswaar geen illegale inhoud is, maar dat de mogelijke gevolgen van regulering van desinformatie (bijvoorbeeld door middel van zichtbaarheidsreducties) voor gebruikers gelijk kunnen zijn. Dit betekent dat ook voor lichtere remedies als factchecken in bescherming moet worden voorzien.

Introductie

Wat is echt en wat is echt nep? Desinformatie kan de lezer in flinke verwarring achterlaten. Wordt ook betrouwbare informatie als onbetrouwbaar afgedaan? Deze twijfel kan ook gevolgen hebben voor het democratisch proces.¹ Het kabinet-Schoof I heeft desinformatie op het oog als beleidsthema.² Het kabinet brengt desinformatie in het regeerprogramma in verband met openbare ordeverstoringen, hybride dreigingen en conflicten in het buitenland.³ Als mogelijke remedies worden informatievoorziening door de publieke omroep en het vergroten van de weerbaarheid van het publiek genoemd.⁴ Desinformatie heeft dus duidelijk de aandacht van politici – al zijn de interventies nog weinig specifiek.

Wat is echt en wat is echt nep? Desinformatie kan de lezer in flinke verwarring achterlaten. Wordt ook betrouwbare informatie als onbetrouwbaar afgedaan?

Online wordt de hoop gevestigd op de digitale dienstenverordening, beter bekend als de Digital Services Act (hierna DSA).⁵

De Europese Commissie communiceerde de aanpak van de DSA in één adem met de aanpak van illegale inhoud.⁶ Dit roept het beeld op dat desinformatie net als illegale inhoud verwijderd dient te worden. Illegale inhoud is echter omschreven in de DSA als inhoud in strijd met het recht.⁷ Veel vormen van desinformatie vallen daarbuiten omdat het niet in 'harde' wetgeving wordt geadresseerd. De Europese Commissie benadert desinformatie vaak genuanceerder.⁸ Deze nuance is passend omdat desinformatie niet letterlijk voorkomt in de artikelen van de DSA.⁹

In plaats daarvan wordt desinformatie (hoofdzakelijk)¹⁰ geadresseerd via zorgvuldigheidsverplichtingen die enkel van toepassing zijn op zeer grote onlineplatforms (in het Engels *very large online platforms* (VLOPs)).¹¹ Deze zien alleen op diensten met gemiddeld meer dan 45 miljoen maandelijkse gebruikers binnen de Europese Unie die zijn aangewezen door de Europese Commissie.¹² Voorbeelden hiervan zijn Instagram, X en Facebook.¹³ VLOPs zijn verplicht risicoanalyses uit te voeren die bijvoorbeeld zien op 'eventuele werkelijke of voorzienbare negatieve effecten op de burgerdialoog en verkiezingsprocessen, en de openbare veiligheid'¹⁴ die verband houden met de functionaliteiten die onlineplatforms aanbieden, zoals aanbevelingssystemen.¹⁵ Deze analyse kan leiden tot verschillende maatregelen, waaronder

* Mr.drs. A. de Wit is onderzoeker bij de afdeling Encyclopedie van de Rechtswetenschap aan de Universiteit Leiden. De Wit doet onderzoek binnen het Digital Jurisprudence-project naar desinformatie en democratische legitimiteit. Mr.dr. M. Klos is universitair docent bij de afdeling Encyclopedie van de Rechtswetenschap aan de Universiteit Leiden. Klos doet onderzoek naar de vrijheid van meningsuiting op internet en houdt zich bezig met thema's als haatzaaien, nepnieuws, desinformatie en de verspreiding van online terrorismepropaganda.

1 S. van der Linden, U. Ecker & S. Lewandowsky, 'Misinformation is a threat to society – let's not pretend otherwise', *LSE Impact Blog*, 8 oktober 2024; Communication COM(2018)236 final of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 26 April 2018 on Tackling Online Disinformation: A European Approach, p. 185.

2 Rijksoverheid, *Regeerprogramma kabinet-Schoof*, Rijksoverheid september 2024, p. 86, 93, 95 en 107.

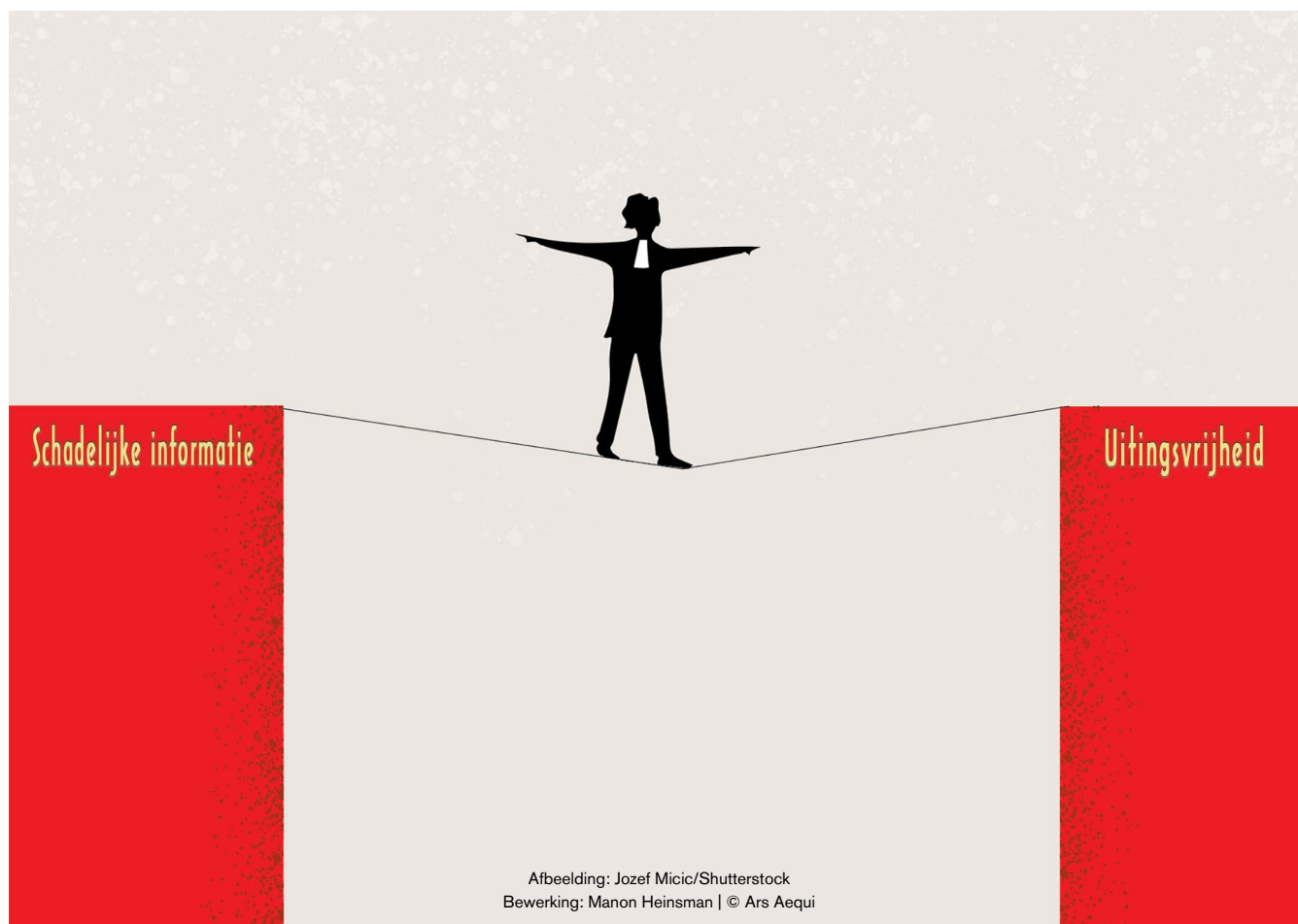
3 *Regeerprogramma kabinet-Schoof* 2024, p. 95 en 107.

4 *Regeerprogramma kabinet-Schoof* 2024, p. 86 en 93.

5 Voor zover het juridisch kader is deze bijdrage gebaseerd op I. Siegel & M. Klos, 'Straffe desinformatiewetgeving? Bedenkingen vanuit Franse en Europese Unie-wetgeving', *AA* (73) 2024, afl. 7/8 (AA20240682); M. Klos, 'Wat offline niet mag, mag ook online (soms) niet', *NTM/NJCM-bull.* (49) 2024, afl. 3. Deze bijdragen bespreken het juridisch kader en de Code of Practices 2018 en 2022 uitgebreider. Deze bijdrage richt zich specifiek op factchecken als maatregel tegen desinformatie binnen de DSA.

6 Europese Commissie, 'The Digital Services Act', *commission.europa.eu*, 27 oktober 2022.

7 De DSA geeft de volgende definitie: "illegale inhoud": 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 tegen het met het Unierecht in overeenstemming zijnde recht van een lidstaat, ongeacht het precieze voorwerp of de precieze aard van dat recht", art. 3(h) Verordening (EU) 2022/2065 van het Europees Parlement en



Afbeelding: Jozef Micic/Shutterstock
Bewerking: Manon Heinsman | © Ars Aequi

de Raad van 19 oktober 2022 over betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitale-dienstenverordening).

8 Europese Commissie, 'Digital Services Act: Questions and Answers', beschikbaar op <https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers> (geraadpleegd op 8 oktober 2024).

9 Zie voor een uitgebreidere bespreking over het aansprakelijkheidssysteem onder de DSA, Klos 2024, p. 215-233.

10 De aanpak van desinformatie kan ook aan de orde komen bij zogenaamde crisisresponsmechanismen en transparantieplichtingen rondom advertenties, zie art. 36 en 39 Verordening (EU) 2022/2065.

11 Hoofdstuk 3, Afdeling 5 Verordening (EU) 2022/2065.

12 Art. 33 lid 1 en 4 Verordening (EU) 2022/2065.

13 Europese Commissie, 'Supervision of the designated very large online platforms and search engines under DSA', beschikbaar op <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (geraadpleegd op 7 oktober 2024).

14 Art. 34 lid 1 onder c Verordening (EU) 2022/2065.

15 Art. 34 lid 2 Verordening (EU) 2022/2065.

16 Art. 35 lid 1 Verordening (EU) 2022/2065.

17 Art. 35 lid 1 onder h Verordening (EU) 2022/2065.

18 Art. 45 Verordening (EU) 2022/2065; European Board for Digital Services, 'Minutes – Fifth Meeting', beschikbaar op <https://digital-strategy.ec.europa.eu/en/policies/dsa-board> (geraad-

aanpassing van functionaliteiten, algemene voorwaarden en procedures.¹⁶ Daarnaast wordt specifiek opgemerkt dat 'aanvatting of aanpassing van de samenwerking met andere aanbieders van onlineplatforms of van onlinezoekmachines aan de hand van de gedragscodes' een mogelijkheid is om deze systeemrisico's te beperken.¹⁷

Deze gedragscodes spelen een grote rol. In dit verband zijn de Code of Practice on Disinformation uit 2018 (hierna Praktijkcode 2018) en de Strengthened Code of Practice on Disinformation (hierna Praktijkcode 2022) van belang. Deze laatste wordt mogelijk een gedragscode zoals bedoeld in de DSA.¹⁸ De DSA gaat uit van een co-regulerings-systeem waarin vrijwillige gedragscodes worden gecombineerd met publiekrechtelijk toezicht. Onder omstandigheden kunnen toezeggingen onder de Praktijkcode 2022 ook onderdeel worden van de verplichtingen onder de DSA.¹⁹

Deze bijdrage bespreekt de wijze waarop desinformatie wordt gereguleerd. Het gaat hierbij niet noodzakelijk om verwijdering, maar om alternatieve remedies voor het schadelijke karakter.²⁰ We zoomen daarbij in op één van deze remedies: het beoordelen van inhoud door (externe) factcheckers. Deze remedie is niet onschuldig: ook als inhoud niet wordt verwijderd kan het reguleren van desinformatie consequenties hebben voor de mogelijk-

heid van gebruikers om zich te uiten.²¹ We besteden daarom ook aandacht aan de mogelijke remedies die zowel onlineplatforms als gebruikers voorhanden hebben.

Deze bijdrage bespreekt de wijze waarop desinformatie wordt gereguleerd. Het gaat hierbij niet noodzakelijk om verwijdering, maar om alternatieve remedies voor het schadelijke karakter

Desinformatie door de lens van de DSA

In de artikelen van de DSA wordt desinformatie niet expliciet geadresseerd. Dit is anders voor de overwegingen.²² In de overwegingen komt in ieder geval naar voren dat desinformatie wordt gezien als een maatschappelijk risico,²³ dat vergroot wordt door manipulatieve technieken,²⁴ als een subtype van misleidende of bedrieglijke inhoud²⁵ en een systeemrisico (bij VLOPs).²⁶

De DSA biedt geen definitie van desinformatie. Dit is anders voor illegale inhoud waaronder desinformatie niet noodzakelijk valt.²⁷ De relevantie van dit onderscheid komt

naar boven als de verplichtingen van online-platforms voor illegale inhoud besproken wordt. In de Praktijkcode 2018 hanteerde de Europese Commissie voor desinformatie 'verifieerbare valse of misleidende informatie' die 1) (cumulatief) 'gecreëerd, gepresenteerd en verspreid is voor economische winst of om het publiek opzettelijk te misleiden' én 2) 'publieke schade kan veroorzaken zoals schade aan het democratische of beleidsproces of publieke goederen of de bescherming van de gezondheid, omgeving of veiligheid van EU-burgers'.²⁸ In 2018 bestond dus een onderscheid tussen desinformatie en niet-opzettelijke verspreiding van misinformatie. Dit is in de Praktijkcode 2022 losgelaten.²⁹ In de praktijk is het namelijk moeilijk te achterhalen of desinformatie opzettelijk is gedeeld terwijl de impact van het delen van onjuiste informatie gelijk kan zijn.

De praktijkcodes uit 2018 of 2022 maken desinformatie niet illegaal.³⁰ Twee misverstanden die kunnen ontstaan is dat onlineplatforms verplicht zouden zijn om desinformatie actief op te sporen en proactief te verwijderen. Door te bespreken hoe onlineplatforms om dienen te gaan met illegale inhoud wordt ook duidelijk dat deze lezing geen steun vindt in de DSA.

Binnen de EU is een conditionele uitzondering voor aansprakelijkheid in het leven geroepen voor onlineplatforms.³¹ Hostingdiensten (waaronder ook onlineplatforms) zijn niet automatisch aansprakelijk voor alle inhoud geplaatst door gebruikers. Allereerst kunnen onlineplatforms niet verplicht worden 'actief onderzoek naar de feiten of omstandigheden die duiden op illegale activiteiten' te doen.³² Daarnaast zijn zij niet aansprakelijk voor inhoud geplaatst door derden zolang zij geen kennis hebben van de inhoud. Het gaat hierbij niet om algemene kennis dat er mogelijk ergens illegale inhoud wordt gedeeld op het platform. De DSA vult dit kennis criterium bijvoorbeeld in met een voldoende onderbouwde melding van een gebruiker waarbij precies wordt aangewezen welke inhoud een illegaal karakter heeft.³³ Zelfs als aanbieders van onlineplatforms wel op de hoogte raken van de inhoud kan worden ontsnapt aan aansprakelijkheid door snel de inhoud ontoegankelijk te maken.³⁴

Wanneer 'weten' aanbieders dat er illegale inhoud is op het onlineplatform? Weten dat er ergens mogelijk illegale inhoud wordt gedeeld is in ieder geval niet voldoende. Dit zou in tegenspraak zijn met artikel 8, waarin een verbod op een algemene monitoringsverplichting is opgenomen. Kort gezegd kunnen onlineplatforms niet verplicht worden alle inhoud te controleren. Artikel 8 brengt ook met zich mee dat rechters niet tot een algemene toezichtsverplichting kunnen bevelen zoals in *Bodegraven-Reeuwijk/Twitter* bleek.³⁵ Dit zou immers betekenen dat onlineplatforms alsnog alle inhoud moeten controleren op illegale inhoud. Rechters kunnen wel bevelen specifieke inhoud te filteren. Dit kan alleen als

de inhoud van een dergelijke gelijke inhoud/strekking is dat het met geautomatiseerde middelen op te sporen en te beoordelen is.³⁶

Desinformatie kan gelet op het systeem van de DSA niet strenger worden aangepakt dan illegale inhoud. Wel kan de aanpak van desinformatie onderdeel worden van de invulling van de verplichting om systeemrisico's aan te pakken. Dit gaat enkel op voor VLOPs. Veel beeldbepalende platforms zijn echter (inmiddels) aangewezen als VLOP. Het gaat hierbij onder anderen om Facebook, Instagram, TikTok, YouTube en X.³⁷ Deze onlineplatforms zijn, op X na, ook partij bij de Praktijkcode 2022.³⁸

Desinformatie wordt niet noodzakelijk als illegale inhoud gereguleerd, maar de bestrijding ervan maakt deel uit van het mitigeren van de systeemrisico's. Een voor de hand liggende manier voor VLOPs om aan die verplichting te voldoen bestaat uit het naleven van de Praktijkcode 2022

Wie checkt de factchecker?

Desinformatie wordt niet noodzakelijk als illegale inhoud gereguleerd,³⁹ maar de bestrijding ervan maakt deel uit van het mitigeren van de systeemrisico's. Een voor de hand liggende manier voor VLOPs om aan die verplichting te voldoen bestaat uit het naleven van de eerdergenoemde Praktijkcode 2022.⁴⁰ Daarin verbinden ondertekenaars zich factchecks van de 'factcheck-gemeenschap' consistent te integreren in hun moderatiebeleid.⁴¹ In deze bijdrage focussen we hierbij op Meta, dat de code heeft ondertekend voor onder meer Facebook en Instagram.⁴²

De inhoudelijke oordelen van factcheckers over het waarheidsgehalte van feitelijke claims worden veelvuldig door VLOPs gebruikt.⁴³ Een belangrijk component van het huidige factcheckbeleid is dat de zichtbaarheid van als onwaar of misleidend bestempelde inhoud significant wordt gereduceerd.⁴⁴ Daarmee worden feitelijke uitspraken op grote onlineplatforms aan een waarheidscheck door factcheckers onderworpen. De belangrijkste reden daarvoor bestaat in het zuiver houden van de informatievoorziening voor een zinvol publiek debat.⁴⁵ Bijdragen die als misleidend of onwaar worden beoordeeld, kunnen zodoende minder aanbevolen worden aan gebruikers (bijv. in de tijdlijn).

Wat betreft de feitenvaststelling in de publieke sfeer gelden factcheckers dus als experts die de feitelijke inhoud van bijdragen in

pleegd op 14 augustus 2024); European Board for Digital Services, 'Seventh meeting of the European Board for Digital Services', 27 september 2024, beschikbaar op <https://digital-strategy.ec.europa.eu/en/news/seventh-meeting-european-board-digital-services>.

19 M. Husovec, *Principles of the Digital Services Act*, Oxford: Oxford University Press 2024, p. 447-450; Siegel & Klos 2024, p. 684-685.

20 Wij sluiten ons aan bij terminologie als remedies in plaats van sancties, zie E. Goldman, 'Content Moderation Remedies', *Michigan Technology Law Review* (28) 2021, afl. 1.

21 Al lijken de DSA en de Europese Commissie voorzichtigheid te betrachten als het gaat om het reguleren van niet-illegale inhoud, zie Husovec 2024, p. 276-279.

22 Overweging 2, 9, 69, 83, 84, 88, 95, 104, 106 en 108 Verordening (EU) 2022/2065. Zie ook Siegel & Klos 2024, p. 686.

23 Overweging 2 en 9 Verordening (EU) 2022/2065.

24 Overweging 69, 83 en 95 Verordening (EU) 2022/2065.

25 Overweging 84 Verordening (EU) 2022/2065.

26 Overweging 108 Verordening (EU) 2022/2065.

27 Art. 3 sub h en overweging 12 Verordening (EU) 2022/2065.

28 Vertaling door MK, zie Europese Commissie, 'Code of Practice on Disinformation', 2018, beschikbaar op <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation> (geraadpleegd op 20 december 2024).

29 Europese Commissie, '2022 Strengthened Code of Practice on Disinformation', 16 juni 2022, beschikbaar op <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>, p. 1. Ook worden desinformatie-operaties door buitenlandse mogendheden hieronder verstaan, zie Siegel & Klos 2024, p. 685. Dit valt echter buiten de scope van deze bijdrage omdat factchecken hier doorgaans een te licht middel voor zal zijn.

30 Al kan wat op EU niveau als desinformatie wordt gereguleerd ook illegale inhoud zijn op het niveau van een lidstaat, zie R. Ó Fathaigh, N. Helberger & N. Appelmann, 'The perils of legally defining disinformation', *Internet Policy Review* (10) 2021, afl. 4, p. 19-20.

31 Zie art. 14 en 15 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 over betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (Richtlijn inzake elektronische handel). De kern hiervan is teruggekomen in art. 6 en 8 Verordening (EU) 2022/2065. Zie voor een bespreking van de (uitzonderingen van) aansprakelijkheid van hostingdiensten onder de Richtlijn inzake elektronische handel, F. Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US*, Cheltenham: Edward Elgar Publishing 2020, p. 36-47.

32 Art. 8 Verordening (EU) 2022/2065.

33 Art. 16 Verordening (EU) 2022/2065.

34 Art. 6 lid 1 onder a en b Verordening (EU) 2022/2065. Dit geldt volgens art. 6 lid 2 echter niet voor inhoud aangeboden door iemand die 'op gezag of onder toezicht van de dienst aanbieder handelt'.

35 Rb. Den Haag (vzr.) 4 oktober 2022, ECLI:NL:RBDHA:2022:10082, 4.7-4.13 (*Bodegraven-Reeuwijk/Twitter*). Deze voorzieningen rechter pas te hierbij de standaard uit *Glawischnig-Piesczek* toe, zie HvJ EU 3 oktober 2019, C-18/18, ECLI:EU:C:2019:821, *RvdW* 2020/395, par. 53 (*Glawischnig-Piesczek*).

36 HvJ EU 3 oktober 2019, C-18/18, ECLI:EU:C:

2019:821, RvdW 2020/395, par. 53 (*Glawisch-nig-Piesczek*). Weliswaar ging het hier om jurisprudentie onder art. 15 Richtlijn 2000/31/EG, in de DSA is echter opgenomen dat de verwijzingen naar verwijderde artikelen uit de richtlijn verwijzen naar de relevante artikelen van de DSA, zie art. 89 Verordening (EU) 2022/2065.

37 Europese Commissie, 'Supervision of the designated very large online platforms and search engines under DSA', beschikbaar op <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (geraadpleegd op 7 oktober 2024).

38 Zo is X geen partij (meer) bij de Praktijkcode, zie Europese Commissie, 'Signatories of the 2022 Strengthened Code of Practice on Disinformation', 16 juni 2022, beschikbaar op <https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation>.

39 Een argument tegen het criminaliseren van desinformatie wordt uitgewerkt in Siegel & Klos 2024.

40 Husovec 2024, p. 447-450. Dit maakt de aanpak van desinformatie door zeer grote onlineplatforms exceptioneel in de zin dat verschillende platforms verschillend worden gereguleerd, zie Klos 2024, p. 226-227.

41 Paragraaf VII onder b, Europese Commissie, '2022 Strengthened Code of Practice on Disinformation', 16 juni 2022, beschikbaar op <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>.

42 Meta, *EU Code of Practice on Disinformation 2022. Subscription Document for Meta*, 14 juni 2022, beschikbaar via <https://ec.europa.eu/newsroom/dae/redirection/document/104042>.

43 In de EU heeft Meta in de periode tussen 1 januari en 30 juni 2024 gebruikgemaakt van 150.000 verschillende factchecks van 29 factcheckorganisaties. 990.000 bijdragen zijn daarmee voorzien van een label en/of de zichtbaarheid daarvan is gereduceerd, zie Meta, *Code of Practice on Disinformation – Report of Meta for the period 01 January 2024 to 30 June 2024*, Code of Practice on Disinformation Transparency Centre september 2024, beschikbaar op <https://disinfocode.eu/signatory-report/meta-september-2024/>, p. 3.

44 Meta stelt: 'We verminderen de verspreiding van Onjuiste en Bewerkte berichten drastisch en verminderen de distributie van Gedeeltelijk onjuist in mindere mate' zie Meta, 'Hoe feiten checken werkt', *Meta Transparency Center*, beschikbaar op <https://transparency.meta.com/en-us/features/how-fact-checking-works> (geraadpleegd op 15 oktober 2024).

45 Zie bijv. Communication COM(2018)236 final, p. 1.

46 Uit empirisch onderzoek naar de taakopvatting van factcheckers blijkt voorts dat zij zichzelf zien als beïnvloeders van de samenleving, zie N. Micallef e.a., 'True or False: Studying the Work Practices of Professional Fact-Checkers', *Proceedings of the ACM on Human-Computer Interaction* (6) 2022/127, afl. CSCW1, p. 27.

47 A. Moore, *Critical Elitism*, Cambridge: Cambridge University Press 2017, p. 42.

48 C. Holst & J. Christensen, 'The epistemic quality of expert bodies: from normative-theoretical concept to empirical measurement', *Acta Politica* 2023, p. 825.

49 L.T. Zagzebski, *Epistemic Authority. A Theory of Trust, Authority and Autonomy in Belief*, Oxford: Oxford University Press 2012, p. 99.

50 Zagzebski 2012, p. 107.

51 Zagzebski 2012, p. 107.

het publiek debat borgen.⁴⁶ In bredere zin kan de belofte van de inzet van expertise in een democratie zo worden geformuleerd dat onze collectieve beslissingen van hogere kwaliteit zijn als we die goed geïnformeerd nemen.⁴⁷ Omdat expertise een zware stem heeft in het publieke debat is het van belang de legitimiteit van expertise te beschouwen.⁴⁸ Elke vorm van autoriteit – of dit nu politieke, ouderlijke of epistemische autoriteit is – beperkt immers de individuele autonomie.⁴⁹

Voor de legitimatie van politieke autoriteit bestaat al een sterke democratische en rechtsstatelijke infrastructuur. Bij de epistemische autoriteit van factcheckers is die legitimatie vooralsnog minder stevig.

Epistemische autoriteit ziet op de vaststelling van kennis, zodanig dat het eigen oordeel wordt opgeschort en men zich voegt naar het oordeel van de expert.⁵⁰ Het advies van de expert wordt opgevolgd omdat het de expert is. Het eigen oordeel wordt zodoende opgeschort en degene die het advies krijgt schikt zich naar het oordeel van de expert. Het kunnen geven van opschortende redenen geldt in de literatuur als het belangrijkste kenmerk van legitieme (epistemische) autoriteit.⁵¹ Nu de individuele autonomie hierdoor vergaand kan worden beknot is de vraag onder welke voorwaarden epistemische autoriteit gelegitimeerd kan worden cruciaal. Politiek filosoof Alfred Moore heeft in zijn boek *Critical Elitism* voorgesteld de legitimiteit van epistemische autoriteit te verenigen met democratische controle.⁵² Dat klinkt op het eerste oog wat paradoxaal, nu deze controle indruist tegen de idee van een opschortende reden. Deze opschorting is in beginsel in tijd beperkt (het ontvangen van advies) terwijl een autoriteitsrelatie over een lange tijd bestaat (het toedichten van legitimiteit aan expertise). Toegespitst op factcheckers betekent dit dat de autoriteit van een factchecker niet voor elke factcheck opnieuw beoordeeld hoeft te worden, maar de onderliggende autoriteitsrelatie moet wel vatbaar zijn voor controle. Legitieme autoriteit moet kunnen rekenen op de voortdurende acceptatie van degenen die eraan onderworpen zijn.⁵³ Die voortdurende acceptatie is alleen legitiem wanneer er een context van kritiek bestaat waarin het gezag kan worden gecontroleerd en op gezette momenten ook kan worden bevraagd.⁵⁴ In algemene zin kan een context van kritiek gecreëerd worden door *credentials* te checken, debat tussen experts waar te nemen, belangen van de autoriteit transparant weer te geven, *track records* op te vragen en lekenkennis mee te nemen.⁵⁵ Uiteraard is het afhankelijk van de aard van de autoriteitsrelatie hoe die context in concreto gevormd wordt.

Denk bijvoorbeeld aan een patiënt die een geneeskundige behandelingsovereenkomst sluit met een arts.⁵⁶ De patiënt accepteert daarmee op een bepaald moment de autoriteit van de arts. Het gevolg daarvan is dat de arts bijvoorbeeld medicijnen kan voorschrijven. In lijn met de opschortingsthese hoeft

een arts daarbij niet steeds zijn redenen tot in detail uit te leggen. Tegelijkertijd behelst de acceptatie op het moment van het sluiten van de overeenkomst niet een totale onderwerping van de patiënt aan de arts op medisch gebied. De noodzakelijke context van kritiek wordt hier gevormd door onder meer het recht van de patiënt om inlichtingen over de behandeling te verkrijgen (art. 7:448 BW), het recht op een *second opinion* van een andere arts (art. 38 Modelregeling arts-patiënt) en het recht om verklaringen aan het medisch dossier toe te voegen (art. 7:454 lid 2 BW). Deze maatregelen stellen de patiënt in staat om ook als leek te beoordelen of de behandeling hem wel dient, en of hij de relatie voort wil zetten.

Hoe moet nu de autoriteitsrelatie tussen factcheckers en gebruikers van VLOPs beoordeeld worden? De belangrijkste manier waarop factcheckers democratisch gecontroleerd zouden kunnen worden is door hun factchecks onderwerp van het publieke debat te maken. Het moet voor gebruikers inzichtelijk zijn welke bijdragen getoetst worden, welke methodologie daarbij gehanteerd wordt,⁵⁷ welke bronnen gebruikt zijn, wie de toets verricht en er moeten mogelijkheden zijn kritiek te leveren. Hoewel het International Fact-Checking Standards Network (IFCN) zich committeert aan transparantieplichtingen, is het voor veel gebruikers van platforms niet duidelijk welke bijdragen nu precies worden getoetst en wat daar de gevolgen van zijn.⁵⁸ Zichtbaarheidsbeperkingen hebben immers juist als doel bijdragen aan het debat te onttrekken, wat controle bemoeilijkt. Bijkomend probleem is dat de epistemische autoriteit van een factchecker niet echt opgezegd kan worden door de gebruiker. En waar de epistemische autoriteit van een arts gelimiteerd is tot specifieke medische handelingen, beoordelen factcheckers een in beginsel thematisch onbegrensde hoeveelheid posts. Dergelijke factoren spreken te meer in het voordeel van een sterkere controle door gebruikers.

In de regulering van desinformatie worden we geconfronteerd met het feit dat we dienen te koorddansen tussen de bescherming van de uitingsrechten enerzijds en de aanpak van de (mogelijke) schadelijke effecten van desinformatie anderzijds

Waarborgen en remedies

In de regulering van desinformatie worden we geconfronteerd met het feit dat we dienen te koorddansen tussen de bescherming van de uitingsrechten enerzijds en de aanpak van de

(mogelijke) schadelijke effecten van desinformatie anderzijds. In de Praktijkcode van 2018 was het onjuiste karakter van desinformatie op zichzelf geen reden om over te gaan tot verwijderen.⁵⁹ Deze stelligheid is uit de Praktijkcode 2022 verdwenen. Wel kan uit de Praktijkcode 2022 worden opgemaakt dat de directe aanpak alleen ziet op valse of misleidende inhoud die ook schadelijk is.⁶⁰

Ook hier kan worden gewezen op de omgang met illegale inhoud. Gebruikers die van mening zijn dat de inhoud die ze aantreffen illegaal is, kunnen dit melden aan het onlineplatform. Hiervoor moet het onlineplatform digitale en toegankelijke mechanismen in het leven roepen. In beginsel geldt dit alleen voor illegale inhoud.⁶¹ Ondertekenaars van de Praktijkcode 2022 dienen dit ook voor desinformatie te doen.⁶² Als gebruikers het oneens zijn met beslissingen kunnen ze gebruik maken van interne klachtenmechanismen (bezwaarprocedure bij het onlineplatform zelf).⁶³ Het gaat hierbij zowel om de melder als de gebruiker wiens inhoud is onderworpen aan een contentmoderatiebeslissing. Als onlineplatforms de mogelijkheid bieden om te klagen over niet-illegale inhoud, dan staat dit mechanisme ook open voor klachten over niet (of onvoldoende) ingrijpen na een dergelijke klacht.⁶⁴ Bij de aanpak van desinformatie onder de Praktijkcode 2022 zal dit doorgaans het geval zijn.⁶⁵ Ook staat na een dergelijke interne geschillenprocedure de mogelijkheid open om naar een gecertificeerde buitengerechtelijke geschillenbeslechtsinstantie of de rechter te stappen. Deze mogelijkheid staat eveneens expliciet open voor melders.⁶⁶

Onlineplatforms dienen, als ze desinformatie opnemen in de algemene voorwaarden, rekening te houden met de uitspraken van gebruikers. Dit ziet zowel op het opstellen als toepassen van de algemene voorwaarden als op concrete moderatiegevallen.⁶⁷

Conclusie

De aanpak van desinformatie zal een veel complexere (her)beoordeling vergen dan een verwijderbeslissing bij illegale inhoud. In het geval van illegale inhoud is de enige optie verwijdering. In het geval van desinformatie is verwijdering slechts één van de opties (en de meest vergaande). Maatregelen zoals factchecken kunnen alleen aan de orde zijn als inhoud niet voor verwijdering in aanmer-

king komt. De discussie kan zich daarbij gaan concentreren op de zwaarte van de sanctie (of beter gezegd: remedie), maar zeker ook de waardering van de feiten door bijvoorbeeld een factchecker. Online desinformatie wordt voornamelijk aangepakt door de verspreiding te beperken. Dit valt deels te verklaren door het feit dat voornamelijk de grootschalige verspreiding van desinformatie problematisch is. Anders dan illegale inhoud is het niet zo dat desinformatie per definitie verwijderd moet worden. Dit maakt dat desinformatie op verschillende – andere – manieren wordt geadresseerd.

De aanpak van desinformatie zal een veel complexere (her)beoordeling vergen dan een verwijderbeslissing bij illegale inhoud. In het geval van illegale inhoud is de enige optie verwijdering. In het geval van desinformatie is verwijdering slechts één van de opties (en de meest vergaande)

Eén voorbeeld van de aanpak van desinformatie is factchecken. Desinformatie wordt daarbij niet alleen voorzien van een waarschuwing, context of disclaimer. Factchecken kan ook gevolgen hebben voor de verspreiding door middel van aanbevelingssysteem. Daarmee wordt factchecken in de sfeer van inhoudsmoderatie getrokken. Factchecken is dus niet slechts een extra informatievoorziening.

Hierbij kan worden gewezen op het versterken van de context van kritiek door kritiek op factchecken mogelijk te maken. Dit brengt onlineplatforms wel in een moeilijke situatie. Zij kunnen overwegen slechts nog met waarschuwingslabels met duidelijke uitleg te werken, en te stoppen met het gebruik van zichtbaarheidsreducties om deze kritiek te faciliteren. Tegelijkertijd kan dit als gevolg hebben dat (schadelijke) desinformatie toch makkelijk toegankelijk blijft voor gebruikers. 'Wie checkt de factchecker?' blijft de komende tijd van belang.

52 Moore 2017, p. 8.

53 Moore 2017, p. 66.

54 Moore 2017, p. 74.

55 Moore 2017, p. 81-89.

56 Art. 7:446 BW.

57 Die methodologie staat momenteel nog in de kinderschoenen, waardoor het selectie- en beoordelingsbeleid vaak neerkomt op een subjectief wenselijkheidsoordeel van factcheckers, zie J.E. Uscinski, 'What Are We Doing When We Research Misinformation', *Political Epistemology* 2023, afl. 2, p. 4.

58 Vier van de vijf principes hebben betrekking op transparantie, maar daarbij gaat het om transparantie van factcheckers over hun gebruikte bronnen, belangen en correctiebeleid. Over de relatie met het platform en de gevolgen van de factchecks wordt niks gezegd, zie International Fact-Checking Network, 'The commitments of the Code of Principles', *Poynter Institute*, beschikbaar op <https://ifcncodeofprinciples.poynter.org/the-commitments> (geraadpleegd op 15 oktober 2024).

59 Europese Commissie, '2018 Code of Practice on Disinformation', beschikbaar op <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation> (geraadpleegd op 20 december 2024).

60 Zie bijv. Commitment 23 van de '2022 Strengthened Code of Practice on Disinformation', p. 25.

61 Art. 16 lid 1 Verordening (EU) 2022/2065.

62 Indien online platforms zich verbinden aan Commitment 23 van de '2022 Strengthened Code of Practice on Disinformation', p. 25.

63 Art. 20 Verordening (EU) 2022/2065.

64 Overweging 58 Verordening (EU) 2022/2065.

65 Commitment 23 van de '2022 Strengthened Code of Practice on Disinformation', p. 25.

66 Art. 21 lid 1 Verordening (EU) 2022/2065.

67 Art. 14 lid 4 Verordening (EU) 2022/2065.