De invloed van online desinformatie en microtargeting op digitale verkiezingscampagnes: mogelijkheden, gevaren en toekomstperspectief.



Naam: Nadien Hassan (s1381903)  
Begeleider: Prof.dr. T.E. McGonagle  
Datum: 01 juli 2021  
Woordenaantal: 14367 (excl. literatuurlijst)

Inhoudsopgave:

[Hoofdstuk 1 – Inleiding 3](#_Toc76086163)

[1.1 Introductie 3](#_Toc76086164)

[1.2 Probleemstelling 4](#_Toc76086165)

[1.3 Methodologie en opzet 5](#_Toc76086166)

[Hoofdstuk 2 – Definities en reikwijdte 7](#_Toc76086167)

[2.1 Online desinformatie 7](#_Toc76086168)

[2.2 Digitale politieke microtargeting 9](#_Toc76086169)

[2.3 Digitale verkiezingscampagnes 10](#_Toc76086170)

[Hoofdstuk 3 – Juridisch kader 13](#_Toc76086171)

[3.1 De vrijheid van meningsuiting en het recht op informatie 13](#_Toc76086172)

[3.2 Verplichtingen voor de staat 14](#_Toc76086173)

[3.3. Het recht op privacy en de bescherming van persoonsgegevens 15](#_Toc76086174)

[3.4 De aansprakelijkheid van online platforms 17](#_Toc76086175)

[Hoofdstuk 4 – De gevolgen van online desinformatie en microtargeting voor digitale verkiezingscampagnes 20](#_Toc76086176)

[4.1 Potentiële gevaren van online desinformatie 20](#_Toc76086177)

[4.2 Potentiële gevaren van microtargeting 21](#_Toc76086178)

[4.3 Enige nuancering vanuit nationaal perspectief 22](#_Toc76086179)

[Hoofdstuk 5 – Maatregelen 24](#_Toc76086180)

[5.1 Regelgevende initiatieven in Europa 24](#_Toc76086181)

[5.2 Zelfregulerende maatregelen 25](#_Toc76086182)

[5.3 Zelfregulering in de praktijk: effectief en proportioneel? 26](#_Toc76086183)

[5.4 Versterking van de Code en toekomstperspectief 28](#_Toc76086184)

[5.5 De Digital Services Act 29](#_Toc76086185)

[5.6 Nederlandse Gedragscode Transparantie Online Politieke Advertenties 31](#_Toc76086186)

[Conclusie 34](#_Toc76086187)

[Literatuur- en jurisprudentielijst 37](#_Toc76086188)

# Hoofdstuk 1 – Inleiding

## **1.1 Introductie**

Enkele decennia geleden werd informatie voornamelijk door professionele media en journalisten de wereld in geholpen. Met hun onderzoekende, analyserende en informerende taak fungeren zij als het ware als ‘publieke waakhond’ ten opzichte van de staat. Dit is een cruciale rol die onmisbaar is in een democratische rechtsstaat als Nederland.[[1]](#footnote-1)

In het huidige digitale tijdperk speelt een groot deel van de persoonlijke levenssfeer van individuen zich online af. Sociale media zijn inmiddels zo indringend aanwezig dat *instagrammen* als werkwoord in het Algemeen Nederlands Woordenboek is opgenomen.[[2]](#footnote-2) Professionele media worden dan ook niet meer als het enige kanaal gezien dat individuen op al dan niet kritische wijze toegang verschaft tot belangrijke informatie.[[3]](#footnote-3) Vandaag de dag kan eenieder, ongeacht functie, status of academische achtergrond, zichzelf toegang verschaffen tot en meedoen aan het publieke debat. Bovendien kunnen diezelfde individuen, bijvoorbeeld door middel van sociale media, inhoud plaatsen op het internet zonder de tussenkomst van professionele media of journalisten en hun doorgaans kritische en selectieve blik op het weergeven van informatie. Deze ontwikkeling draagt bij aan de mogelijkheid voor burgers om hun recht op vrije meningsuiting uit te oefenen.[[4]](#footnote-4) Dit is belangrijk, aangezien het recht op vrije meningsuiting één van de kernwaarden van een democratische rechtsstaat is. Wel is het van belang om in te zien dat deze ontwikkeling ook tot andere, negatieve, gevolgen kan leiden. Het gemakkelijker verspreiden van informatie gaat namelijk hand in hand met het gemakkelijker verspreiden van desinformatie. Hoewel desinformatie een lange geschiedenis kent en dus geen nieuw verschijnsel is, lijkt het begrip desinformatie in het huidige digitale tijdperk steeds meer aandacht te genieten. Op dit moment is het bijvoorbeeld een zeer actueel onderwerp vanwege de grote hoeveelheid misleidende informatie die rondgaat over het corona- en vaccinatiebeleid.[[5]](#footnote-5)   
  
Naast de toenemende aandacht voor (online) desinformatie neemt ook de aandacht voor de inzet van gepersonaliseerde politieke advertenties, ook wel ‘microtargeting’, toe.[[6]](#footnote-6) De steeds verdere digitalisering van de samenleving draagt eraan bij dat het democratische politieke gebeuren verandert. Waar verkiezingscampagnes vroeger werden gevoerd door deur-aan-deurbezoeken, verkiezingsborden, radio- en tv-debatten en het uitzenden van reclame, komen er vandaag de dag ook onlinecampagnes bij kijken. Het online voeren van campagne biedt nieuwe mogelijkheden aan politieke actoren om kiezers, zonder tussenkomst van de media of journalisten, te bereiken en kan bovendien voor meer maatschappelijke betrokkenheid zorgen.[[7]](#footnote-7) Voor sommige groepen, met name jongeren, wordt deelname aan het publieke debat nu immers makkelijker en daarmee ook toegankelijker gemaakt. Toch brengt de relatief snelle groei van onlinecampagnes en de daarmee gepaard gaande inzet van gepersonaliseerde politieke advertenties ook kwetsbaarheden met zich mee.[[8]](#footnote-8) Welke kwetsbaarheden dit zijn, wat deze kwetsbaarheden betekenen voor de integriteit van digitale verkiezingscampagnes in Nederland en welke maatregelen hiertegen kunnen worden getroffen zal in het vervolg van deze scriptie uitvoerig worden besproken.

## **1.2 Probleemstelling**

De problematiek rondom online desinformatie en de inzet van gepersonaliseerde politieke advertenties (hierna: microtargeting) is geen nieuwe problematiek. Tot voor kort heerste echter de gedachte dat online desinformatie en microtargeting de afgelopen jaren niet van grote invloed zijn geweest op de Nederlandse samenleving.[[9]](#footnote-9) Inmiddels blijkt deze problematiek in de Nederlandse politieke context ook veel aandacht te genieten.[[10]](#footnote-10) Zo werd begin februari 2021 nog de ‘Nederlandse Gedragscode Transparantie Online Politieke Advertenties’ gepubliceerd, met het doel desinformatie en manipulatie van de Tweede Kamerverkiezingen in maart 2021 tegen te gaan.[[11]](#footnote-11) Ondanks de toenemende aandacht voor deze problematiek is de invloed ervan op de Nederlandse samenleving nog steeds niet volledig helder.[[12]](#footnote-12) Zo is er geen eenduidige juridische definitie van ‘desinformatie’ en lijkt de focus op manipulatie van verkiezingen vooral op de inmenging van buitenlandse actoren in de nationale verkiezingsprocedure te liggen.[[13]](#footnote-13)

Europa staat dan ook voor de vraag welke passende maatregelen genomen kunnen worden om online desinformatie – en daarbij microtargeting – te bestrijden, zonder dat de vrijheid van meningsuiting en het recht op informatie in het gedrang komen. De Europese Commissie presenteerde in september 2018 de EU Code of Practice on Disinformation, waarin zelfregulering door sociale media ter bestrijding van online desinformatie centraal stond.[[14]](#footnote-14) Hierop volgde in december 2020 de introductie van de Digital Services Act. In de Digital Services Act – dat vooralsnog slechts een voorstel is – staat modernisering van de inmiddels ‘gedateerde’ regels omtrent digitale platforms centraal, zodat deze in het huidige digitale tijdperk passen.[[15]](#footnote-15)

De eerdergenoemde Tweede Kamerverkiezingen van 2021 hebben inmiddels plaatsgevonden. De verkiezingscampagnes hebben zich, mede dankzij alle coronaperikelen, voornamelijk online afgespeeld.[[16]](#footnote-16) Dit maakt de hierboven beschreven problematiek rondom online desinformatie en microtargeting relevanter dan ooit tevoren. Welke gevaren liggen op de loer? Welke juridische mogelijkheden zijn inzetbaar in de strijd tegen online desinformatie en manipulatie? Is er behoefte aan nieuwe specifieke regelgeving of zelfregulerende maatregelen? De volgende onderzoeksvraag tracht hier duidelijkheid over te scheppen:

‘Zijn de huidige regelgevende en zelfregulerende initiatieven – met het oog op de vrijheid van meningsuiting en het recht op informatie – effectief en proportioneel ter bestrijding van de potentiële gevaren van online desinformatie en microtargeting in de context van digitale verkiezingscampagnes, of is aanvullende regelgeving op Europees dan wel nationaal niveau wenselijk vanuit juridisch perspectief?’

Deze onderzoeksvraag is zowel evaluerend als voorspellend van aard. Om de beantwoording van de onderzoeksvraag te realiseren kom ik tot de volgende deelvragen:  
1. Wat is de definitie van online desinformatie, microtargeting en digitale verkiezingscampagnes en welk juridisch kader ligt aan deze begrippen ten grondslag?  
2. Welke potentiële gevaren van online desinformatie en microtargeting liggen op de loer en welke invloed hebben deze op de integriteit van digitale verkiezingscampagnes in Nederland?   
3. In welke opzichten zijn de reeds bestaande maatregelen tegen online desinformatie en microtargeting in de context van digitale verkiezingscampagnes voor verbetering vatbaar?

## **1.3 Methodologie en opzet**

Om de probleemstelling en de deelvragen van dit onderzoek te kunnen beantwoorden, wordt er gebruik gemaakt van kwalitatief literatuur- en jurisprudentieonderzoek. De problematiek rondom online desinformatie en het gebruik van microtargeting is relevant op mondiaal niveau. Om tot een adequate beantwoording van de hoofdvraag te komen wordt er in deze scriptie, naast nationale bronnen, dus ook veelvuldig gebruik gemaakt van internationale bronnen. Het literatuuronderzoek bestaat voornamelijk uit relevante wetgeving, richtlijnen, boeken, (advies)rapporten, tijdschriftartikelen en kamerstukken. Het jurisprudentieonderzoek behelst naast relevante nationale rechtspraak ook Europeesrechtelijke rechtspraak. Om deze documenten te vinden zal er gebruik worden gemaakt van verschillende zoekmachines zoals legalintelligence.com, eur-lex.europa.eu, scholar.google.nl en mediaforum.nl.

Deze scriptie bestaat uit een vijftal hoofdstukken. Hierin wordt allereerst de definitie en de reikwijdte van de begrippen ‘online desinformatie’, ‘microtargeting’ en ‘digitale verkiezingscampagnes’ kritisch geanalyseerd. Bovendien wordt kritisch onderzoek gedaan naar het feit dat de fenomenen online desinformatie en microtargeting, ondanks hun lange geschiedenis, in het huidige digitale tijdperk een groter gevaar zijn gaan vormen voor de integriteit van online verkiezingscampagnes.

Vervolgens wordt het juridisch kader met betrekking tot het tegengaan van online desinformatie en het reguleren van gepersonaliseerde politieke advertenties uiteengezet. Voorts wordt de rol van online platforms geanalyseerd. Het juridisch kader blijft daarna de rode draad in het vervolg van deze scriptie vormen.

Daaropvolgend worden in hoofdstuk 4 de potentiële gevaren van online desinformatie en microtargeting in de context van digitale verkiezingscampagnes geïdentificeerd. Hierbij zal ook de noodzaak voor het tegengaan van deze fenomenen worden besproken. De verwezenlijking van deze gevaren in nationale context wordt in paragraaf 4.3 gerelativeerd.

Voorts wordt in hoofdstuk 5 op de huidige regelgevende en zelfregulerende initiatieven op Europees en nationaal niveau gereflecteerd. Hierbij wordt met name ingegaan op de effectiviteit en proportionaliteit van deze initiatieven in het licht van de vrijheid van meningsuiting, het daarmee samenhangende recht op informatie en het recht op privacy en bescherming van persoonsgegevens. Ook zal een door de Europese Commissie recentelijk gepubliceerd voorstel, namelijk de Digital Services Act, kritisch worden geanalyseerd.

Tot slot wordt in de conclusie, met inachtneming van de hierboven beschreven analyse, een antwoord gevormd op de centrale onderzoeksvraag. Ook worden de nodige aanbevelingen gedaan voor het versterken van de huidige regelgevende initiatieven en eventueel toekomstig onderzoek.

# Hoofdstuk 2 – Definities en reikwijdte

In dit hoofdstuk worden de begrippen ‘online desinformatie’ en ‘microtargeting’ gedefinieerd. Het is voor het vervolg van deze scriptie van wezenlijk belang dat er duidelijkheid bestaat omtrent de omvang van deze begrippen. Er zal daarom een definitie van de begrippen worden gegeven en er zal – ter illustratie – ook bij enkele actuele voorbeelden worden stilgestaan. Verder komen recente technologische ontwikkelingen aan bod, als gevolg waarvan de ‘oude’ fenomenen desinformatie en microtargeting – in de context van digitale verkiezingscampagnes – een (steeds grotere) rol zijn gaan spelen.

## 2.1 Online desinformatie

De totstandkoming van desinformatie en de verspreiding hiervan ter beïnvloeding van het publieke debat is van alle tijden. [[17]](#footnote-17) Nieuwe technologieën die de verspreiding van desinformatie faciliteren hebben de zorgen omtrent dit fenomeen echter doen toenemen. De steeds verdere digitalisering van de samenleving heeft onder andere tot een sterke toename van het (online) nieuwsaanbod en een verandering in de nieuwsdistributie geleid. Waar men voorheen voornamelijk via sites van kranten en omroepen online nieuws raadpleegde, bereiken veel berichten hun publiek tegenwoordig via sociale mediakanalen. [[18]](#footnote-18)

Deze veranderingen kunnen het publieke debat zowel in positieve als in negatieve zin beïnvloeden. In eerste instantie hebben deze ontwikkelingen positieve gevolgen, omdat online nieuws gemakkelijker, sneller en goedkoper toegankelijk is via diverse binnenlandse en buitenlandse media. Bovendien wordt het vinden van meer diepgang op specifieke onderwerpen en het vergelijken van verschillende bronnen voor gebruikers vergemakkelijkt. Ook belangrijk is de interactiemogelijkheid tussen verschillende gebruikers door te reageren op berichten of hierover te communiceren. [[19]](#footnote-19)

Ondanks deze positieve gevolgen zijn er echter ook zorgen over de digitalisering van het nieuws. Het verspreiden van desinformatie kan risico’s voor het functioneren van de democratische rechtsstaat met zich brengen. [[20]](#footnote-20) Zo wordt het steeds moeilijker om de herkomst van informatie en de juistheid hiervan te beoordelen. [[21]](#footnote-21) Dit leidt niet alleen tot een verminderd vertrouwen in de juistheid van het informatieaanbod, maar kan ook tot een onterechte beïnvloeding van de maatschappelijke meningsvorming leiden. [[22]](#footnote-22)

Desinformatie is een breed en complex begrip dat geen eenduidige juridische definitie kent. [[23]](#footnote-23) Hoewel er verschillende definities van desinformatie in omloop zijn, komen deze definities op een aantal punten met elkaar overeen. Zo hebben zij met elkaar gemeen dat het in ieder geval moet gaan om een vorm van informatie die onjuist of misleidend is en schadelijke gevolgen kan hebben. [[24]](#footnote-24)

Voor een adequate beantwoording van de centrale onderzoeksvraag in deze scriptie is het van belang een duidelijke en goed afgebakende definitie van desinformatie te formuleren. De definitie die in het vervolg van deze scriptie zal worden aangehouden is de definitie van desinformatie die de Europese Commissie hanteert. Deze definitie luidt als volgt:

“Aantoonbaar foute of misleidende informatie die wordt gecreëerd, gepresenteerd en verspreid voor economisch gewin of om het publiek opzettelijk te bedriegen, en die schade in het publieke domein kan veroorzaken.” [[25]](#footnote-25)

In deze scriptie wordt er van ‘online’ desinformatie gesproken. Dit betreft op het internet voorkomende desinformatie, die veelal door middel van sociale media de wereld in geholpen wordt.

Wardle en Derakhshan[[26]](#footnote-26) spreken – naast desinformatie – ook van misinformatie en malinformatie. Het begrip misinformatie duidt op het per ongeluk creëren of verspreiden van foutieve informatie. Anders dan bij desinformatie is hierbij dus geen sprake van een schadelijke intentie. Malinformatie duidt op het opzettelijk gebruiken van waarheidsgetrouwe informatie om een individu, organisatie of land schade toe te brengen. Anders dan bij misinformatie is hier dus wel sprake van opzettelijkheid en een schadelijke intentie, maar gaat het niet om foutieve informatie. Er kan in algemene zin dus een onderscheid worden gemaakt tussen informatie die foutief is en informatie die wordt verspreid met de intentie schade te berokkenen.

Achter het begrip desinformatie schuilen ook andere categorieën uitingen die invloed kunnen hebben op digitale verkiezingscampagnes. Denk bijvoorbeeld aan propaganda; satire of parodie; clickbait; hoaxes en complottheorieën. Vanuit juridisch perspectief zijn – ondanks de overlappingen – vooral de verschillen tussen deze categorieën van belang. Sommige categorieën kunnen immers als bedreigingen voor de democratie worden gezien, terwijl andere juist bescherming genieten op grond van artikel 10 EVRM.[[27]](#footnote-27) In het volgende hoofdstuk wordt ingegaan op de reikwijdte van dit artikel.

In de literatuur is ook ‘nepnieuws’ een veel gebezigde term. Hoewel dit een pakkende term is die lekkerder over de tong rolt dan ‘online desinformatie’, is het om twee redenen van belang deze term te vermijden. [[28]](#footnote-28) Allereerst is de term ontoereikend om de complexiteit van het begrip desinformatie te weergeven. Desinformatie hoeft immers niet altijd ‘nep’ van aard te zijn: het kan ook om informatie gaan die deels waar is. Ook hoeft het niet per definitie om ‘nieuws’ te gaan. In sommige gevallen kan het namelijk gemanipuleerde video’s, gepersonaliseerde reclames of bijvoorbeeld illustraties betreffen. Ten tweede kan de term ‘nepnieuws’ ook een misleidend karakter hebben. Zo zijn er bijvoorbeeld (aanhangers van) politici die de term gebruiken om verslaggeving af te keuren waarin een standpunt wordt ingenomen of verdedigd waar zij het niet mee eens zijn. Hiermee komt de betrouwbaarheid van mediaorganisaties, en dus ook de persvrijheid, in het geding. Bovendien blijkt uit onderzoek dat burgers de term nepnieuws voornamelijk met politieke fanatiekelingen en slechte journalistiek associëren en dus niet zozeer met schadelijke, destructieve vormen van desinformatie. [[29]](#footnote-29)

## **2.2 Digitale politieke microtargeting**

In 2016 vonden twee onverwachte gebeurtenissen plaats: eerst leidde de succesvolle leave-campagne in Groot-Brittannië tot de Brexit en kort daarna werd Donald Trump verkozen tot de 45ste president van de Verenigde Staten. [[30]](#footnote-30) Beide gebeurtenissen hebben met elkaar gemeen dat er een lange en dure politieke campagne aan vooraf is gegaan. Deze campagnes zijn, klaarblijkelijk, het resultaat van microtargeting: een relatief nieuwe manier van politieke communicatie. [[31]](#footnote-31) Aan beide campagnes zou Cambridge Analytica, een Brits bedrijf, een bijdrage hebben geleverd door persoonlijkheidsgerichte politieke boodschappen onder de aandacht van specifieke doelgroepen te brengen. Er werden, op basis van hun Facebookprofielen, tientallen miljoenen persoonlijkheidsprofielen opgesteld van (Amerikaanse) burgers zonder dat het meerendeel van deze burgers hiervan op de hoogte werd gesteld. Hoewel niet duidelijk is welk effect dit op de uitkomsten van het Britse referendum en de Amerikaanse verkiezingen heeft gehad, heeft dit in ieder geval bijgedragen aan een groeiend onaangenaam gevoel ten aanzien van grote techbedrijven.[[32]](#footnote-32)

Het gebruik van data om politieke campagnes te bevorderen is een relatief nieuw fenomeen.[[33]](#footnote-33) Tegenwoordig kan er met behulp van relatief nieuwe technieken dan ook een steeds beter beeld worden verkregen van het gedrag, de standpunten en gevoelens van burgers. [[34]](#footnote-34) Men laat steeds meer digitale sporen achter en commerciële bedrijven worden steeds beter in het omzetten van die sporen in informatie die bruikbaar is om toekomstig gedrag van mensen, hun kwetsbaarheden en hun voorkeuren te voorspellen. [[35]](#footnote-35)

Digitale politieke microtargeting is een strategie waarbij gegevens over burgers worden gebruikt om groepen te identificeren van (min of meer) gelijkgestemde individuen. De basis van microtargeting bestaat dus uit data. [[36]](#footnote-36) Door persoonlijke data van burgers te gebruiken kunnen op maat gemaakte boodschappen worden gecreëerd. Naar deze groepen kunnen vervolgens gericht digitale politieke advertenties worden verstuurd die in lijn met hun standpunten liggen. Dergelijke advertenties zijn overigens alleen zichtbaar voor personen die binnen de groep van gelijkgestemde individuen vallen. Bij microtargeting wordt dus, anders dan bij traditionelere vormen van adverteren, niet een groep, maar juist het individu als uitgangspunt genomen.[[37]](#footnote-37) Hoe specifieker de beschikbare informatie over een individu is, hoe gerichter de advertenties kunnen worden ingezet en hoe relevanter de advertenties zijn die naar de ontvanger worden verstuurd, hoe groter de kans op overtuiging wordt. Zo kan een ZZP’er bijvoorbeeld de boodschap krijgen dat een politieke partij meer inkomenszekerheid voor zelfstandigen belooft, terwijl een docent juist onderwijsgerelateerde advertenties van dezelfde politieke partij te zien krijgt. Met microtargeting worden in beginsel dus alleen de mensen bereikt die interessant zijn voor de politieke adverteerder. [[38]](#footnote-38)

Microtargeting heeft raakvlakken met zowel de juridisch-politieke als de ethisch-maatschappelijke dimensie en kent naast positieve gevolgen ook negatieve gevolgen. [[39]](#footnote-39) Met name aan dat laatste wordt, vanuit juridisch-politiek oogpunt, aandacht besteed in deze scriptie.

## **2.3 Digitale verkiezingscampagnes**

De ontwikkeling van technologie kan worden gezien als een zegen en een vloek. Zo heeft de verbrandingsmotor voor meer mobiliteit gezorgd, maar draagt deze ontwikkeling tegelijkertijd voor een wezenlijk deel bij aan de klimaatverandering. Plastic verlengt de houdbaarheid van voedingsmiddelen, maar vervuilt ook de oceanen. Zo zijn er nog talloze andere voorbeelden denkbaar van technologische ontwikkelingen die een positieve bijdrage leveren aan de maatschappij, maar tegelijkertijd een keerzijde kennen. Dit geldt ook voor digitale technologie: ICT kan immers voor zowel goede als kwade doeleinden worden ingezet. [[40]](#footnote-40)

Ter illustratie: ter voorbereiding op de verkiezingen van 17 maart 2021 werd er door politici gebruik gemaakt van de app Clubhouse. Via deze app, die gericht is op audio en dus geen visueel beeld laat zien, kunnen individuen op een laagdrempelige manier met politici in gesprek gaan.[[41]](#footnote-41) Dergelijke ongedwongen gesprekken kunnen eraan bijdragen dat (vooral) jongeren actiever meedoen aan het publieke debat en sneller naar de stembus gaan. Een ander voorbeeld van een positief gevolg van digitale ontwikkelingen omtrent verkiezingen is dat het kabinet een samenwerking is aangegaan met influencers[[42]](#footnote-42) om het naleven van de coronaregels onder jongeren te bevorderen. Zij zorgen ervoor dat de boodschap op een toegankelijke manier, bijvoorbeeld via vlogs, bij jongeren aankomt. [[43]](#footnote-43)

Naast positieve voorbeelden zijn er ook negatieve voorbeelden te noemen van digitalisering van verkiezingscampagnes. Zo deelde Geert Wilders (PVV) in februari 2017 een gemanipuleerde foto van Alexander Pechtold (D66) op Twitter, waarin de toenmalig D66-leider in een foto van een pro-shariademonstratie was gefotoshopt. [[44]](#footnote-44) In datzelfde jaar kwam aan het licht dat de partij Denk nepaccounts had gebruikt op verschillende sociale mediakanalen om (politici van) andere partijen te bekritiseren en om bovendien het beeld te wekken dat Denk een grotere online aanhang had. [[45]](#footnote-45) In 2018 kwam Denk opnieuw in opspraak, vanwege een online nepadvertentie die door Denk-politici was ontworpen. Hierin werd de illusie gewekt dat de slogan ‘Na 15 maart gaan we Nederland zuiveren’ campagnemateriaal van de PVV zou zijn. Nadat dit door journalisten kenbaar werd gemaakt, werden zij er door Denk-politici van verweten hen in een kwaad daglicht te plaatsen. [[46]](#footnote-46)

Zoals bovenstaande voorbeelden illustreren werd er in de aanloop naar de Tweede Kamerverkiezingen in 2017 dus al flink gebruik gemaakt van digitale vormen van communicatie door politici. Het coronavirus heeft er echter (noodgedwongen) voor gezorgd dat de verkiezingscampagnes zich in de aanloop naar de Tweede Kamerverkiezingen van maart 2021 vooral online hebben afgespeeld. [[47]](#footnote-47) Wanneer in deze scriptie van verkiezingscampagnes gesproken wordt, dan wordt daarmee de periode voorafgaand aan de verkiezingen bedoeld waarin partijen hun verkiezingsprogramma’s bekendmaken, hier reclame over maken en hier met elkaar over in debat gaan. Deze periode loopt door tot het einde van de verkiezingen, te weten de dag waarop gestemd kan worden. De focus van deze scriptie ligt op digitale verkiezingscampagnes. Met andere woorden: verkiezingscampagnes die digitaal – via online platforms – worden gevoerd.

Naast de potentiële voordelen die online communicatie en online advertenties met zich brengen, leveren deze ook risico’s op. Binnen de Nederlandse politiek heersen dan ook zorgen over de toepassing van digitalisering in verkiezingscampagnes. Dit bleek in 2017 al uit de brief uit die Minister Ollongren van Binnenlandse Zaken eind 2017 naar de Tweede Kamer heeft verstuurd. Hierin uitte zij haar ongerustheid met betrekking tot de publieke opinie en de online beïnvloeding daarvan. [[48]](#footnote-48) Meer recent, namelijk in oktober 2020, heeft de Tweede Kamer de motie Middendorp/Kuiken gesteund, waarin Kajsa Ollongren, de Minister van Binnenlandse zaken, werd verzocht om een regeling voor de transparantie van online advertenties. [[49]](#footnote-49) In de aanloop naar de Tweede Kamerverkiezingen van 2021 initieerde Ollongren de Nederlandse Gedragscode Transparantie Online Politieke Advertenties (hierna: Gedragscode). Deze Gedragscode had tot doel om manipulatie van verkiezingen door misbruik van sociale media en (online) desinformatie rond de Nederlandse Tweede Kamerverkiezingen tegen te gaan.[[50]](#footnote-50) In de Gedragscode werden (vrijwillige) gedragsregels voor politieke partijen en online platforms over online advertenties in de Nederlandse politieke context opgesteld. [[51]](#footnote-51) Dit geeft de bezorgdheid weer over veranderingen voor de democratie door digitalisering en laat bovendien de noodzaak zien voor het tegengaan en reguleren van de in paragraaf 2.1, respectievelijk 2.2 beschreven fenomenen met betrekking tot digitale verkiezingscampagnes. In hoofdstuk 5.6 van deze scriptie zal er uitgebreid worden stilgestaan bij de relevantie van de Gedragscode en de verhouding tussen de Gedragscode en het recht op vrije meningsuiting en deelname aan het publieke debat.

**Tussenconclusie**Desinformatie is een relatief oud fenomeen dat – vanwege het omvangrijke en complexe karakter – vooralsnog niet eenduidig (juridisch) kan worden gedefinieerd. Wel kan er in ieder geval worden geconcludeerd dat het om een vorm van onjuiste en misleidende informatie gaat met mogelijk schadelijke gevolgen. Van belang is overigens om desinformatie van de – wellicht bekendere – term nepnieuws te onderscheiden, nu desinformatie niet per definitie nep is. Microtargeting is – anders dan desinformatie – een relatief nieuw fenomeen waarbij commerciële bedrijven de digitale sporen die door mensen wordt achtergelaten omzetten in bruikbare informatie om toekomstig gedrag, maar ook kwetsbaarheden en voorkeuren van burgers te voorspellen. Nu verkiezingscampagnes in het huidige Covid-19-tijdperk vrijwel volledig digitaal worden gevoerd, leidt dit ertoe dat desinformatie en microtargeting zich steeds sneller ontwikkelen. Naast de bijbehorende voordelen die digitale verkiezingscampagnes met zich brengen, komen er dus ook risico’s bij kijken.

# Hoofdstuk 3 – Juridisch kader

In het vorige hoofdstuk zijn de begrippen ‘online desinformatie’ en ‘microtargeting’ gedefinieerd. In dit hoofdstuk wordt het juridisch kader voor het tegengaan van online desinformatie en de regulering van microtargeting geïdentificeerd. Hierbij wordt eerst gekeken naar de reikwijdte van het recht op vrijheid van meningsuiting en informatie: wordt online desinformatie beschermd door de vrijheid van meningsuiting en vormt het gebruik van microtargeting een gevaar voor het recht op informatie? Vervolgens worden de (positieve) verplichtingen van de staat besproken. Hierna wordt het recht op privacy en bescherming van persoonsgegevens toegelicht. Dit is van belang nu er, met name bij de inzet van gepersonaliseerde online politieke advertenties, veelvuldig gebruik wordt gemaakt van data van burgers. Tot slot komt de aansprakelijkheid van internetplatforms aan bod. Onder welke omstandigheden kunnen zij al dan niet aansprakelijk worden gesteld voor content die hun gebruikers genereren? Het juridisch kader dat in dit hoofdstuk wordt geschetst dient ook in de volgende hoofdstukken – bij de bespreking van de potentiële gevaren (hoofdstuk 4) en de beoordeling van de huidige maatregelen (hoofdstuk 5) – in acht te worden genomen.

## **3.1 De vrijheid van meningsuiting en het recht op informatie**

De vrijheid van meningsuiting, en het daarmee samenhangende recht op informatie, is een fundamenteel mensenrecht dat onder andere is vastgelegd in respectievelijk artikel 10 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) en artikel 11 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest). Dit recht omvat de vrijheid om een mening te vormen en informatie te verstrekken of te ontvangen zonder dat hier bijvoorbeeld voorafgaande toestemming voor nodig is. Bovendien dient mediavrijheid- en pluriformiteit te worden gerespecteerd.[[52]](#footnote-52)

De uitspraken van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) over de vrijheid van meningsuiting in de context van online desinformatie en gepersonaliseerde online politieke advertenties kunnen als leidraad dienen voor de interpretatie van artikel 10 EVRM. Hoewel de vrijheid van meningsuiting ook door artikel 11 van het Handvest wordt gewaarborgd, heeft het Hof van Justitie van de Europese Unie (hierna: HvJEU), dat belast is met de interpretatie van dit artikel, zich tot op heden nog niet over de vrijheid van meningsuiting in het kader van gepersonaliseerde online politieke advertenties gebogen.[[53]](#footnote-53) Bovendien biedt het EHRM een ruimere bescherming op dit gebied. [[54]](#footnote-54) Om uiteenlopende standaarden te voorkomen zullen de uitspraken van het EHRM leidend worden geacht en valt de jurisprudentie van het HvJEU buiten de reikwijdte van deze paragraaf.

Het EHRM legt in de uitspraak Handyside tegen het Verenigd Koninkrijk uit dat het belang van de vrije meningsuiting essentieel is voor pluralisme, tolerantie en ruimdenkendheid binnen het publieke debat. Bovendien worden beledigende, verontrustende en schokkende opvattingen beschermd door de vrijheid van meningsuiting.[[55]](#footnote-55) Het Hof benadrukt verder dat het, met name in de periode die aan verkiezingen voorafgaat, essentieel is dat verschillende soorten opvattingen en informatie in beginsel worden beschermd, zodat burgers zich kritisch in politieke discussies kunnen mengen. [[56]](#footnote-56) Het belang van de vrijheid van meningsuiting en informatie is groot: het vormt immers de kern van een democratische samenleving. [[57]](#footnote-57)

Het recht op vrijheid van meningsuiting en informatie is echter geen absoluut recht [[58]](#footnote-58): de overheid mag dit recht inperken als aan de voorwaarden van artikel 10, tweede lid, EVRM wordt voldaan. De beperkingen moeten dan wel een legitiem doel dienen, bij wet voorzien zijn en noodzakelijk worden geacht in een democratische samenleving. [[59]](#footnote-59) Bovendien gelden er bepaalde verantwoordelijkheden en plichten. Zo dient er bij de uitoefening van dit recht te goeder trouw te worden gehandeld en dienen publicaties op feitelijke, accurate en betrouwbare informatie te berusten. [[60]](#footnote-60) Per casus dient te worden beoordeeld of hieraan wordt voldaan. [[61]](#footnote-61) Uit artikel 17 EVRM blijkt dat uitingen die in strijd zijn met de fundamentele waarden van het EVRM niet worden beschermd. [[62]](#footnote-62) Zo wordt satire – dat is bedoeld om te provoceren en meningen uit te lokken – bijvoorbeeld wel beschermd, maar hate speech niet. [[63]](#footnote-63)

Professionele media en journalisten vervullen van oudsher de rol van publieke waakhond binnen de democratische samenleving. [[64]](#footnote-64) De rol van de traditionele media is de afgelopen decennia echter sterk veranderd. Met de komst van het internet zijn veel nieuwe mogelijkheden ontstaan om informatie te verspreiden onder gebruikers. Bovendien maakte het internet een verandering door rond het nieuwe millennium, waarin de internetgebruiker centraal staat: informatie wordt nu niet meer alleen door gebruikers ontvangen, maar ook zelf door hen gegenereerd. [[65]](#footnote-65) Er is een grote hoeveelheid aan ‘user generated content’ beschikbaar voor internetgebruikers. Dit is dus informatie die niet door traditionele media wordt verzorgd. [[66]](#footnote-66) Deze verandering brengt met zich dat nu ook de ‘gewone’ burger de rol van publieke waakhond kan bekleden. Het EVRM dient dan ook zoveel mogelijk uitgelegd te worden met het oog op de huidige omstandigheden: een statische interpretatie van het EVRM dient voorkomen te worden. [[67]](#footnote-67) Bovendien dienen de rechten die door het EVRM worden gewaarborgd zodanig te worden uitgelegd en toegepast, dat deze daadwerkelijk effectief blijken. [[68]](#footnote-68)

## **3.2 Verplichtingen voor de staat**

Zoals besproken in de vorige paragraaf is uitoefening van de vrijheid van meningsuiting essentieel in een democratische samenleving. Aan de staat komt dan ook de verplichting toe om de effectieve uitoefening van dit recht te bevorderen. Negatieve verplichtingen, waarin de staat zich onthoudt van activiteiten die inbreuk maken op dit recht, volstaan niet voor een effectieve uitoefening van de vrije meningsuiting. De staat dient actief beleid te ontwikkelen waarin realisatie en bescherming van de vrijheid van meningsuiting naar voren komt. [[69]](#footnote-69) In de jurisprudentie wordt door het EHRM een onderscheid gemaakt tussen drie soorten positieve verplichtingen voor de Staat met betrekking tot de vrijheid van meningsuiting. Allereerst dient de staat adequate maatregelen te treffen om de vrije meningsuiting te beschermen en effectieve uitoefening van dit recht te garanderen. [[70]](#footnote-70) Hierbij komt aan de staat enige mate van beoordelingsvrijheid (margin of appreciation) toe: de staat mag dus zelf invullen welke maatregelen passend worden geacht. [[71]](#footnote-71) Ten tweede dient de staat zorg te dragen voor een gunstig klimaat omtrent deelname aan het publieke debat, zodat individuen hun recht op uitingsvrijheid zorgeloos kunnen uitoefenen. [[72]](#footnote-72) Ten derde dient de staat een pluralistisch informatieaanbod te verwezenlijken door toegang te garanderen tot onpartijdige informatie. [[73]](#footnote-73) Met de komst van het internet en de steeds verdere digitalisering van de samenleving is ook de omvang van het informatieaanbod gegroeid. Toch leidt een omvangrijk informatieaanbod niet per definitie tot verscheidenheid van de informatie die daadwerkelijk wordt waargenomen. [[74]](#footnote-74)

Uit het bovenstaande kan dus worden geconcludeerd dat de staat actief moet ingrijpen als het gaat om het effectief garanderen van pluralisme. [[75]](#footnote-75) Het EHRM benadrukt het belang van een ‘plurality of voices’ met betrekking tot onderwerpen die van publiek belang zijn. Bovendien moet iedereen effectief kunnen deelnemen aan het publieke debat. Dit geldt dus ook voor kleine actiegroepen en individuen. [[76]](#footnote-76) Dit brengt met zich dat grote partijen het publieke debat niet mogen verstoren of domineren. Vrijwillige maatregelen die bepaalde vormen van gepersonaliseerde online politieke advertenties beperken kunnen er, met name wanneer zij door dominante internetdiensten worden genomen, voor zorgen dat bepaalde groepen onnodig worden beperkt in hun vermogen om doeltreffend te communiceren. Dit is schadelijk voor het pluralisme. [[77]](#footnote-77)

Het EHRM heeft in *Animal Defenders[[78]](#footnote-78)* een verband tussen pluralisme en de regulering van gepersonaliseerde online politieke advertenties gelegd. Het EHRM erkent in deze uitspraak dat een beperking van een vrij en pluralistisch debat het gevolg kan zijn van concurrerende voordelen die machtige financiële groepen op het gebied van betaalde advertenties verkrijgen. Opnieuw wordt de positieve verplichting genoemd die de staat kan hebben om in te grijpen en pluralisme op effectieve wijze te garanderen.

## **3.3. Het recht op privacy en de bescherming van persoonsgegevens**

Het recht op privacy is een fundamenteel mensenrecht dat wordt gewaarborgd door respectievelijk artikel 8 EVRM en artikel 7 en 8 Handvest. Hoewel artikel 8 EVRM ook van toepassing is op digitale persoonsgegevens, bieden artikel 7 en 8 Handvest en de Algemene Verordening Gegevensbescherming (hierna: AVG) specifiekere bescherming ten aanzien van persoonsgegevens. [[79]](#footnote-79) De verwerking van persoonsgegevens valt onder het recht op bescherming van persoonsgegevens. De AVG ziet erop toe dat er rechtmatig met persoonsgegevens wordt omgegaan. Het verwerken van persoonsgegevens dient te berusten op één van de grondslagen uit de AVG, zoals het verkrijgen van toestemming om tot verwerking over te gaan. Het gaat hierbij om informatie over een natuurlijke persoon die direct of indirect identificeerbaar is. [[80]](#footnote-80)

Politieke advertenties kunnen op internetdiensten verzamelde persoonsgegevens gebruiken om gericht gesponsorde berichten te verspreiden. Relevante internetdiensten, zoals Google en Facebook, zorgen vervolgens voor gerichte communicatie met het online publiek. [[81]](#footnote-81) De AVG is hierbij zeer relevant, gezien het feit dat deze op de verwerking van persoonsgegevens van toepassing is. De AVG vereist eerlijkheid, rechtmatigheid en transparantie bij een dergelijke verwerking. Ook dient de regelgeving onder onafhankelijk toezicht te worden geplaatst en dienen de rechten van betrokkenen te worden beschermd. [[82]](#footnote-82) The European Data Protection Board (EDPB) heeft richtlijnen omtrent het gebruik van persoonsgegevens in de context van online politieke verkiezingscampagnes opgesteld. [[83]](#footnote-83)

In 2019 is de Nederlandse Autoriteit Persoonsgegevens een onderzoek gestart naar het gebruik van persoonsgegevens in de context van digitale verkiezingscampagnes. [[84]](#footnote-84) Het gaat om een verkennend onderzoek dat zich uitstrekt tot de inzet van derden die de politieke partijen bij hun verkiezingscampagnes bijstaan. De Autoriteit Persoonsgegevens ziet er – in dit onderzoek – met name op toe dat de extra waarborgen die omtrent privacy in de AVG zijn opgenomen worden nageleefd. De AVG is breed toepasbaar: zijn brede doelstellingen en relatief open bepalingen dragen bij aan de significante rol die het kan spelen ten aanzien van de bescherming van de vrijheden en rechten van internetgebruikers. Ook kan de AVG met betrekking tot desinformatiecampagnes bescherming bieden tegen disproportionele verwerking van persoonsgegevens. [[85]](#footnote-85)

Europese wetgeving vereist, anders dan bijvoorbeeld Amerikaanse wetgeving, dat het gebruik van persoonsgegevens om mensen mogelijkerwijs te beïnvloeden eerlijk, transparant en wettig moet zijn. Hoewel het niet per definitie onwettig is om feitelijk onjuiste informatie te publiceren, zou onderzoek van het publiek met gerichte onware boodschappen geen wettelijke basis hebben volgens de AVG. Opmerking verdient hierbij dat veel handelingen van de betrokken internetdiensten ten aanzien van persoonsgegevens het subject zijn van onderzoeken en rechtszaken. [[86]](#footnote-86)

Voor de verwerking van bijzondere categorieën persoonsgegevens die relevant zijn voor (gepersonaliseerde online) politieke advertenties bevat de AVG een specifieke – beperkendere – regeling. In beginsel geldt dat de verwerking van dergelijke gegevens niet is toegestaan. [[87]](#footnote-87) Bovendien gelden hierbij een aantal uitzonderingen die strikt geïnterpreteerd moeten worden, zoals de uitdrukkelijke toestemming van de betrokkene voor verwerking van de persoonsgegevens. [[88]](#footnote-88)

## **3.4 De aansprakelijkheid van online platforms**

Online platforms zijn in de loop der jaren steeds belangrijker geworden. Dominante sociale mediakanalen beschikken over een groot online marktaandeel en vormen daarmee een gevaar voor het pluralistische informatieaanbod.[[89]](#footnote-89) Zo is Facebook niet alleen in het bezit van Facebook Messenger, maar ook van Instagram en WhatsApp. Ter illustratie: Facebook en andere sociale mediakanalen worden gemiddeld gezien door 31% van de gebruikers aangewend voor het nieuws- en informatieaanbod.[[90]](#footnote-90) Dit brengt een zekere macht voor het platform met zich mee. Bovendien wordt er tijdens verkiezingscampagnes – zoals besproken in paragraaf 2.3 – door politici in toenemende mate gebruik gemaakt van sociale mediakanalen om op een laagdrempelige manier in aanraking met kiezers te komen. Het is daarom relevant om de aansprakelijkheid van deze platforms te analyseren.

De richtlijn inzake elektronische handel (hierna: e-Commercerichtlijn) omvat regels omtrent de aansprakelijkheid van internetplatforms voor online content. [[91]](#footnote-91) Dit is belangrijk, aangezien het HvJEU heeft bepaald dat sociale mediakanalen als hostingdienstverlener worden aangemerkt wanneer zij informatie – die door gebruikers is verstrekt – op hun servers opslaan. [[92]](#footnote-92) Alvorens een internetplatform als host kan worden aangemerkt – en dus onder de uitzonderingsbepaling van artikel 14 e-Commercerichtlijn valt – dient aan een aantal voorwaarden te worden voldaan. [[93]](#footnote-93) Zo dient de informatie die door gebruikers wordt verstrekt enkel opgeslagen of doorgegeven te worden. De praktijken omtrent de content op een platform dat als ‘host’ wordt aangemerkt mogen bovendien slechts een automatisch, technisch en passief karakter hebben en het platform mag geen controle of kennis hebben over de opgeslagen of doorgegeven informatie. [[94]](#footnote-94) Wanneer het platform wel kennis verkrijgt over informatie met een illegaal karakter of illegale activiteiten, moet er prompt worden gehandeld om de toegang tot deze informatie onmogelijk te maken of de informatie te verwijderen. [[95]](#footnote-95)

De richtlijn Audiovisuele Mediadiensten (hierna: AVMD-richtlijn)[[96]](#footnote-96) heeft tot doelstelling een minimum aan harmonisatie in de EU te waarborgen omtrent audiovisuele mediadiensten, om belemmeringen voor het vrije verkeer van deze diensten weg te nemen. De AVMD-richtlijn is uit de vroegere richtlijn ‘Televisie zonder grenzen’ voortgekomen en ziet, naast traditionele televisieomroep, ook toe op audiovisuele mediadiensten. Sinds de herziening van de richtlijn in 2018, kunnen nu ook aanbieders van videoplatformdiensten onder de reikwijdte van de richtlijn vallen. [[97]](#footnote-97)

Niet alle bepalingen van de AVMD-richtlijn hebben echter betrekking op aanbieders van videoplatformdiensten. De nadruk ligt voornamelijk op schadelijke inhoud voor minderjarigen, misdrijven op het gebied van misbruik van kinderen, vreemdelingenhaat en racisme, bepaalde soorten illegale content – zoals het aanzetten tot haat of geweld, en het uitlokken van een terroristisch misdrijf in het openbaar. [[98]](#footnote-98) De lidstaten dienen ervoor te zorgen dat de aanbieders van videoplatformdiensten die onder hun bevoegdheid vallen adequate maatregelen treffen ter bescherming van minderjarigen en het publiek in algemene zin tegen programma’s, audiovisuele commerciële communicatie en door gebruikers ontwikkelde video’s die inhoud zoals hierboven beschreven weergeven. De artikelen 12 tot en met 15 van de e-Commerce richtlijn zijn hierbij onverkort van toepassing. [[99]](#footnote-99)

Het EHRM en het HvJEU hebben zich in de loop der jaren in toenemende mate uitgelaten over de aansprakelijkheid van internetplatforms. Zo oordeelde het HvJEU dat het opleggen van een toezichtplicht aan een internetplatform ten aanzien van online content onverenigbaar met artikel 15 e-Commercerichtlijn is. [[100]](#footnote-100) Toezichtverplichtingen zijn in speciale gevallen overigens wel geoorloofd. [[101]](#footnote-101) In 2015 deed de Grote Kamer van het EHRM uitspraak over de aansprakelijkheid van online nieuwsplatforms ten aanzien van de commentaren van hun gebruikers. [[102]](#footnote-102) In deze casus ging het om comments die als hate speech kunnen worden aangemerkt. Gebruikers lieten deze op het desbetreffende nieuwsplatform achter en dit leidde niet tot een schending van het recht op vrije meningsuiting van het platform. Hierbij werden een aantal relevante factoren in overweging genomen, zoals de aard van de content, de manier waarop het platform werd beheerd en de doeltreffendheid van zowel de getroffen maatregelen als de opgelegde sancties. [[103]](#footnote-103) In 2016 was het EHRM van oordeel dat een platform kan volstaan met het ontwikkelen van een doeltreffend ‘notice and take downsystem’ voor beledigende comments, maar niet voor comments die evident onrechtmatig zijn. [[104]](#footnote-104) In de uitspraak Pihl tegen Zweden bouwt het EHRM voort op dit oordeel door vast te stellen dat een blogbeheerder niet verantwoordelijk kan worden gehouden voor een snel verwijderd lasterlijk bericht van een gebruiker. [[105]](#footnote-105)

Kortom, uit de jurisprudentie van het EHRM kan worden afgeleid dat de kans op aansprakelijkheid voor internetplatforms toeneemt, naarmate de redactionele controle hoger is. [[106]](#footnote-106) Hierbij dient wel te worden opgemerkt dat het bij online desinformatie, ondanks het onwenselijke karakter ervan, wel vaak om legale content gaat. De aansprakelijkheid van internetplatforms is pas aan de orde in het geval dat illegale content door derden op het desbetreffende platform verschijnt.

**Tussenconclusie**  
Online desinformatie is veelal gericht op de beïnvloeding van het publieke debat. Dit raakt de kern van de democratische samenleving. Aan de staat komt de verplichting toe om actief in te grijpen om een pluralistisch informatieaanbod te garanderen, maar de effectieve uitoefening van het recht op vrijheid van meningsuiting mag hier niet door worden belemmerd.

Het verschil tussen *Delfi* en verwante uitspraken van het EHRM in deze context is dat het in *Delfi* om hate speech ging. Hate speech kan worden gezien als doorslaggevende factor: wanneer er slechts sprake is van desinformatie dient de effectieve uitoefening van de vrije meningsuiting alsnog te worden gewaarborgd.

Internetplatforms moeten zich houden aan de verplichtingen die hen op grond van de AVG toekomen. Wat betreft de aansprakelijkheid van internetplatforms kan op basis van de jurisprudentie van het EHRM worden geconcludeerd dat zij verantwoordelijk kunnen worden gehouden voor illegale content die door derden wordt gegenereerd. Hierbij is van belang om in acht te nemen dat online desinformatie vaak legale content betreft.

# Hoofdstuk 4 – De gevolgen van online desinformatie en microtargeting voor digitale verkiezingscampagnes

In hoofdstuk 2 van deze scriptie werd kort stilgestaan bij de risico’s voor de democratische rechtsstaat die online desinformatie en microtargeting – in het kader van digitale verkiezingscampagnes – mogelijk met zich brengen. Met name de beïnvloeding van de opinievorming en het publieke debat bleek in dit verband problematisch te zijn. Een helder en concreet juridisch kader – zoals geanalyseerd in hoofdstuk 3 – is dan ook van essentieel belang in de strijd tegen negatieve beïnvloeding van dergelijke democratische kernwaarden. In dit hoofdstuk zal kritisch worden gekeken naar de potentiële gevaren van de verspreiding van online desinformatie en de inzet van microtargeting. Bovendien zal worden gekeken naar de mate waarin verwezenlijking van dergelijke gevaren plaatsvindt in de context van Nederlandse digitale verkiezingscampagnes: is een nuance hier op zijn plaats?

## **4.1 Potentiële gevaren van online desinformatie**

Digitalisering zorgt voor wereldwijde verbondenheid en heeft er bovendien toe geleid dat de toegang tot informatie laagdrempelig is. De overvloed van informatie kan echter tot gevolg hebben dat individuen het kaf niet meer van het koren kunnen scheiden. Door de grote hoeveelheid aan beschikbare informatie en data op het internet is het bovendien voor vrijwel iedereen mogelijk om informatie – en dus ook desinformatie – te vergaren en te verspreiden. De online verspreiding van desinformatie kan de informatievoorziening – die cruciaal is voor een goed geïnformeerde democratische gedachtewisseling – ondermijnen. [[107]](#footnote-107) Toegang tot betrouwbaar nieuws is – in een democratische samenleving als Nederland – immers van wezenlijk belang voor individuen om een mening te kunnen vormen omtrent actuele maatschappelijke en politieke kwesties en om bovendien effectief van het stemrecht gebruik te kunnen maken. [[108]](#footnote-108)

Online desinformatie kan verschillende vormen aannemen en wordt op dit moment veelal in de vorm van misleidende teksten door bots[[109]](#footnote-109) verspreid. Deze vorm van verspreiding is vooralsnog relatief ‘eenvoudig’ te detecteren. Technologie blijft zich echter ontwikkelen en de verwachting is dan ook dat bots steeds geavanceerder zullen worden en dus steeds moeilijker van mensen te onderscheiden zullen zijn. Dit kan tot gevolg hebben dat de online verspreiding van desinformatie in de (nabije) toekomst moeilijker kan worden gedetecteerd. [[110]](#footnote-110) Bovendien maken recente technologische ontwikkelingen het mogelijk om beeld en geluid relatief makkelijk te manipuleren. [[111]](#footnote-111) Zogeheten ‘deepfakes’[[112]](#footnote-112) duiken vandaag de dag in toenemende mate op. [[113]](#footnote-113) Snelle technologische ontwikkelingen op het gebied van kunstmatige intelligentie en machine learning kunnen ervoor zorgen dat ook deepfakes in de toekomst moeilijker onderscheiden kunnen worden van origineel beeld- en geluidmateriaal. [[114]](#footnote-114)

De verspreiding van online desinformatie beïnvloedt niet alleen de maatschappelijke meningsvorming en het publieke debat, maar kan ook manipulatie van verkiezingen tot gevolg hebben. Uit onderzoek is gebleken dat grootschalige online verspreiding van desinformatie in de Verenigde Staten heeft plaatsgevonden tijdens de Amerikaanse presidentsverkiezingen in 2016. [[115]](#footnote-115) Later zijn ook omtrent de Europese verkiezingen desinformatiecampagnes gevoerd. In beide gevallen werden desinformatieberichten voornamelijk door Russische bots via sociale mediakanalen verspreid. [[116]](#footnote-116) Hoewel onduidelijk is in welke mate de publieke opinie daadwerkelijk is beïnvloed, heeft dit wel tot grote zorgen over het functioneren van de democratische samenleving geleid. [[117]](#footnote-117) Het feit dat de publieke opinie – en daarmee ook het besluitvormingsproces – kan worden beïnvloed, kan namelijk manipulatie van verkiezingscampagnes tot gevolg hebben. Het wordt bovendien niet alleen steeds moeilijker om te achterhalen waar informatie vandaan komt, maar ook om de juistheid van informatie te beoordelen. Dit kan tot een afname in het vertrouwen van de juistheid van het informatieaanbod leiden. [[118]](#footnote-118)

## **4.2 Potentiële gevaren van microtargeting**

Het vanuit de Verenigde Staten overgewaaide fenomeen ‘microtargeting’ kent zowel voordelen als nadelen voor de democratie. Dankzij microtargeting kunnen politieke partijen burgers effectief bereiken en kan bovendien politieke betrokkenheid onder stemgerechtigden worden gestimuleerd. Microtargeting kent echter ook een keerzijde: het verzamelen van persoonsgegevens kan een bedreiging vormen voor het recht op privacy. Verder kan het onduidelijk zijn wat een politieke partij precies belooft, wanneer deze partij steeds verschillende boodschappen naar verschillende stemgerechtigden verstuurt. [[119]](#footnote-119) Als een kiezer veel politieke advertenties van een partij over een bepaald onderwerp te zien krijgt, dan kan dit tot de onterechte conclusie leiden dat dit onderwerp een speerpunt voor de partij is. Het is in veel gevallen lastig te achterhalen of een politieke advertentie op maat gemaakt is en dit kan tot gevolg hebben dat een verkeerd beeld van de prioriteiten van een politieke partij wordt geschetst. Dit kan bijvoorbeeld problematisch zijn wanneer er compromissen moeten worden gesloten tijdens onderhandelingen met coalitiepartners. Zo kan een kiezer op een politieke partij stemmen vanwege hun standpunt over het onderwijs, maar kan die partij haar standpunt matigen of zelfs (deels) van het standpunt afzien tijdens coalitie-onderhandelingen. Bovendien is het ook voor politici moeilijk te duiden welke onderwerpen binnen hun partij doorslaggevend voor de kiezers zijn en welke niet. [[120]](#footnote-120)

Een andere bedreiging is dat microtargeting afbreuk doet aan het publieke debat. Kiezers kunnen door campagnes die via massamedia worden gevoerd in aanraking komen met een aantal grote onderwerpen. Denk bijvoorbeeld aan thema’s als immigratie, onderwijs en gezondheidszorg. De standpunten van politieke partijen met betrekking tot dergelijke onderwerpen zijn dan bekend onder het merendeel van de kiezers. Met de kennis die zij via de campagnes vergaren kunnen kiezers zich in maatschappelijke discussies mengen. In het geval van microtargeting komen kiezers echter enkel in aanraking met standpunten over de specifieke onderwerpen die voor hen relevant zijn en met hun eigen opvattingen stroken. Dit maakt het moeilijker voor hen om met anderen te discussiëren over maatschappelijke kwesties. [[121]](#footnote-121)

## **4.3 Enige nuancering vanuit nationaal perspectief**

Uit paragraaf 2 en 3 van dit hoofdstuk is gebleken dat de online verspreiding van desinformatie en de inzet van microtargeting door politieke partijen tijdens (digitale) verkiezingscampagnes het publieke debat op negatieve wijze kunnen beïnvloeden. Dit is zorgelijk, nu deelname aan het publieke debat één van de kernelementen van een democratische samenleving is. Toch is enige nuancering vanuit nationaal perspectief hier op zijn plaats.

Ten eerste is Nederland gebonden aan de relatief strenge Europese privacyregels die voortkomen uit de in hoofdstuk 3 besproken AVG. Hoewel politieke partijen persoonsgegevens van hun leden en van diegenen die daar expliciete toestemming voor geven mogen verwerken[[122]](#footnote-122), is het in beginsel op grond van de AVG verboden om persoonsgegevens met betrekking tot iemands politieke voorkeuren te verzamelen. Dergelijke gegevens behoren namelijk tot de bijzondere categorie van (gevoelige) persoonsgegevens. [[123]](#footnote-123) Bovendien moet transparantie geboden worden over de persoonsgegevens die verwerkt worden en waarom deze verwerkt worden (bijvoorbeeld middels een privacyverklaring). [[124]](#footnote-124)

Behoudens de AVG is op grond van de e-Privacyrichtlijn, kort samengevat, vereist dat een bedrijf transparant is over het gebruik van tracking cookies en andere technieken die vergelijkbaar zijn. [[125]](#footnote-125) Als er dus cookies worden gebruikt voor, in dit geval, politieke microtargeting, dan dient het bedrijf – om microtargeting transparanter te maken – mensen dus te informeren over het doel van het gebruik van cookies. Voor politieke microtargeting betekent dat dus dat mensen geïnformeerd moeten worden over het feit dat zij op internet gevolgd worden om hen gerichte (gepersonaliseerde) politieke advertenties te kunnen sturen.

In de Verenigde Staten vormen data brokers een grote industrie. Dit zijn bedrijven die in persoonsgegevens handelen. [[126]](#footnote-126) In Europa zijn de privacyregels echter strenger dan in de Verenigde Staten en is het dus lastiger om aan gedetailleerde informatie over kiezers te komen. [[127]](#footnote-127)

Ten tweede kent Nederland een meerpartijenstelsel. Anders dan in landen met een tweepartijenstelsel, zoals de Verenigde Staten, vormt microtargeting daarom een minder groot gevaar. In het Nederlandse systeem zijn er immers veel meer partijen die met elkaar concurreren om de stem van de kiezer voor zich te winnen dan in de Verenigde Staten. Dat maakt het moeilijker om gerichte advertenties naar kiezers van één partij te sturen. Het is immers makkelijker in te schatten of iemand Republikein of Democraat is, dan of iemand Groenlinks, D66 of misschien toch PvdA stemt. [[128]](#footnote-128)

Ten derde kunnen de potentiële gevaren worden genuanceerd, omdat kiezers ook toegang hebben tot informatiebronnen die niet gepersonaliseerd zijn, zoals de reguliere media. [[129]](#footnote-129) Dit kan het ‘informatiebubbel’ achtige element van microtargeting deels wegnemen. [[130]](#footnote-130)

**Tussenconclusie**De mogelijke gevolgen van de verspreiding van online desinformatie en de inzet van microtargeting kunnen een bedreiging vormen voor de democratie. Hierbij is voornamelijk de beïnvloeding van de publieke opinie en besluitvormingsprocessen zorgelijk, omdat dit tot manipulatie van verkiezingen kan leiden. De impact en het bereik van desinformatie neemt toe door snelle technologische ontwikkelingen, zoals de opkomst van deepfakes, die het moeilijker maken om gemanipuleerd geluid- en beeldmateriaal van het origineel te onderscheiden. Ook de inzet van microtargeting kan deelname aan het publieke debat ondermijnen. Toch moeten het bereik en de impact van microtargeting voor Nederland niet overdreven worden: Nederland is immers gebonden aan de relatief strenge Europeesrechtelijke normen omtrent transparantie en privacybescherming.

# **Hoofdstuk 5 – Maatregelen**

Uit de voorgaande hoofdstukken kan worden afgeleid dat online desinformatie – en de daarmee samenhangende inzet van microtargeting – een complex en omvangrijk karakter heeft. Bovendien bestaat er voor de problemen die naar aanleiding van de verspreiding van online desinformatie en de inzet van gepersonaliseerde politieke advertenties ontstaan vooralsnog geen eenduidige juridische oplossing. [[131]](#footnote-131)

In dit hoofdstuk zal er dan ook worden gekeken naar (juridische) mogelijkheden om deze fenomenen in de toekomst beter te kunnen reguleren. De focus ligt hierbij op sociale mediaplatforms die, zoals besproken in hoofdstuk 3, een aanzienlijke rol spelen ten aanzien van zowel de verspreiding van online desinformatie als de inzet van gepersonaliseerde politieke advertenties. Er wordt, vanwege het grensoverschrijdende karakter van de problematiek – allereerst stilgestaan bij de reeds bestaande regelgevende en zelfregulerende maatregelen in Europa. Hierbij zal de EU Code of Practice on Online Disinformation – het belangrijkste voorbeeld van zelfregulerende maatregelen in Europa – worden geanalyseerd. Voorts zal er kritisch worden gekeken naar het toekomstperspectief van zelfregulerende maatregelen op Europees niveau. Hierbij zal de Guidance on Strengthening the Code of Practice worden besproken en vervolgens zal de Digital Services Act – het recentelijk gepubliceerde voorstel van de Europese Commissie – worden geanalyseerd. Ook zal er kritisch worden gekeken naar de relevantie van de Nederlandse Gedragscode Transparantie Online Politieke Advertenties, die tot doel heeft de transparantie rondom politieke advertenties te vergroten.[[132]](#footnote-132) Er zal worden afgesloten met een tussenconclusie.

## **5.1 Regelgevende initiatieven in Europa**

Uit hoofdstuk 3 is gebleken dat sociale mediakanalen in de loop der jaren een steeds grotere rol zijn gaan spelen in de informatievoorziening binnen de samenleving. Bovendien worden dergelijke platforms in toenemende mate door politici aangewend om potentiële kiezers te bereiken. Dit roept logischerwijs de vraag op hoe Europa het beste om kan gaan met de regulering van sociale mediaplatforms en de desinformatie die daarop wordt verspreid, alsmede de gepersonaliseerde politieke advertenties die daarop worden getoond.

De opvatting dat sociale mediaplatforms verantwoordelijk zijn voor de bestrijding van online desinformatie heeft ertoe geleid dat enkele Europese landen nationale regelgeving hebben geïnitieerd. Zo heeft Frankrijk specifieke wetgeving omtrent (het tegengaan) van desinformatie ontwikkeld. Hierin is onder andere bepaald dat een rechtbank een online platform de opdracht kan geven om onjuiste misleidende beschuldigingen die opzettelijk, geautomatiseerd of kunstmatig op grote schaal worden verspreid te verwijderen.[[133]](#footnote-133) Ter verduidelijking van deze bepaling heeft het Hof van Justitie bepaald dat het om gesponsorde inhoud moet gaan. Dat betekent dat het om inhoud moet gaan die gepromoot wordt middels geautomatiseerde instrumenten (zoals bots), of dat betalingen van derden plaatsvinden om meer informatie kunstmatig te verspreiden. [[134]](#footnote-134)

Ook Duitsland heeft uiteindelijk een wet ingevoerd waarin regels worden gegeven waarmee handhaving door sociale mediaplatforms wordt bewerkstelligd. [[135]](#footnote-135) Das Netzwerkdurchsetzungsgesetz (hierna: NetzDG) [[136]](#footnote-136) verplicht sociale mediaplatforms om – binnen 24 uur na het ontvangen van een melding – evident illegale content te blokkeren of zelfs te verwijderen. [[137]](#footnote-137) Voor content die niet direct als illegaal kan worden bestempeld wordt een termijn van zeven dagen aangehouden. Wanneer het afhankelijk van feitelijke omstandigheden is of content als illegaal kan worden aangemerkt, geldt een langere termijn. [[138]](#footnote-138) Wanneer sociale mediaplatforms de regels niet naleven kunnen zij een flinke boete riskeren die kan oplopen tot 5 miljoen euro. [[139]](#footnote-139) Het is – met het oog op de potentiële gevaren die de verspreiding van online desinformatie met zich mee kan brengen en de rol van online platforms hierin – begrijpelijk dat er regelgeving op nationaal niveau wordt ontwikkeld waarin sociale mediaplatforms verantwoordelijk worden gehouden.

Toch strekken dergelijke ontwikkelingen niet tot aanbeveling. Dergelijke ontwikkelingen kunnen namelijk strijdigheid opleveren met het recht op de vrijheid van meningsuiting. De vage termen die worden gebruikt en de hoge sancties die tegenover niet-naleving van de regelgeving staan hebben tot gevolg dat sociale mediakanalen in geval van twijfel ook content zullen blokkeren of zelfs verwijderen die achteraf niet illegaal blijkt te zijn. Dit komt de vrije meningsuiting niet ten goede. [[140]](#footnote-140)

Daarnaast is het problematisch dat private partijen als sociale mediaplatforms de bevoegdheid wordt gegeven om de toelaatbaarheid van content te beoordelen. [[141]](#footnote-141) Niet alleen ontbreekt hierbij een rechterlijke controle, maar ook worden gebruikers doorgaans niet in de gelegenheid gesteld om beroep in te stellen tegen het verwijderen van hun content door sociale mediakanalen. Verder is regelgeving omtrent online desinformatie en de regulering van sociale mediakanalen op nationaal niveau veelal inadequaat ten aanzien van het grensoverschrijdende bereik van het internet. Bovendien is het voor de nationale overheid lastig om controle uit te oefenen op digitale gemeenschappen. [[142]](#footnote-142)

## **5.2 Zelfregulerende maatregelen**

In hoofdstuk 3 is de steeds belangrijkere rol besproken die online platforms zijn gaan spelen in de online informatievoorziening. Ook spelen online platforms een steeds grotere rol met betrekking tot digitale verkiezingscampagnes, doordat politici veelvuldig gebruik maken van deze platforms om campagne te voeren. Gezien hun rol worden zij dan ook veelal geacht zich in te spannen ter bescherming van de potentiële gevaren van online desinformatie. [[143]](#footnote-143)

Uit paragraaf 5.1 blijkt dat wetgeving omtrent online desinformatie op nationaal niveau strijdigheid kan opleveren met het recht op vrijheid van meningsuiting. De Europese Commissie ziet het opstellen van wetgeving op Europees niveau als een soort ‘ultimum remedium’: het zou een mogelijkheid kunnen zijn in het geval dat andere maatregelen ontoereikend blijken, maar het geniet niet de voorkeur. [[144]](#footnote-144) Een andere reden waarom wetgeving niet altijd geschikt is in de strijd tegen desinformatie is dat reeds bestaande wetgeving – ontworpen voor de offline omgeving – vaak moeilijk toepasbaar is op de huidige online omgeving die zich kenmerkt door het dynamische karakter. Het opstellen van nieuwe wetgeving, daarentegen, kost relatief veel tijd en heeft bovendien niet het flexibele karakter dat nodig is voor de dynamiek van de online omgeving. [[145]](#footnote-145) Daarnaast maakt het globale karakter van het internet in combinatie met de geringe expertise van overheden en de gedecentraliseerde technische omgeving het moeilijk voor (nationale) overheden om regulering van de online omgeving te bewerkstelligen. [[146]](#footnote-146)

Waar wetgeving niet de beste oplossing blijkt te zijn in de strijd tegen online desinformatie, lijkt zelfregulering een uitweg te bieden. Zelfregulering is een privaatrechtelijk verschijnsel dat uit niet-statelijke regels bestaat. De regulerende partij is tegelijkertijd de partij die gereguleerd wordt. [[147]](#footnote-147) Naast de relatief lage kosten en de snelheid waarmee zelfregulering – in vergelijking tot het opstellen van nieuwe wetgeving – tot stand komt, kent zelfregulering ook een flexibel karakter. Bovendien is de nodige expertise aanwezig bij de regulerende sector en omdat de regels op de waarden van de desbetreffende sector zijn afgestemd kan dit leiden tot een grote(re) bereidheid om de regels daadwerkelijk na te leven. [[148]](#footnote-148)

Naast hierboven genoemde voordelen kent zelfregulering echter ook nadelen. [[149]](#footnote-149) Zo kan de eerdergenoemde flexibiliteit tot rechtsonzekerheid leiden. Regels kunnen immers relatief makkelijk worden aangepast. Bovendien bestaat het risico dat niet het publieke belang, maar het eigen belang van de sector wordt nagestreefd. Ook kan zelfregulering slechts beperkt worden afgedwongen en ontbreekt de democratische legitimiteit, nu online platforms zelf de regulerende partij worden.

## **5.3 Zelfregulering in de praktijk: effectief en proportioneel?**

In 2018 heeft de Europese Commissie – naar aanleiding van het voorstel van de HLEG [[150]](#footnote-150) – de EU Code of Practice on Online Disinformation (hierna: Code) aangenomen. Dit is een belangrijk voorbeeld van zelfregulerende maatregelen op Europees niveau, waarin online platforms zich op vrijwillige basis verbinden om online desinformatie te bestrijden. Hoewel het hier in beginsel om het aangaan van een vrijwillige verbintenis gaat, komt er mogelijk wel een politieke druk bij kijken. Het doel van de Code is om ondertekenende partijen actief te laten bijdragen aan het tegengaan van de verspreiding van online desinformatie. Tegelijkertijd dient het recht op vrije meningsuiting en een vrij toegankelijk internet te worden gewaarborgd. [[151]](#footnote-151)

Ondertekenende partijen zouden de implementatie, de voortgang en het functioneren omtrent de Code twaalf maanden na ondertekening evalueren en rapporten. [[152]](#footnote-152) Inmiddels zijn de meeste maatregelen onafhankelijk geëvalueerd. Uit de evaluaties blijkt in ieder geval dat het bestaan van de Code of Practice een stap in de goede richting is in de gezamenlijke bestrijding van online desinformatie. Toch worden er een aantal verbeterpunten voorgesteld om effectiviteit [[153]](#footnote-153) van de Code te garanderen.

Allereerst zouden verbeteringen met betrekking tot de terminologie en interpretatie op hun plaats zijn. Om de verspreiding van desinformatie daadwerkelijk tegen te kunnen gaan, zou er onder de partijen consensus moeten bestaan over wat er nu precies onder desinformatie wordt verstaan. Het feit dat er geen eenduidige (juridische) definitie is kan ertoe leiden dat het lastig is om onoprecht gedrag of een onbetrouwbare informatiebron te detecteren. De Europese Commissie zou hierin een leidende rol moeten aannemen om de discussie en organisatie omtrent dit onderwerp onder het grote aantal partijen te faciliteren en te bevorderen. [[154]](#footnote-154)

Ten tweede is er geen instantie die tegen niet-naleving van de partijen optreedt. Het (jaarlijkse) evaluatieproces kan als zelfrapportering worden aangemerkt, nu de beoordeling weliswaar door een derde partij geschiedt, maar deze partij door de platforms zelf wordt aangesteld. [[155]](#footnote-155) Het aanstellen van een daadwerkelijke onafhankelijke instantie die tegen eventuele niet-naleving van de partijen optreedt en mogelijke implicaties omtrent de vrijheid van meningsuiting behandelt zou hier een uitkomst voor kunnen bieden. [[156]](#footnote-156)

De Code kent op dit moment nog een ‘a la carte’ benadering, waarbij de ondertekenende partijen ervoor kunnen kiezen om zich tot bepaalde verplichtingen van de Code te verbinden, en andere verplichtingen naast zich neer te leggen. Om partijen te stimuleren zich tot meer verplichtingen te verbinden, zou het stimuleren van innovatieve inbrengen mogelijkerwijs een oplossing kunnen bieden. Deze benadering zou ook aan andere platforms – die de Code niet ondertekend hebben – kunnen worden gericht. Door hen de mogelijkheid te bieden om verplichtingen voor te stellen die bij hun eigen businessmodel aansluiten, zouden zij gestimuleerd worden om zich ook aan de Code te verbinden. [[157]](#footnote-157)

Wat de proportionaliteit betreft dient er sprake te zijn van eerbiediging van het recht op vrijheid van meningsuiting en het daarmee samenhangende recht op informatie. [[158]](#footnote-158)

Uit hoofdstuk 2 is gebleken dat online desinformatie geen illegale content behelst, maar dat het gaat om content die – vanuit maatschappelijk oogpunt – slechts onwenselijk is. Dit leidt tot de vraag of desinformatie zomaar mag worden verwijderd door online platforms.

Ter illustratie het volgende voorbeeld: in 2020 heeft de voorzieningenrechter zich in een kort geding tegen respectievelijk YouTube en Facebook over deze vraag gebogen. In beide gevallen merkte de voorzieningenrechter op dat online platforms afspraken omtrent desinformatie met de Europese Commissie hebben gemaakt. Nu de Europese Commissie online platforms heeft verzocht om desinformatie met betrekking tot Covid-19 tegen te gaan, mochten zowel YouTube als Facebook hieraan gerelateerde desinformatie verwijderen. [[159]](#footnote-159)

Dat er door de voorzieningenrechter wordt geoordeeld dat desinformatie omtrent Covid-19 – op verzoek van de Europese Commissie – mag worden verwijderd, is opmerkelijk. Hoewel de Code uiteindelijk tot doel heeft om desinformatie tegen te gaan, is afgesproken dat online platforms niet zonder meer mogen worden gevraagd om informatie die onjuist is te verwijderen. Ook worden platforms ontmoedigd om zelf dergelijk beleid uit te voeren. Volgens de Code zouden platforms, zoals YouTube en Facebook, desinformatie in eerste instantie tegen moeten gaan door bijvoorbeeld voor meer transparantie te zorgen en ‘factchecking’ mogelijk te maken. [[160]](#footnote-160) Bovendien mogen internetbedrijven, zoals terecht door de voorzieningenrechter in het kort geding tegen Facebook is opgemerkt, in beginsel zelf beslissen wat zij wel of niet op hun platforms toestaan. Het verwijderen van desinformatie door online platforms berust – zolang het niet als onrechtmatig of illegaal kan worden gekwalificeerd – niet op een juridische plicht. De Code verplicht platforms dus niet om desinformatie – wanneer het slechts om valse beweringen gaat – te verwijderen. Er mogen slechts passende maatregelen door de Staat worden getroffen op het moment dat de dominantie van machtige platforms de effectieve uitoefening van het recht op vrije meningsuiting belemmert. [[161]](#footnote-161)

## **5.4 Versterking van de Code en toekomstperspectief**

De bedreigingen die gepaard gaan met de verspreiding van online desinformatie ontwikkelen zich relatief snel. Met name de ontwikkelingen omtrent het coronavirus – dat bovendien een belangrijk onderwerp van discussie is geweest in de afgelopen (digitale) verkiezingscampagnes in Nederland[[162]](#footnote-162) – hebben de gevaren en uitdagingen die de strijd tegen desinformatie met zich brengt nog eens benadrukt. Ondanks de maatregelen die tot op heden zijn genomen, blijft de urgentie bestaan om de verspreiding van (online) desinformatie te bestrijden. [[163]](#footnote-163) Het waarborgen van het recht op vrije meningsuiting en de deelname aan een vrij en toegankelijk maatschappelijk debat blijft hierbij van cruciaal belang.

Op 26 mei 2021 heeft de Europese Commissie dan ook de Guidance on Strengthening the Code of Practice on Disinformation [[164]](#footnote-164) (hierna: Guidance) gepubliceerd. De Guidance is bedoeld om de positie van de Code of Practice on Disinformation – naar aanleiding van evaluaties omtrent de tekortkomingen ervan – te versterken en de Code tot een effectiever middel in het tegengaan van desinformatie te maken. In de Guidance wordt onder andere een oproep gedaan voor meer betrokkenheid van de ondertekenende partijen. Zo zouden ondertekenende partijen desinformatie financieel minder aantrekkelijk moeten maken, gebruikers moeten versterken in het aannemen van een actieve rol om de verspreiding van desinformatie te voorkomen, beter moeten samenwerken met fact-checkers in verschillende EU-lidstaten en onderzoekers een kader moeten bieden waarbinnen zij toegang tot data hebben. [[165]](#footnote-165)

Met de versterking van de Code op de bovengenoemde gebieden worden de tekortkomingen die uit de eerste jaarlijkse evaluaties zijn gebleken voor een wezenlijk deel weggenomen. Gezien het feit dat de Guidance zeer recentelijk is gepubliceerd, blijft het onduidelijk in welke mate de beoogde verbeteringen daadwerkelijk tot versterking van de Code zullen leiden. Bovendien zijn niet alle verbeterpunten meegenomen. Zo wordt het bereiken van meer consensus omtrent de definitie van desinformatie vrijwel geheel buiten beschouwing gelaten. Ook het bevorderen van de legitimiteit van de Code, door ondertekening van de Code aantrekkelijker te maken voor andere partijen dan online platforms – zoals grote adverteerders – blijft buiten beschouwing.

## **5.5 De Digital Services Act**

In het verlengde van de vorige paragraaf, waarin de toekomst van de zelfregulerende maatregelen centraal stond, zal in deze paragraaf kritisch worden gekeken naar een voorstel dat potentieel toekomstige regels bevat omtrent online platforms.

De Europese Commissie heeft op 15 december 2020 twee voorstellen gepubliceerd voor nieuwe verordeningen betreffende het reguleren van digitale diensten binnen de Europese Unie. Het gaat om de ‘Digital Services Act’ en de ‘Digital Markets Act’, die tot doel hebben een veiligere online omgeving te creëren waarbinnen bescherming van de fundamentele rechten van de gebruikers van digitale diensten centraal staat en innovatie, concurrentiekracht en groei op zowel Europees als mondiaal niveau worden bevorderd. [[166]](#footnote-166) In deze paragraaf wordt – omwille van de omvang en de reikwijdte van deze scriptie – alleen de Digital Services Act (hierna: DSA) besproken. Van belang om hierbij op te merken is dat de DSA op dit moment slechts een voorstel is en dus nog aan verandering onderhevig kan zijn.

De aanleiding voor de DSA wordt gevormd door de opkomst van innovatieve en nieuwe diensten – zoals sociale mediakanalen – en de invloed die deze diensten in toenemende mate op het dagelijks leven hebben. De DSA legt de focus op de regulering van diverse online tussenpersonen. Hierbij wordt onderscheid gemaakt tussen zeer grote onlineplatforms en simpele doorgiftediensten. Vanwege dit onderscheid is er dan ook sprake van verschillende niveaus van regulering. [[167]](#footnote-167)

De verplichtingen die in de DSA zijn opgenomen zijn gericht tot aanbieders van ‘intermediary services’ (tussenhandelsdiensten[[168]](#footnote-168)). De DSA maakt een onderscheid tussen verschillende categorieën van tussenhandelsdiensten, waarbij voor iedere categorie een eigen set aan regels geldt. [[169]](#footnote-169) Zo gelden voor de ‘mere conduit’ diensten[[170]](#footnote-170) de lichtste verplichtingen en de zwaarste verplichtingen gelden voor de ‘very large online platforms (VLOPs)’.[[171]](#footnote-171)

De aansprakelijkheidsregeling van de e-Commercerichtlijn is in hoofdstuk II van de DSA herzien. In de DSA zijn – anders dan in de e-Commercerichtlijn – definities opgenomen van de verschillende tussenhandelsdiensten. [[172]](#footnote-172)

Hostingdiensten[[173]](#footnote-173) hebben in de DSA[[174]](#footnote-174) – net als in de e-Commercerichtlijn[[175]](#footnote-175) – een relatief grote verantwoordelijkheid. Hostingdiensten zijn vrijgesteld van aansprakelijkheid voor informatie van derden die zij opslaan en doorgeven. [[176]](#footnote-176) Deze vrijstelling is van toepassing in de gevallen dat de dienstverlener geen kennis heeft van de illegale inhoud of onwettige activiteit. Mocht de dienstverlener kennis verkrijgen van het illegale of onwettige karakter, dan dient de dienstverlener prompt te handelen om de inhoud weg te halen of de toegang daartoe te blokkeren. Hierbij is wel van belang dat het recht op vrije meningsuiting gewaarborgd blijft. Deze verantwoordelijkheid die aan de dienstverlener toekomt brengt dus een duidelijk spanningsveld met zich mee. [[177]](#footnote-177) Er staan namelijk twee belangen tegenover elkaar: enerzijds het belang dat er geen onrechtmatige inhoud wordt gepubliceerd en anderzijds het belang van de uitingsvrijheid en de vrijheid om bepaalde misstanden te bekritiseren. Hoewel de belangen tegen elkaar moeten worden afgewogen om tot een beoordeling te komen van de vraag of een bepaalde publicatie onrechtmatig is, staan deze niet in hiërarchische verhouding tot elkaar. Het hangt dus af van de omstandigheden van het geval welk belang het zwaarst weegt. [[178]](#footnote-178)

Een actueel voorbeeld van een dergelijk spanningsveld is het huidige corona- en vaccinatiebeleid – en de daarbij horende complottheorieën [[179]](#footnote-179) – dat bovendien een belangrijk onderwerp was tijdens de afgelopen (digitale) verkiezingscampagnes in Nederland. Zowel onder burgers als onder politici heersen verschillende opvattingen over dit beleid. [[180]](#footnote-180) Zo tweette FvD-lijsttrekker Thierry Baudet onlangs dat hij zich niet zal laten vaccineren tegen het coronavirus, vanwege het verwaarloosbare risico van het virus, de ernstige bijwerkingen en het onduidelijke effect op de lange termijn van de vaccinatie op het immuunsysteem. [[181]](#footnote-181)

Twitter stelt tijdens verkiezingen samen te werken met experts, onderzoekers en politieke partijen om ervoor te zorgen dat eventuele misleidende berichten op de juiste wijze worden gerapporteerd. Waar misleidende inhoud van gebruikers doorgaans van Twitter wordt verwijderd, maakt het platform voor politici een uitzondering. Het bedrijf wil namelijk wel ingrijpen bij berichten die een misleidend karakter hebben, maar wil politici tegelijkertijd niet het zwijgen opleggen. Zo werd bovenstaande tweet van Baudet niet verwijderd, maar wel germarkeerd als ‘misleidend’. [[182]](#footnote-182) Het promoten van terrorisme of dreigen met geweld door politici vormt echter wel een aanleiding voor het platform om berichten te verwijderen. Dat gebeurde bijvoorbeeld begin 2021, toen de voormalige Amerikaanse president Donald Trump geschorst werd vanwege zijn tweets rond de bestorming van het Capitool. [[183]](#footnote-183) Het verschil tussen de tweet van Trump en de tweet van Baudet is dat Trump – anders dan Baudet – met zijn tweet aanzette tot geweld. Baudet werd dan ook niet geschorst. Het markeren van zijn berichten als misleidend heeft tot doel om andere gebruikers te waarschuwen en het verspreiden van dergelijke informatie te bemoeilijken. [[184]](#footnote-184)

## **5.6 Nederlandse Gedragscode Transparantie Online Politieke Advertenties**

Ook op nationaal gebied zijn maatregelen getroffen om digitale verkiezingscampagnes te beschermen tegen de gevaren van online desinformatie en microtargeting.

De Nederlandse Gedragscode Transparantie Online Politieke Advertenties[[185]](#footnote-185) (hierna: Gedragscode) werd begin februari 2021 gepubliceerd, met als doel desinformatie in de aanloop naar de Tweede Kamerverkiezingen in Nederland tegen te gaan. De Gedragscode volgt op een eerdere motie van de Kamerleden Middendorp (VVD) en Kuiken (PvdA)[[186]](#footnote-186), waarin zij meer toegankelijkheid omtrent politieke advertenties wilden realiseren, en op eerdere initiatieven van de Europese Commissie, zoals de hierboven besproken EU Code of Practice on Disinformation. [[187]](#footnote-187)

Anders dan de Code of Practice is de Gedragscode ook door politieke partijen ondertekend. De Gedragscode bouwt voor een groot deel voort op de Code of Practice, maar behelst daarnaast ook randvoorwaarden met betrekking tot het plaatsen van (gepersonaliseerde) politieke advertenties op sociale mediakanalen. Hoewel de Gedragscode – anders dan de Code of Practice – richtlijnen omtrent de kwalificatie van desinformatie vrijwel volledig buiten beschouwing laat, worden online platforms wel geacht om informatie omtrent de verkiezingsprocedure die als onjuist is aangemerkt ‘tegen te gaan’. Een concrete invulling van wat er in dit geval precies onder tegengaan wordt verstaan ontbreekt. Onduidelijk is dus of hiermee het verwijderen van berichten, het blokkeren van een gebruiker of slechts het aanmerken dat het om onjuiste informatie gaat wordt bedoeld. In overeenstemming met de Code of Practice zou laatstgenoemde manier de meest voor de hand liggende invulling van ‘tegengaan’ zijn. Zoals besproken in paragraaf 5.3 dienen platforms namelijk terughoudend om te gaan met het verwijderen van informatie die onjuist is. Zolang er geen sprake is van een illegaal karakter kan het verwijderen van (onjuiste) informatie immers strijdigheid met het recht op de vrije meningsuiting opleveren, terwijl dit recht juist dient te worden gewaarborgd. [[188]](#footnote-188) Ook uitingen die onwaar zijn worden in beginsel namelijk door de vrijheid van meningsuiting beschermd. Met name in de context van het publieke debat zou het voor burgers een zware opgave zijn om de juistheid van beweringen volledig na te trekken voordat deze kunnen worden geuit. Op politici berust echter – bezien vanuit hun hoedanigheid – de verantwoordelijkheid om juiste informatie met betrekking tot het verkiezingsproces te verschaffen. [[189]](#footnote-189) De Gedragscode vraagt politici dan ook zich te onthouden van gedrag dat onethisch is, het bewust plaatsen, aanbevelen of verspreiden van inhoud die misleidend is en het plaatsen, aanbevelen of verspreiden van inhoud die aanzet tot geweld of haatzaait. [[190]](#footnote-190)

Een ander opvallend punt aan de Gedragscode is het niet bindende karakter ervan. De Gedragscode is vrijblijvend en – ondanks het feit dat ondertekenende partijen zich aan de plichten committeren – dus niet afdwingbaar. Dit is opmerkelijk, nu het ontbreken van consequenties bij niet-naleving van de Code of Practice door ondertekenende partijen één van de kritiekpunten is die – mede door minister Ollongren (die de Gedragscode liet opstellen) – op de Code of Practice werd geuit. [[191]](#footnote-191)

De meerwaarde van de Gedragscode – ten opzichte van de Code of Practice – is gelegen in het feit dat de Gedragscode beter kan worden toegespitst op de Nederlandse (verkiezings)context. Bovendien worden politieke partijen en online platforms bij elkaar gebracht. Ondanks dat er geen daadwerkelijke rechtsgrond is om naleving af te dwingen, kunnen politieke partijen en online platforms elkaar bij niet-naleving publiekelijk aanspreken. Dit kan bevorderend werken voor de vrijwillige naleving van de Gedragscode. [[192]](#footnote-192)

**Tussenconclusie**Hoewel er in Europa reeds enkele wetgevingsinitiatieven bestaan, verdienen zelfregulerende maatregelen de voorkeur ten opzichte van regelgevende maatregelen. Het belangrijkste voorbeeld van zelfregulerende maatregelen, namelijk de EU Code of Practice on Disinformation, is hierbij een stap in de goede richting. Toch blijken er – naar aanleiding van de eerste jaarlijkse evaluaties – verbeterpunten mogelijk. Een aantal van deze verbeterpunten zijn opgenomen in de Guidance on Strengthening de EU Code of Practice on Disinformation. Een belangrijk verbeterpunt dat hierin ontbreekt is het bereiken van meer consensus onder ondertekenende partijen omtrent de definitie van desinformatie.

De Digital Services Act – dat vooralsnog slechts een voorstel is en dus nog aan verandering onderhevig kan zijn – categoriseert tussenhandelsdiensten op basis van grootte, waarbij voor elke categorie een eigen set aan regels is opgenomen. Aan hostingdiensten wordt een relatief grote verantwoordelijkheid toegekend om illegale inhoud of onwettige activiteiten tegen te gaan, maar bescherming van de vrije meningsuiting blijft hierbij van fundamenteel belang.

De Nederlandse Gedragscode Transparantie Online Politieke Advertenties verbindt – anders dan de Code – niet alleen online platforms, maar ook politieke partijen. Een voordeel van de Gedragscode ten opzichte van de Code of Practice is dat deze beter toegespitst is op de Nederlandse politieke context. Wel is van belang dat individuen – voor de effectieve uitoefening van het recht op vrije meningsuiting – actief kunnen deelnemen aan het publieke debat. Het is daarom belangrijk dat er steeds voor het lichtste middel wordt gekozen om misleidende of onware informatie tegen te gaan. [[193]](#footnote-193)

# Conclusie

Uit het voorgaande kan worden geconcludeerd dat desinformatie een vorm van onware en misleidende informatie is. Achter dit begrip schuilen bovendien andere categorieën uitingen die – tijdens digitale verkiezingscampagnes – impact kunnen hebben op de meningsvorming van individuen. Microtargeting is het omzetten van digitale sporen in bruikbare informatie om toekomstig gedrag van potentiële kiezers te voorspellen. Net als de verspreiding van online desinformatie kan microtargeting tot beïnvloeding van het publieke debat leiden. Er zou zelfs voorzichtig kunnen worden geconcludeerd dat microtargeting tot versterking van de manipulerende werking van online desinformatie zou kunnen leiden. Beide fenomenen hebben zich de afgelopen jaren dan ook relatief snel ontwikkeld tot een krachtig instrument om de publieke opinie en verkiezingsuitslagen te manipuleren. Toch bestaat er ook een positieve kant aan de ontwikkeling van deze fenomenen. Zo kan microtargeting voor meer maatschappelijke betrokkenheid zorgen, nu deelname aan het publieke debat voor bepaalde groepen toegankelijker wordt gemaakt. Bovendien vindt verwezenlijking van de negatieve gevolgen van microtargeting niet snel plaats in Nederland, nu Nederland een meerpartijenstelsel kent, gebonden is aan de relatief strenge Europese regels omtrent privacybescherming en transparantie, en burgers ook toegang hebben tot andere informatiebronnen.

Aan de staat komt de verplichting toe om een pluralistisch informatieaanbod te garanderen, maar de effectieve uitoefening van het recht op vrije meningsuiting mag hier niet door worden geraakt. Online platforms spelen een steeds belangrijkere rol in zowel de verspreiding van online desinformatie als de inzet van microtargeting en komen daardoor steeds meer onder druk te staan. Er wordt van online platforms verwacht dat zij zich aan de verplichtingen houden die hen op grond van de AVG toekomen. De toenemende druk op en verantwoordelijkheid van online platforms heeft bovendien tot regelgevende initiatieven in enkele Europese lidstaten geleid. Hoewel dergelijke wetgeving in Nederland (nog) niet aan de orde is, ligt de voorkeur niet bij het ontwikkelen van meer (nationale) regelgeving, maar bij het versterken van de positie van de reeds bestaande zelfregulerende maatregelen.

De in 2018 opgestelde EU Code of Practice on Disinformation is het belangrijkste voorbeeld van zelfregulerende maatregelen op Europees niveau. Om de effectiviteit en proportionaliteit te versterken zijn er – naar aanleiding van jaarlijkse evaluaties – in de recentelijk gepubliceerde Guidance verbeterpunten opgesteld. Het effect van deze verbeterpunten op de effectiviteit van de Code of Practice moet uit de praktijk nog blijken. Opmerkelijk is wel dat het bereiken van meer consensus omtrent de definitie van desinformatie onder de ondertekenende partijen niet als verbeterpunt is opgenomen in de Guidance.

Recentelijk is ook de Digital Services Act – dat momenteel nog een voorstel is en dus aan verandering onderheving kan zijn – gepubliceerd. In het huidige voorstel staat modernisering van de regels omtrent online platforms centraal, zodat deze in het huidige digitale tijdperk passen. In het voorstel worden tussenhandelsdiensten op basis van grootte gecategoriseerd, waarbij iedere categorie met een eigen set aan regels te maken heeft. Wel blijft ook hier bescherming van de vrijheid van meningsuiting van cruciaal belang.

Voorts is op nationaal niveau een Gedragscode opgesteld om meer transparantie omtrent (gepersonaliseerde) online politieke advertenties te garanderen. Ondanks kritiek op het niet-afdwingbare karakter van de Code of Practice, verbindt de Nederlandse Gedragscode ondertekenende partijen op vrijwillige, en dus (vooralsnog) niet afdwingbare, basis. De Gedragscode voegt – ten opzichte van de Code of Practice – wel iets toe in het kader van Nederlandse digitale verkiezingscampagnes: de Gedragscode is namelijk beter op de Nederlandse politieke context toegespitst.

Uit dit onderzoek kunnen een aantal verbeteringen en aanbevelingen worden gedestilleerd omtrent de reeds bestaande maatregelen tegen online desinformatie en microtargeting. Aanvullende regelgeving op Europees dan wel nationaal niveau is niet wenselijk, nu desinformatie een complex begrip is dat moeilijk juridisch af te bakenen is. Een grote zorg is dat de complexiteit en de veranderlijkheid van de fenomenen zich niet leent voor regelgeving in de vorm van wetten op Europees dan wel nationaal niveau. Zelfregulering verdient dan ook de voorkeur.

Zoals blijkt uit de recentelijk gepubliceerde Guidance – die tot doel heeft de Code of Practice te versterken – is het van cruciaal belang dat de betrokken partijen blijven samenwerken, dat er evaluaties blijven plaatsvinden en dat er verder onderzoek blijft worden gedaan in de strijd tegen de relatief snelle ontwikkeling van online desinformatie en microtargeting en de verwezenlijking van de daarbij horende gevaren. Ook strekt het tot aanbeveling om regelmatig empirisch onderzoek uit te voeren (bijvoorbeeld door het afnemen van interviews met burgers of een publieke opiniepeiling) om zo meer inzicht te verkrijgen in de mate waarin de maatschappij zich daadwerkelijk bewust is van de gevaren van de manipulatiefenomenen en zo nodig meer bewustwording te creëren.

Het is bovendien raadzaam om het niet-afdwingbare karakter van de huidige (zelfregulerende) maatregelen aan de kaak te stellen. Nu de negatieve gevolgen van de verspreiding van online desinformatie en de inzet van microtargeting in potentie een groot gevaar voor de integriteit van digitale verkiezingscampagnes – en daarmee de kern van de democratie – kunnen opleveren en er geen duidelijke algemene wet op Europees dan wel nationaal niveau bestaat, is het van belang dat bepalingen uit bijvoorbeeld de Code of Practice of de Gedragscode een afdwingbaar karakter krijgen voor ondertekenende partijen.

Tot slot sluit ik mij aan bij de aanbeveling uit het rapport voor het ministerie van Binnenlandse Zaken en Koninkrijksrelaties dat door het Instituut voor Informatierecht (IViR) is gepubliceerd. Het waarborgen van pluralisme is in het kader van online desinformatie en de regulering van microtargeting van cruciaal belang. Uit artikel 10 EVRM vloeit – op basis van het leerstuk van positieve verplichtingen – voort dat structurele maatregelen moeten worden getroffen in het kader van de promotie van pluralisme van het medialandschap. Denk bijvoorbeeld aan beperkingen die op (gepersonaliseerde) politieke advertenties kunnen worden gelegd en het reguleren van massamediale aspecten van social mediaplatforms. Met name transparantie is hierbij van groot belang. Verder onderzoek naar de vraag welke maatregelen in potentie het meest nodig en geschikt zijn voor het tegengaan van de verspreiding van (online) desinformatie via internetplatforms is noodzakelijk. Denk hierbij aan het versterken van de informatiepositie van nationale overheden, het investeren in handhavingsmogelijkheden, en het in kaart brengen van de informatiebehoeftes van verschillende actoren binnen de maatschappij om de transparantie beter te reguleren. [[194]](#footnote-194)

# Literatuur- en jurisprudentielijst

Europese jurisprudentie  
**Hof van Justitie van de Europese Unie**HvJ EU 24 november 2011, C-70/10, ECLI:EU:C:2011:771 (Scarlet Extended/SABAM)

HvJ EU 12 februari 2012, C-360/10, ECLI:EU:C:2012:85 (SABAM/Netlog)

**Europees Hof voor de Rechten van de Mens**EHRM 7 december 1976, nr. 5493/72, ECLI:CE:ECHR:1976:1207JUD000549372 (Handyside/Verenigd Koninkrijk)

EHRM 25 april 1978, nr. 5856/72, ECLI:CE:ECHR:1978:0425JUD000585672 (Tyrer/Verenigd Koninkrijk).

EHRM 26 april 1979, nr. 6538/74, ECLI:CE:ECHR:**1979**:0426JUD000653874 (Sunday Times/Verenigd Koninkrijk).

EHRM 9 oktober 1979, nr. 6289/73, ECLI:CE:ECHR:1979:1009JUD000628973 (Airey/Ierland)

EHRM 26 maart 1985, nr. 8978/80 ECLI:CE:ECHR:1985:0326JUD000897880 (X en Y/Nederland).

EHRM 8 juli 1986, nr. 9815/82, ECLI:CE:ECHR:1986:0708JUD000981582 (Lingens/Oostenrijk)

EHRM 24 november 1993, nr. 13914/88, ECLI:CE:ECHR:1993:1124JUD001391488 (Informationsverein Lentia e.a./Oostenrijk)

EHRM 19 februari 1998, nr. 24839/94, ECLI:CE:ECHR:1998:0219JUD002483994 (Bowman/Verenigd Koninkrijk).

EHRM 16 maart 2000, nr. 23144/93, ECLI:CE:ECHR:2000:0316JUD002314493 (Ozgür Gündem/Turkije).

EHRM 15 februari 2005, nr. 68416/0, ECLI:CE:ECHR:2005:0215JUD006841601 (Steel en Morris/Verenigd Koninkrijk).

EHRM 2 december 2008, nr. 2872/02, ECLI:CE:ECHR:2008:1202JUD000287202 (K.U./Finland)

EHRM 14 april 2009, nr. 37374/05, ECLI:CE:ECHR:2009:0414JUD003737405 (Társaság a Szabadságjogokért/Hongarije).

EHRM 14 september 2010, nr. 2668/07, ECLI:CE:ECHR:2010:0914JUD000266807 (Dink/Turkije).

EHRM 12 september 2011, nr. 28955/06, ECLI:CE:ECHR:2011:0912JUD002895506 (Palomo Sánchez e.a./Spanje).

EHRM 28 juni 2012, nrs. 15054/07 en 15066/07, ECLI:CE:ECHR:2012:0628JUD001505407 (Ressiot e.a./Frankrijk).

EHRM 22 april 2013, nr. 48876/08, ECLI:CE:ECHR:2013:0422JUD004887608 (Animal Defenders International/Verenigd Koninkrijk).

EHRM 16 juni 2015, nr. 64569/09, ECLI:CE:ECHR:2015:0616JUD006456909 (Delfi AS/Estland).

EHRM 2 februari 2016, nr. 22947/13, ECLI:CE:ECHR:2016:0202JUD002294713, (Magyar Tartalomszolgáltatók Egyesülete en Index.hu Zrt/Hongarije)

EHRM 29 maart 2016, nr. 56925/08, ECLI:CE:ECHR:2016:0329JUD005692508 (Bédat/Zwitserland).

EHRM 9 maart 2017, nr. 74742/14, ECLI:CE:ECHR:2017:0207DEC007474214 (Pihl/Zweden).

Nationale jurisprudentie  
Rechtbank Amsterdam 9 september 2020, ECLI:NL:RBAMS:2020:4435  
  
Rechtbank Amsterdam 13 oktober 2020, ECLI:NL:RBAMS:2020:4966

Primaire bronnen **Internationale regelgevingEuropees Verdrag voor de Rechten van de Mens**   
Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, Rome, 4 november 1950.

**International Verdrag inzake Burgerrechten en Politieke Rechten**   
Internationaal Verdrag inzake burgerrechten en politieke rechten, New York, 16 december 1966.

**Richtlijn 2000/31/EG**Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (‘Richtlijn inzake elektronische handel’)

**Richtlijn 2010/13/EU**   
Richtlijn 2010/13/EU van het Europees Parlement en de Raad van 10 maart 2010 betreffende coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten.

**Verordening (EU) 2016/679**   
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.

**Richtlijn (EU) 2018/1808**   
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.

**Handvest van de Grondrechten van de Europese Unie**   
Handvest van de Grondrechten van de Europese Unie, 2016/C, 202/02, 7 juni 2016.

**Europese Unie***Communicaties, rapporten en opinies***European Commission, HLEG Report on fake news and online disinformation 2018**   
European Commission, Report of the independent High-Level Expert Group on fake news and online disinformation 2018, A multi-dimensional approach to disinformation, maart 2018.

**EC Communication COM(2018) 236**   
Europese Commissie Communicatie, Tackling online disinformation: a European Approach, COM(2018)236 Final, 26 april 2018

**Sounding Board’s final opinion 2018**   
The Sounding Board’s unanimous final opinion on the so-called Code of Practice, 24 september 2018, <https://ec.europa.eu/digital-single-market/en/news/code-practicedisinformation>.

**EC Communication COM(2020) 790**Europese Commissie Communicatie, On the European democracy action plan, COM(2020)790 Final, 3 december 2020

**EC Communication COM(2020)825**  
Europese Commissie Communicatie, On a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020)825 Final, 15 december 2020

*Overig***European Commission, Factsheet on tackling online disinformation 2018**   
European Commission, Factsheet on tackling online disinformation, 26 april 2018, <https://ec.europa.eu/digital-single-market/en/news/factsheet-tackling-online-disinformation>.

**EU Code of Practice on Disinformation 2018**   
EU Code of Practice on Disinformation, 26 september 2018, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

**Staff Working Document (SWD (2020)180**Staff Working Document SWD (2020)180 Final – Assessment of the Code of Practice on Disinformation <https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement>

**EC Communication COM(2021) 262 final**European Commission, Guidance on Strengthening the Code of Practice on Disinformation, (COM(2021) 262 final), 26 mei 2021

**European Commission, 26 mei 2021**European Commission presents Guidance to strengthen the Code of Practice on Disinformation, Press Release 26 May 2021, <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585>

**Nationaal**

**NetzDG 2017**   
Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)/Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), 1 september 2017, Bundesgesetzblatt, Jahrgang 2017, Teil I, Nr. 61, 7 september 2017 (inwerkingtreding: 1 oktober 2017)

*Kamerstukken en kamerbrieven***Minister Ollongren, brief aan Tweede Kamer** **18 december 2017**   
Minister Ollongren (BZK) brief aan Tweede Kamer over de heimelijke beïnvloeding van de publieke opinie door statelijke actoren.  
 **Kamerstukken II 2020/21, 30821, 118****Kamerstukken II, 2020/2021, 35570-VII, nr. 10**

**Kamerstukken I 2020/21, 35526, AG**

**Minister Ollongren, brief aan Tweede Kamer 16 november 2020**Minister Ollongren (BZK), brief aan de Tweede Kamer over maatregelen om desinformatie richting de Tweede Kamer verkiezingen tegen te gaan.

**Minister Ollongren, brief aan Tweede Kamer 9 februari 2021**   
Minister Ollongren (BZK), brief aan de Tweede Kamer over de voortgang van de maatregelen om desinformatie richting de Tweede Kamerverkiezingen tegen te gaan.

**Minister Slob, brief aan Tweede Kamer 17 december 2019**Minister Slob, brief aan Tweede Kamer over Co- en zelfregulering in de mediasector.

*Overig***Nederlandse Gedragscode Transparantie Online Politieke Advertenties**Nederlandse Gedragscode Transparantie Online Politieke Advertenties, 9 februari 2021, <https://www.rijksoverheid.nl/documenten/richtlijnen/2021/02/09/nederlandse-gedragscode-transparantie-online-politieke-advertenties>.

Secundaire bronnen*Boeken* **Andreotti e.a. 2015**   
O. Andreotti e.a., *Journalism at risk. Threats, challenges and perspectives*, Strasbourg: Council of Europe Publishing 2015.

**Boom e.a. 2009**   
W. Boom, M. Faure, N. Huls en N. Philipsen, *Handelspraktijken, reclame en zelfregulering*, Pilotstudy Maatschappelijke Reguleringsinstrumenten voor het Wetenschappelijk Onderzoeken Documentatiecentrum Ministerie van Justitie (projectnummer 1535), Den Haag: Boom Juridische Uitgevers 2009.

**Hammarberg e.a. 2011**  
T. Hammarberg, D. Mijatović, A. White, A.R. Olsson, M. Haraszti, B. Boev, B. Bukovska, D. Korff, I. Brown, *Human rights and a changing media landscape*, Strasbourg: Council of Europe Publishing 2011.

**Jakubowicz 2011**  
K. Jakubowicz, *Media revolution in Europe: ahead of the curve,* Strasbourg: Council of Europe Publishing 2011.

**De Ridder, Vliegenthart & Zuure 2020**J. de Ridder, R. Vliegenthart, J. Zuure, *Doen, durven of de waarheid? Democratie in digitale tijden*, Amsterdam: Amsterdam University Press 2020.

*Tijdschriftartikelen***Bennett, *International Data Privacy Law* 2016, p. 261-275**C.J. Bennett, ‘Voter databases, micro-targeting and data protection law: can political parties’ campaign in Europe as they do in North America?’, *International Data Privacy Law*, Volume 6, Issue 4, November 2016, p. 261-275

**Broekstra, *Mediaforum* 2015, p. 2-11**   
R. Broekstra, ‘Private communicatiemacht-hebbers en onze uitingsvrijheid’, Mediaforum 2015-I, p. 2-11.

**Couldry, *European Journal of Communication* 2009, p. 437-449**   
N. Couldry, ‘Does ‘the Media’ Have a Future?’, *European Journal of Communication* 2009, Vol 24(4), p. 437-449.

**Dobber, Fathaigh, Zuiderveen Borgesius, *Internet Policy Review* 2019, p. 1-20**T. Dobber, R. Ó Fathaigh, F.J. Zuiderveen Borgesius, ‘The regulation of online political micro-targeting in Europe’, Internet Policy Review 2019, Vol. 8(4), p. 1-20, [DOI: 10.14763/2019.4.1440](https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe)

**Fallis, *Library Trends* 2015, p. 401-426**D. Fallis, ‘What is disinformation?’, *Library Trends* 2015, Vol63(3), p. 401-426

**Geus & Sickinghe, *Mediaforum 2021*, p. 42-50**   
M. Geus en F. Sickinghe, ‘De Digital Services Package als beoogd wereldwijd rolmodel (deel 1 – Digital Services Act)’, *Mediaforum 2021-2*, p. 42-50

**Harrison & Barthel, *New Media & Society* 2009, p. 155-178**  
T.M. Harrison & B. Barthel, ‘Wielding new media in Web 2.0: exploring the history of engagement with the collaborative construction of media products’, *New Media & Society* 2009, Vol 11(1&2), p. 159-160

**Jamieson, *The Forum* 2013, p. 429-435**  
K.H. Jamieson, ‘Messages, Micro-targeting, and New Media Technologies’, *The Forum* 2013, Vol11(3), p. 429-435, [DOI:10.1515/for-2013-0052](https://www.researchgate.net/publication/277392741_Messages_Micro-Targeting_and_New_Media_Technologies)

**Lievens & Voorhoof, *Mediaforum* 2016, p. 182-185**   
E. Lievens en D. Voorhoof, ‘Internet portalen niet aansprakelijk voor de verspreiding van beledigende – maar niet ‘duidelijk onrechtmatige’ – commentaren van gebruikers’, Mediaforum 2016-7, p. 182-185.

**McGonagle en de Boer, *Mediaforum* 2012, p. 338-345**   
T. McGonagle en K. de Boer, ‘A brave new media world revisited: een nog kritischer blik op het nieuwe mediabeleid van de Raad van Europa’, Mediaforum 2012-II/12, p. 338-345.

**McGonagle, *NQHR* 2017, p. 203-209**   
T. McGonagle, ‘‘‘Fake news’’: False fears or real concerns?’, *Netherlands Quarterly of Human Rights* 2017, Vol. 35(4), p. 203-209.

**McGonagle, *Mediaforum* 2018, p. 180-184**   
T. McGonagle, ‘De Raad van Europa en online desinformatie: laveren tussen zorgen en zorgplichten?’, *Mediaforum* 2018-6, p. 180-184.

**Oosterveld & Oostveen, *Mediaforum* 2013, p. 146-153**   
M. Oosterveld en M. Oostveen, ‘Van ‘public watchdog’ naar ‘public watchblog’: het EHRM en journalistieke weblogs’, Mediaforum 2013-6, p. 146-153.

**Plaizier & Klus, *Mediaforum* 2018, p. 190-193**C. Plaizier, M. Klus, ‘Nepnieuws in Nederland: verschijningsvormen en potentiële oplossingen voor dit containerbegrip’, *Mediaforum* 2018, p. 190-193

**Susser, Roessler & Nissenbaum, *Internet Policy Review* 2019, p. 1-22**D. Susser, B. Roessler, H. Nissenbaum, ‘Technology, autonomy and manipulation’, *Internet Policy Review* 2019, Vol8(2), p. 1-22, [DOI: 10.14763/2019.2.1410](https://policyreview.info/articles/analysis/technology-autonomy-and-manipulation)

**Van Til, *Mediaforum 2019*, p. 1-12**G. van Til, ‘Zelfregulering door online platforms: een waar wondermiddel tegen online desinformatie?’, *Mediaforum* 2019, p. 1-12

**Zuiderveen Borgesius, e.a., *Internet Policy Review* 2016, p. 1-16**  
F.J. Zuiderveen Borgesius, D. Trilling, J. Möller, B. Bodó, C.H. de Vreese, & N. Helberger, ‘Should We Worry about Filter Bubbles?’, *Internet Policy Review* 2016, 5(1). <https://doi.org/10.14763/2016.1.401>

**Zuiderveen Borgesius e.a.,*Utrecht Law Review* 2018, p. 82-96**F. J. Zuiderveen Borgesius, J. Möller, S. Kruikemeier, R. Fathaigh, K. Irion, T. Dobber, B. Bodo, C. de Vreese, ‘Online Political Microtargeting: Promises and Threats for Democracy’ *Utrecht Law Review* 2018, Vol 14(1), p. 82-96, [DOI: 10.18352/ulr.420](https://www.utrechtlawreview.org/articles/abstract/10.18352/ulr.420/)

**Zuiderveen Borgesius e.a., *NJB 2019/528*, p. 662-669**F.J. Zuiderveen Borgesius, J. Möller, T. Dobber, S. Kruikemeier, K. Irion, S. Stapel, R. Fathaigh, B. Bodo, C. de Vreese, ‘Online politieke microtargeting: een zegen of een vloek voor de democratie?’, *NJB 2019/528,* p. 662-669

*Rapporten***Bohemen, van, e.a. 2020**  
P. van Boheemen, G. Munnichs & E. Dujso, *Digitale dreigingen voor de democratie – Over nieuwe technologie en desinformatie*, 2020, Den Haag: Rathenau Instituut.

**EDRi 2017**EDRi, *Recommendations on the German bill “Improving Law Enforcement on Social Networks” (NetzDG)*, 20 juni 2017

**Hoboken, van, e.a. 2019**  
J. van Hoboken, N. Appelman, R. Ó Fathaigh, P. Leerssen, T. McGonagle, N. van Eijk & N. Helberger, *De verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties*, Rapport voor het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Eindrapport), IViR, december 2019.

**McGonagle 2013**   
T. McGonagle, The Council of Europe against online hate speech: Conundrums and challenges (MCM 2013(005), Expert paper for the Council of Europe Conference of Ministers responsible for Media and Information Society, ‘Freedom of Expression and Democracy in the Digital Age: Opportunities, Rights, Responsibilities’, Republic of Serbia, Belgrado: 7-8 November 2013 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059bfce>

**McGonagle 2015**   
T. McGonagle, Freedom of expression: Still a Precondition for Democracy?, Strasbourg: Council of Europe Conference Report 13-14 October 2015, <https://www.ivir.nl/publicaties/download/1707.pdf>

**McGonagle e.a. 2018**   
T. McGonagle, E. Coche, C. Plaizier en M. Klus, *Inventarisatie methodes om “nepnieuws” tegen te gaan*, bijlage bij *Kamerstukken II 2017/18*, 32 827-127, 25 april 2018

**Polyakova & Boyer 2018**   
A. Polyakova & S. Boyer, *The Future of Political Warfare: Russia, the West, and the coming age of global digital competition. The New Geopolitics Europe*, Brookings – Robert Bosch Foundation Transatlantic initiative: 2018.

**Polyakova & Fried 2019**A. Polyakova & D. Fried, *Democratic defense against disinformation 2.0*, Atlantic Council Eurasia Center 2019.

**Raad voor het Openbaar Bestuur 2019**  
Advies van de Raad voor het Openbaar Bestuur, *Zoeken naar de Waarheid. Over waarheidsvinding in de democratie in het digitale tijdperk*, 2019.

**Ramirez e.a 2014**E. Ramirez, J. Brill, M.K. Ohlhausen, J.D. Wright and T. McSweeny, *Data Brokers: A Call For Transparency and Accountability: A report of the Federal Trade Commission,* May 2014, [www.ftc.gov](http://www.ftc.gov).

**Reuters Institute 2020**  
Reuters Institute for the Study of Journalism, *Digital News Report 2020*, University of Oxford: Reuters Institute 2020.

**Wardle & Derakhshan 2018**   
C. Wardle & H. Derahkshan, Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making (Council of Europe Report DGI(2017)09), Strasbourg: Council of Europe 2018.

*Nieuwsartikelen en blogs***Algemeen Dagblad, 6 februari 2017**Pechtold noemt ‘creatief knip-plakwerk’ Wilders ophitsend’, 6 februari 2017 *AD* <https://www.ad.nl/binnenland/pechtold-noemt-creatief-knip-en-plakwerk-wilders-ophitsend~abfbc7cb/> (laatst geraadpleegd op 6 juni 2021)

**Bakker, *Nu.nl* 18 december 2020**S. Bakker, ‘Deze onwaarheden over de coronavaccins gaan nu rond’, *Nu.nl* 18 december 2020, nu.nl/coronavirus/6097360/deze-onwaarheden-over-de-coronavaccins-gaan-nu-rond.html (laatst geraadpleegd op 15 april 2021)

**Dujic*, NOS* 24 augustus 2020**  
F. Dujic, ‘Deepfakes hebben effect op meningen: ‘mensen trappen er vol in’’*NOS* 24 augustus 2020, <https://nos.nl/artikel/2345204-deepfakes-hebben-effect-op-meningen-mensen-trappen-er-vol-in>

**Becker6 juni 2016**  
J. Becker, ‘Wanneer is er sprake van onrechtmatige publicaties?*’,* 6 juni 2016, <https://www.dirkzwager.nl/kennis/artikelen/wanneer-is-sprake-van-onrechtmatige-publicaties/?t=b&utm_expid=.rUxlHM_fRVuvpi9UF7RdhA.1&utm_referrer=https%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3D%26esrc%3Ds%26source%3Dweb%26cd%3D1%26ved%3D2ahUKEwj93rTk___kAhXQbVAKHQ3zDEQQFjAAegQIBBAB%26url%3Dhttps%253A%252F%252Fwww.dirkzwager.nl%252Fkennis%252Fartikelen%252Fwanneer-is-sprake-van-onrechtmatige-publicaties%252F%26usg%3DAOvVaw1ezhNWDpX0BGfw8xl-upTg> (laatst geraadpleegd op 25 juni 2021)

**Bos, 25 juni 2020**  
R. Bos, ‘Onderzoekers stellen een lijst samen met de vijf opvallendste complottheorieën over het coronavirus’, 25 juni 2020, <https://www.quest.nl/maatschappij/cultuur/a32957787/onderzoekers-komen-met-top-vijf-coronavirus-complotten/> (laatst geraadpleegd op 25 juni 2021

**Van Gemert & Bolhuis, 11 januari 2021**  
S. van Gemert & T. Bolhuis, ‘Deze 5 onwaarheden vertelde Thierry Baudet over het coronavirus’, 11 januari 2021, <https://eenvandaag.avrotros.nl/item/deze-5-onwaarheden-vertelde-thierry-baudet-over-het-coronavirus/> (laatst geraadpleegd op 25 juni 2021)

**De Goede, *Rtlnieuws* 2 april 2020**  
A. de Goede, ‘Kabinet huurt influencers in voor coronacampagne: ‘Hou je aan de regels’’*, Rtlnieuws* 2 april 2020, <https://www.rtlnieuws.nl/nieuws/politiek/artikel/5078491/influencers-gaan-opdracht-over-overheid-jongeren-overtuigen> (laatst geraadpleegd op 25 juni 2021)

**De Goede & Hankel, *Rtlnieuws.nl* 10 maart 2021**  
A. de Goede & A. Hankel, ‘Alles voor de aandacht: politici smijten met geld om online gezien te worden’, *Rtlnieuws.nl* 10 maart 2021, [rtlnieuws.nl/nieuws/politiek/artikel/5218807/artijen-smijten-met-geld-en-doen-online-de-gekste-dingen-ze-willen](https://www.rtlnieuws.nl/nieuws/politiek/artikel/5218807/artijen-smijten-met-geld-en-doen-online-de-gekste-dingen-ze-willen) (laatst geraadpleegd op 15 april 2021)

**Khaddari, *Parool* 2 maart 2021**  
R. Khaddari, ‘Politiek vindt weg naar Clubhouse: ‘Mensen willen graag meepraten’’, *Parool* 2 maart 2021, <https://www.parool.nl/nederland/politiek-vindt-weg-naar-clubhouse-mensen-willen-graag-meepraten~b5ae28ea/> (laatst geraadpleegd op 25 juni 2021)

**Kieskamp, *Trouw* 1 maart 2021**  
W. Kieskamp, ‘De online verkiezingscampagne wordt platter én dieper (en professioneler)’, *Trouw* 1 maart 2021, <https://www.trouw.nl/politiek/de-online-verkiezingscampagne-wordt-platter-en-dieper-en-professioneler~b70a148d/> (laatst geraadpleegd op 15 april 2021)

**Klos, *Nederland Rechtsstaat* 30 oktober 2020**  
M. Klos, ‘Mag desinformatie verwijderd worden door internetplatforms?’, *Nederland Rechtsstaat* 30 oktober 2020 <https://www.nederlandrechtsstaat.nl/forum/id357/05-03-2021/gedragscode-politieke-advertenties-blog-3-desinformatie-over-verkiezingen-verwijderen-of-labelen?.html> (laatst geraadpleegd op 6 juni 2021) **Klos, *Nederland Rechtsstaat*, 5 maart 2021**M. Klos, ‘Desinformatie over verkiezingen: verwijderen of labelen?’, *Nederland Rechtsstaat,* 5 maart 2021 <https://www.nederlandrechtsstaat.nl/forum/id357/05-03-2021/gedragscode-politieke-advertenties-blog-3-desinformatie-over-verkiezingen-verwijderen-of-labelen?.html> (laatst geraadpleegd op 15 april 2021)

**Maasbommel, 6 januari 2021**  
S. Maasbommel, ‘Een gedragscode inzake politieke advertenties: meer dan goede intenties?’, 6 januari 2021, <https://www.europa-nu.nl/id/vle4mmj4s0xa/nieuws/een_gedragscode_inzake_politieke>

**NOS, 20 juni 2018**  
‘Denk werkte aan nepadvertentie PVV’, 20 juni 2018 *NOS* <https://nos.nl/artikel/2237443-denk-werkte-aan-nepadvertentie-pvv> (laatst geraadpleegd op 6 juni 2021)

**Nu.nl, 10 februari 2017**  
‘Politieke partij Denk maakt gebruik van nepaccount op sociale media’, 10 februari 2017 *Nu.nl* <https://www.nu.nl/politiek/4459251/politieke-partij-denk-maakt-gebruik-van-nepaccounts-sociale-media.html>

**Shaban, Timberg & Dwoskin, *The Washington Post*** **31 oktober 2017**   
H. Shaban, C. Timberg and E. Dwoskin, ‘Facebook, Google and Twitter testified on Capitol Hill. Here’s what they said.’, *The Washington Post* 31 oktober 2017, <https://www.washingtonpost.com/news/the-switch/wp/2017/10/31/facebook-google-andtwitter-are-set-to-testify-on-capitol-hill-heres-what-to-expect/>, (laatst geraadpleegd op 6 juni 2021).  
  
**Van Uffelen, *Volkskrant.nl* 4 januari 2021**  
X. van Uffelen, ‘Digitale campagne politieke partijen onder de loep’, *Parool* 4 januari 2021, volkskrant.nl/nieuws-achtergrond/digitale-campagne-politieke-partijen-onder-de-loep~b9339112/ (laatst geraadpleegd op 15 april 2021)

**Vroegop, *Algemeen Dagblad* 9 maart 2021**  
B. Vroegop, ‘Twitter noemt tweet van Baudet misleidend, dit zijn de gevolgen’, *AD* 9 maart 2021, <https://www.ad.nl/tech/twitter-noemt-tweet-van-baudet-misleidend-dit-zijn-de-gevolgen~aa9bb784/>

1. T. Hammarberg e.a., *Council of Europe Publishing* 2011, p. 7 [↑](#footnote-ref-1)
2. Instagrammen. (2012). In *Algemeen Nederlands Woordenboek*. Geraadpleegd op 25 maart 2021, http://anw.inl.nl/article/instagrammen [↑](#footnote-ref-2)
3. Gebaseerd op N. Couldry, *European Journal of Communication* 2009, p. 438-441 [↑](#footnote-ref-3)
4. K. Jakubowicz, *Council of Europe Publishing* 2011, p. 17-18 [↑](#footnote-ref-4)
5. Zie bijvoorbeeld S. Bakker, ‘Deze onwaarheden over de coronavaccins gaan nu rond’, 18 december 2020, nu.nl/coronavirus/6097360/deze-onwaarheden-over-de-coronavaccins-gaan-nu-rond.html [↑](#footnote-ref-5)
6. Zie bijvoorbeeld A. de Goede en A. Hankel, ‘Alles voor de aandacht: politici smijten met geld om online gezien te worden’, 10 maart 2021, [rtlnieuws.nl/nieuws/politiek/artikel/5218807/artijen-smijten-met-geld-en-doen-online-de-gekste-dingen-ze-willen](https://www.rtlnieuws.nl/nieuws/politiek/artikel/5218807/artijen-smijten-met-geld-en-doen-online-de-gekste-dingen-ze-willen) en X. van Uffelen, ‘Digitale campagne politieke partijen onder de loep’, 4 januari 2021, volkskrant.nl/nieuws-achtergrond/digitale-campagne-politieke-partijen-onder-de-loep~b9339112/ [↑](#footnote-ref-6)
7. Europese Commissie, *‘*Betreffende het actieplan voor Europese democratie’, COM(2020) 790 final, par. 1 [↑](#footnote-ref-7)
8. Europese Commissie, *‘*Betreffende het actieplan voor Europese democratie’, COM(2020) 790 final, par. 1 [↑](#footnote-ref-8)
9. Van Boheemen e.a. 2020, p. 3 [↑](#footnote-ref-9)
10. Zie bijvoorbeeld *Kamerstukken II* 2020/21, 30821, 118 en *Kamerstukken I* 2020/21, 35526, AG [↑](#footnote-ref-10)
11. M. Klos., ‘Desinformatie over verkiezingen: verwijderen of labelen?’, 5 maart 2021, <https://www.nederlandrechtsstaat.nl/forum/id357/05-03-2021/gedragscode-politieke-advertenties-blog-3-desinformatie-over-verkiezingen-verwijderen-of-labelen?.html> [↑](#footnote-ref-11)
12. Van Hoboken e.a. 2019, p. 12 [↑](#footnote-ref-12)
13. Minister Ollongren, brief aan Tweede Kamer 16 november 2020 [↑](#footnote-ref-13)
14. EU Code of Practice on Disinformation, 26 september 2018, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> [↑](#footnote-ref-14)
15. Digital Services Act, 15 september 2020, <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN> [↑](#footnote-ref-15)
16. Zie bijvoorbeeld W. Kieskamp, ‘De online verkiezingscampagne wordt platter én dieper (en professioneler)’, 1 maart 2021, <https://www.trouw.nl/politiek/de-online-verkiezingscampagne-wordt-platter-en-dieper-en-professioneler~b70a148d/> [↑](#footnote-ref-16)
17. Nieuwenhuis, *Mediaforum* 2018, p. 166 [↑](#footnote-ref-17)
18. Van Keulen e.a. 2018, p. 11-12 [↑](#footnote-ref-18)
19. Van Keulen e.a. 2018, p. 11-12. [↑](#footnote-ref-19)
20. Idem [↑](#footnote-ref-20)
21. McGonagle, *NQHR* 2017, p. 206-207 [↑](#footnote-ref-21)
22. Nieuwenhuis, *Mediaforum* 2018, p. 170 [↑](#footnote-ref-22)
23. Van Hoboken e.a. 2019, p. 12 [↑](#footnote-ref-23)
24. Zie bijvoorbeeld: Wardle & Derakhshan 2018, p. 21, European Commission, HLEG Report on fake news and online disinformation 2018, p. 11, European Commission, ‘Tackling online disinformation: a European Approach’, COM (2018) 236 final, par. 3.1.1 [↑](#footnote-ref-24)
25. European Commission, ‘Tackling online disinformation: a European Approach’, COM (2018) 236 final, par. 3.1.1 [↑](#footnote-ref-25)
26. Wardle & Derakhshan 2018, p. 20 [↑](#footnote-ref-26)
27. McGonagle, *Mediaforum* 2018, p.180 [↑](#footnote-ref-27)
28. McGonagle, *NQHR* 2017, p. 204 [↑](#footnote-ref-28)
29. European Commission, HLEG Report on fake news and online disinformation 2018 p.10 [↑](#footnote-ref-29)
30. J. de Ridder e.a. 2020, p. 257 [↑](#footnote-ref-30)
31. Idem [↑](#footnote-ref-31)
32. J. de Ridder e.a. 2020, p. 260 [↑](#footnote-ref-32)
33. Political Party Innovation Primer 1, ‘Digital Microtargeting’, International Institute for Democracy and Electoral Assistance 2018, p. 8 [↑](#footnote-ref-33)
34. Political Party Innovation Primer 1, ‘Digital Microtargeting’, International Institute for Democracy and Electoral Assistance 2018, p. 6 [↑](#footnote-ref-34)
35. J. de Ridder e.a. 2020, p. 261 [↑](#footnote-ref-35)
36. Idem [↑](#footnote-ref-36)
37. J. de Ridder e.a. 2020, p. 258 [↑](#footnote-ref-37)
38. Gebaseerd op J. de Ridder e.a. 2020, p. 257-261 [↑](#footnote-ref-38)
39. Political Party Innovation Primer 1, ‘Digital Microtargeting’, International Institute for Democracy and Electoral Assistance 2018, p. 6 [↑](#footnote-ref-39)
40. Van Keulen e.a. 2018, p. 10 [↑](#footnote-ref-40)
41. R. Khaddari, ‘Politiek vindt weg naar Clubhouse: ‘Mensen willen graag meepraten’’, 2 maart 2021, <https://www.parool.nl/nederland/politiek-vindt-weg-naar-clubhouse-mensen-willen-graag-meepraten~b5ae28ea/> [↑](#footnote-ref-41)
42. Influencers hebben veelal een groot bereik op sociale mediakanalen en hebben vaak een sterke connectie met hun volgers. [↑](#footnote-ref-42)
43. A. de Goede, ‘Kabinet huurt influencers in voor coronacampagne: ‘Hou je aan de regels’’, 2 april 2020, <https://www.rtlnieuws.nl/nieuws/politiek/artikel/5078491/influencers-gaan-opdracht-over-overheid-jongeren-overtuigen> [↑](#footnote-ref-43)
44. ‘Pechtold noemt ‘creatief knip-plakwerk’ Wilders ophitsend’, 6 februari 2017 *AD* <https://www.ad.nl/binnenland/pechtold-noemt-creatief-knip-en-plakwerk-wilders-ophitsend~abfbc7cb/> [↑](#footnote-ref-44)
45. ‘Politieke partij Denk maakt gebruik van nepaccount op sociale media’, 10 februari 2017 *Nu.nl* <https://www.nu.nl/politiek/4459251/politieke-partij-denk-maakt-gebruik-van-nepaccounts-sociale-media.html> [↑](#footnote-ref-45)
46. ‘Denk werkte aan nepadvertentie PVV’, 20 juni 2018 *NOS* <https://nos.nl/artikel/2237443-denk-werkte-aan-nepadvertentie-pvv> [↑](#footnote-ref-46)
47. W. Kieskamp, ‘De online verkiezingscampagne wordt platter én dieper (en professioneler)’, 1 maart 2021 *Trouw* <https://www.trouw.nl/politiek/de-online-verkiezingscampagne-wordt-platter-en-dieper-en-professioneler~b70a148d/> [↑](#footnote-ref-47)
48. Minister Ollongren, brief aan Tweede Kamer over de heimelijke beïnvloeding van de publieke opinie door statelijke actoren, 18 december 2017 [↑](#footnote-ref-48)
49. Kamerstukken II, 2020/2021, 35570-VII, nr. 10 [↑](#footnote-ref-49)
50. M. Klos., Desinformatie over verkiezingen: verwijderen of labelen*?*, *Nederland rechtsstaat* 5 maart 2021, <https://www.nederlandrechtsstaat.nl/forum/id357/05-03-2021/gedragscode-politieke-advertenties-blog-3-desinformatie-over-verkiezingen-verwijderen-of-labelen?.html> [↑](#footnote-ref-50)
51. Nederlandse Gedragscode Transparantie Online Politieke Advertenties, 9 februari 2021 [↑](#footnote-ref-51)
52. Vloeit voort uit artikel 11 Handvest naar aanleiding van jurisprudentie van het EHRM. [↑](#footnote-ref-52)
53. Van Hoboken e.a. 2019, p. 39 [↑](#footnote-ref-53)
54. Artikel 52 lid 3 Handvest [↑](#footnote-ref-54)
55. EHRM 7 december 1976 (Handyside/Verenigd Koninkrijk), r.o. 49 [↑](#footnote-ref-55)
56. EHRM 19 februari 1998 (Bowman/Verenigd Koninkrijk), r.o. 42 [↑](#footnote-ref-56)
57. EHRM 7 december 1976 (Handyside/Verenigd Koninkrijk), r.o. 49 [↑](#footnote-ref-57)
58. EHRM 2 december 2008 (K.U./Finland), r.o. 49 [↑](#footnote-ref-58)
59. Artikel 10 lid 2 EVRM [↑](#footnote-ref-59)
60. Oosterveld & Oostveen, *Mediaforum* 2013, p. 152. [↑](#footnote-ref-60)
61. EHRM 21 januari 1999 (Fressoz en Roire/Frankrijk), r.o. 54. [↑](#footnote-ref-61)
62. Artikel 17 EVRM [↑](#footnote-ref-62)
63. McGonagle, *NQHR* 2017, p. 204 [↑](#footnote-ref-63)
64. T. Hammarberg e.a., *Council of Europe Publishing* 2011, p. 7 [↑](#footnote-ref-64)
65. Harrison & Barthel, *New Media & Society* 2009, p. 159-160 [↑](#footnote-ref-65)
66. Oosterveld & Oostveen, *Mediaforum* 2013, p. 149 [↑](#footnote-ref-66)
67. EHRM 25 april 1978 (Tyrer/Verenigd Koninkrijk), r.o. 31; McGonagle & de Boer, *Mediaforum* 2012, p. 339 [↑](#footnote-ref-67)
68. Zie voor een vergelijkbare discussie: EHRM 9 oktober 1979 (Airey/Ierland), r.o. 24 [↑](#footnote-ref-68)
69. Harris e.a. 2018, p. 19 [↑](#footnote-ref-69)
70. EHRM 16 maart 2000 (Ozgür Gündem/Turkije) r.o. 43; EHRM 14 september 2010 (Dink/Turkije), r.o. 106; EHRM 12 september 2011 (Palomo Sánchez e.a./Spanje) r.o. 59 [↑](#footnote-ref-70)
71. EHRM 8 juli 1986 (Lingens/Oostenrijk) r.o. 39 [↑](#footnote-ref-71)
72. EHRM 14 september 2010 (Dink/Turkije), r.o. 137 [↑](#footnote-ref-72)
73. EHRM 24 november 1993 (Informationsverein Lentia e.a./Oostenrijk) r.o. 38 [↑](#footnote-ref-73)
74. Broekstra, *Mediaforum* 2015, p. 8. [↑](#footnote-ref-74)
75. Van Hoboken e.a. 2019, p. 39 [↑](#footnote-ref-75)
76. EHRM 15 februari 2005 (Steel and Morris/Verenigd Koninkrijk) r.o. 89 [↑](#footnote-ref-76)
77. Van Hoboken e.a. 2019, p. 39 [↑](#footnote-ref-77)
78. EHRM 22 april 2013 (Animal Defenders International/Verenigd Koninkrijk) r.o. 112 [↑](#footnote-ref-78)
79. Verordening (EU) 2016/679 (AVG) [↑](#footnote-ref-79)
80. Paragraaf 26 AVG en artikel 4 lid 1 AVG [↑](#footnote-ref-80)
81. Van Hoboken e.a. 2019, p. 63 [↑](#footnote-ref-81)
82. Idem [↑](#footnote-ref-82)
83. Zie het Europees Comité voor gegevensbescherming, verklaring 2/2019 over het gebruik van persoonsgegevens in het kader van politieke campagnes, aangenomen op 13 maart 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections\_en.pdf. Zie ook bijlage 1 over de nationale richtsnoeren van de gegevensbeschermingsautoriteit: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections-annexi\_en.pdf. [↑](#footnote-ref-83)
84. Autoriteit Persoonsgegevens “Verkennend onderzoek naar gebruik pesoonsgegevens in verkiezingscampagnes”, 15 februari 2019, https://autoriteitpersoonsgegevens.nl/nl/nieuws/verkennend-onderzoek-naar-gebruik-persoonsgegevens-verkiezingscampagnes [↑](#footnote-ref-84)
85. Van Hoboken e.a. 2019, p. 63 [↑](#footnote-ref-85)
86. Idem [↑](#footnote-ref-86)
87. Artikel 9 lid 1 AVG [↑](#footnote-ref-87)
88. Artikel 9 lid 2 sub a AVG [↑](#footnote-ref-88)
89. Broekstra, *Mediaforum* 2015, p. 8 [↑](#footnote-ref-89)
90. Reuters Institute 2020, p. 10 [↑](#footnote-ref-90)
91. Zie artikel 12-15 Richtlijn 2000/31/EG [↑](#footnote-ref-91)
92. HvJ EU 16 februari 2012 (SABAM/Netlog), r.o. 27 [↑](#footnote-ref-92)
93. Zie artikel 14 Richtlijn 2000/31/EG [↑](#footnote-ref-93)
94. Paragraaf 42 Richtlijn 2000/31/EG [↑](#footnote-ref-94)
95. Artikel 14 lid 1 sub a en sub b Richtlijn 2000/31/EG [↑](#footnote-ref-95)
96. Richtlijn 2010/13/EU [↑](#footnote-ref-96)
97. Richtlijn (EU) 2018/1808 [↑](#footnote-ref-97)
98. Artikel 28 ter lid 1 Richtlijn (EU) 2018/1808 [↑](#footnote-ref-98)
99. Idem [↑](#footnote-ref-99)
100. Artikel 15 lid 1 Richtlijn 2000/31/EG; HvJ EU 24 november 2011 (Scarlet Extended/SABAM e.a.) r.o. 40 [↑](#footnote-ref-100)
101. Paragraaf 47 Richtlijn 2000/31/EG [↑](#footnote-ref-101)
102. EHRM (GK) 16 juni 2015 (Delfi AS/Estland) [↑](#footnote-ref-102)
103. EHRM 16 juni 2015 (Delfi AS/Estland), r.o. 140-143 en r.o. 162 [↑](#footnote-ref-103)
104. Lievens & Voorhoof, *Mediaforum* 2016, p. 184; EHRM 2 februari 2016 (Magyar Tartalomszolgáltatók Egyesülete en Index.hu Zrt/Hongarije) [↑](#footnote-ref-104)
105. EHRM 9 maart 2017 (Pihl/Zweden), r.o. 37 en r.o. 38 [↑](#footnote-ref-105)
106. McGonagle 2015, p. 14 [↑](#footnote-ref-106)
107. Advies van de Raad voor het Openbaar Bestuur, *Zoeken naar de Waarheid. Over waarheidsvinding in de democratie in het digitale tijdperk*, 2019, p. 34-35 [↑](#footnote-ref-107)
108. McGonagle, NQHR 2017, p. 204. [↑](#footnote-ref-108)
109. Dit zijn geautomatiseerde accounts op sociale mediakanalen die menselijk gedrag nabootsen. [↑](#footnote-ref-109)
110. Advies van de Raad voor het Openbaar Bestuur, *Zoeken naar de Waarheid. Over waarheidsvinding in de democratie in het digitale tijdperk*, 2019, p. 34-35 [↑](#footnote-ref-110)
111. Idem [↑](#footnote-ref-111)
112. Zodanig gemanipuleerd beeld- en geluidmateriaal dat het lijkt alsof iemand handelingen heeft verricht die hij in werkelijkheid niet heeft verricht of uitspraken heeft gedaan die hij in werkelijkheid niet heeft gedaan. [↑](#footnote-ref-112)
113. Zie bijvoorbeeld F. Dujic, *NOS* 24 augustus 2020, <https://nos.nl/artikel/2345204-deepfakes-hebben-effect-op-meningen-mensen-trappen-er-vol-in> [↑](#footnote-ref-113)
114. Van Keulen e.a. 2018, p. 55 [↑](#footnote-ref-114)
115. Shaban, Timberg & Dwoskin, *The Washington Post* 31 oktober 2017, <https://www.washingtonpost.com/news/the-switch/wp/2017/10/31/facebook-google-and-twitter-are-set-to-testify-on-capitol-hill-heres-what-to-expect/> [↑](#footnote-ref-115)
116. Polyakova & Boyer 2018, p. 2-3; van Keulen e.a. 2018, p. 35 [↑](#footnote-ref-116)
117. EC Communication COM(2018)236; van Keulen e.a. 2018, p. 11-12; Minister Ollongren, brief aan Tweede Kamer 18 december 2017 [↑](#footnote-ref-117)
118. McGonagle, NQHR 2017, p. 206-207 [↑](#footnote-ref-118)
119. Zuiderveen Borgesius e.a., *NJB 2019/528*, p. 662 [↑](#footnote-ref-119)
120. Zuiderveen Borgesius e.a., *NJB 2019/528*, p. 666 [↑](#footnote-ref-120)
121. Idem [↑](#footnote-ref-121)
122. Art. 22(2)(c) Uitvoeringswet Algemene Verordeningsbescherming (UAVG) [↑](#footnote-ref-122)
123. Art. 9 AVG [↑](#footnote-ref-123)
124. Art. 13-15 AVG. [↑](#footnote-ref-124)
125. Richtlijn 2002/58/EC (laatst herzien in 2009); art. 11.7a Telecommunicatiewet [↑](#footnote-ref-125)
126. Federal Trade Commission, 2014, p. 4 [↑](#footnote-ref-126)
127. Zuiderveen Borgesius e.a., *NJB 2019/528*, p. 667 [↑](#footnote-ref-127)
128. Zuiderveen Borgesius e.a., *NJB 2019/528*, p. 666 - 667 [↑](#footnote-ref-128)
129. Zuiderveen Borgesius e.a., *NJB 2019/528*, p. 668 [↑](#footnote-ref-129)
130. Zuiderveen Borgesius e.a., *Internet Policy Review* 2016, p. 10 [↑](#footnote-ref-130)
131. European Commission, HLEG Report on fake news and online disinformation 2018, p. 11. [↑](#footnote-ref-131)
132. Nederlandse Gedragscode Transparantie Online Politieke Advertenties (2021) [↑](#footnote-ref-132)
133. Van Hoboken e.a. 2019, p. 109 [↑](#footnote-ref-133)
134. Idem [↑](#footnote-ref-134)
135. McGonagle e.a. 2018, p. 39 [↑](#footnote-ref-135)
136. NetzDG 7 september 2017 (inwerkingtreding: 1 oktober 2017). [↑](#footnote-ref-136)
137. Artikel 1, afdeling 3 (2) sub 2, NetzDG. [↑](#footnote-ref-137)
138. Artikel 1, afdeling 3(2) sub 3 NetzDG. [↑](#footnote-ref-138)
139. Artikel 1, afdeling 1 en 4 NetzDG; Van Hoboken e.a. 2019, p. 110 [↑](#footnote-ref-139)
140. EDRi, Recommendations on the NetzDG, 20 juni 2017 [↑](#footnote-ref-140)
141. Boom e.a. 2009, p. 37 [↑](#footnote-ref-141)
142. Boom e.a. 2009, p 35-37 [↑](#footnote-ref-142)
143. EC Communication COM(2018)236, p. 8 [↑](#footnote-ref-143)
144. EC Communication COM(2018)236, p. 9 [↑](#footnote-ref-144)
145. Boom e.a. 2009, p. 35-36 [↑](#footnote-ref-145)
146. Idem [↑](#footnote-ref-146)
147. Kamerbrief over Co-en zelfregulering in de mediasector, 17 december 2019 [↑](#footnote-ref-147)
148. Boom e.a. 2009, p. 35-36 [↑](#footnote-ref-148)
149. Idem [↑](#footnote-ref-149)
150. European Commission, HLEG Report on fake news and online disinformation 2018 [↑](#footnote-ref-150)
151. European Commission, Assessment of the implementation of the Code of Practice on Disinformation 2020 p. 27 [↑](#footnote-ref-151)
152. EU Code of Practice on Disinformation 2018, IV. Assessment Period [↑](#footnote-ref-152)
153. Effectiviteit ziet toe op de mate waarin potentiële gevaren van (gepersonaliseerde) politieke advertenties en online desinformatie door de Code worden verminderd of zelfs worden voorkomen. [↑](#footnote-ref-153)
154. European Commission, Assessment of the implementation of the Code of Practice on Disinformation 2020 p. 32-33 [↑](#footnote-ref-154)
155. Global Partners Digital, 27 september 2018 [↑](#footnote-ref-155)
156. European Commission, Assessment of the implementation of the Code of Practice on Disinformation 2020 p. 34 [↑](#footnote-ref-156)
157. Idem [↑](#footnote-ref-157)
158. EC Communication COM(2018)236, p. 9 [↑](#footnote-ref-158)
159. Rb. Amsterdam 9 september 2020, ECLI:NL:RBAMS:2020:4435; Rb. Amsterdam 13 oktober 2020, ECLI:NL:RBAMS:2020:4966 [↑](#footnote-ref-159)
160. EU Code of Practice on Disinformation 2018. [↑](#footnote-ref-160)
161. M. Klos, ‘Mag desinformatie verwijderd worden door internetplatforms?’, 30 oktober 2020 <https://www.nederlandrechtsstaat.nl/forum/id357/05-03-2021/gedragscode-politieke-advertenties-blog-3-desinformatie-over-verkiezingen-verwijderen-of-labelen?.html> [↑](#footnote-ref-161)
162. J. Kester, ‘Verkiezingscampagne gaat te weinig over Nederland ná corona, zegt een ruime meerderheid van de kiezers’, 19 februari 2021, <https://eenvandaag.avrotros.nl/panels/opiniepanel/alle-uitslagen/item/verkiezingscampagne-gaat-te-weinig-over-nederland-na-corona-zegt-een-ruime-meerderheid-van-de-kiezers/> [↑](#footnote-ref-162)
163. Commission presents Guidance to strengthen the Code of Practice on Disinformation, Press Release 26 May 2021, <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585> [↑](#footnote-ref-163)
164. European Comission Guidance on Strengthening the Code of Practice on Disinformation (COM(2021) 262 final) [↑](#footnote-ref-164)
165. Idem [↑](#footnote-ref-165)
166. Zie <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> [↑](#footnote-ref-166)
167. Geus & Sickinghe, *Mediaforum 2021*, p. 42 [↑](#footnote-ref-167)
168. Tussenhandelsdiensten maken deel uit van de ‘diensten van de informatiemaatschappij’. Zie bijvoorbeeld artikel 1 lid 1 sub b van Richtlijn (EU) 2015/15358. [↑](#footnote-ref-168)
169. Artikel 2 (sub f en h) DSA [↑](#footnote-ref-169)
170. Diensten waarbij de aanbieder slechts fungeert als ‘doorgeefluik’ van informatie die door de afnemers van de dienst is verstrekt (een voorbeeld hiervan zijn internet serviceproviders). [↑](#footnote-ref-170)
171. Online platforms die meer dan 45 miljoen maandelijks actieve gebruikers binnen de Europese Unie hebben. [↑](#footnote-ref-171)
172. Zie artikel 3 tot en met 9 DSA. [↑](#footnote-ref-172)
173. Diensten die informatie van derden opslaan (bijvoorbeeld cloud- en webhosting diensten). Online platforms vormen een afzonderlijke categorie van hosting diensten die informatie niet alleen opslaan, maar ook toegankelijk maken voor derden en verspreiden naar derden. [↑](#footnote-ref-173)
174. Artikel 5 DSA [↑](#footnote-ref-174)
175. Artikel 14 e-Commercerichtlijn [↑](#footnote-ref-175)
176. Zie artikel 5 DSA; zie ook Geus & Sickinghe, *Mediaforum 2021*, p. 44 [↑](#footnote-ref-176)
177. Overweging 22 van de DSA. [↑](#footnote-ref-177)
178. J. Becker, ‘Wanneer is er sprake van onrechtmatige publicaties?’,6 juni 2016, <https://www.dirkzwager.nl/kennis/artikelen/wanneer-is-sprake-van-onrechtmatige-publicaties/?t=b&utm_expid=.rUxlHM_fRVuvpi9UF7RdhA.1&utm_referrer=https%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3D%26esrc%3Ds%26source%3Dweb%26cd%3D1%26ved%3D2ahUKEwj93rTk___kAhXQbVAKHQ3zDEQQFjAAegQIBBAB%26url%3Dhttps%253A%252F%252Fwww.dirkzwager.nl%252Fkennis%252Fartikelen%252Fwanneer-is-sprake-van-onrechtmatige-publicaties%252F%26usg%3DAOvVaw1ezhNWDpX0BGfw8xl-upTg> [↑](#footnote-ref-178)
179. R. Bos, ‘Onderzoekers stellen een lijst samen met de vijf opvallendste complottheorieën over het coronavirus’, 25 juni 2020, <https://www.quest.nl/maatschappij/cultuur/a32957787/onderzoekers-komen-met-top-vijf-coronavirus-complotten/> [↑](#footnote-ref-179)
180. S. van Gemert & T. Bolhuis, ‘Deze 5 onwaarheden vertelde Thierry Baudet over het coronavirus’, 11 januari 2021, <https://eenvandaag.avrotros.nl/item/deze-5-onwaarheden-vertelde-thierry-baudet-over-het-coronavirus/> [↑](#footnote-ref-180)
181. B. Vroegop,’ Twitter noemt tweet van Baudet misleidend, dit zijn de gevolgen’, 9 maart 2021, <https://www.ad.nl/tech/twitter-noemt-tweet-van-baudet-misleidend-dit-zijn-de-gevolgen~aa9bb784/> [↑](#footnote-ref-181)
182. Idem [↑](#footnote-ref-182)
183. Zie het statement van Twitter op 8 januari 2021, <https://blog.twitter.com/en_us/topics/company/2020/suspension> [↑](#footnote-ref-183)
184. B. Vroegop, ‘Twitter noemt tweet van Baudet misleidend, dit zijn de gevolgen’, 9 maart 2021, <https://www.ad.nl/tech/twitter-noemt-tweet-van-baudet-misleidend-dit-zijn-de-gevolgen~aa9bb784/> [↑](#footnote-ref-184)
185. Nederlandse Gedragscode Transparantie Online Politieke Advertenties 2021 [↑](#footnote-ref-185)
186. Kamerstukken II, 2020/2021, 35 570 VII, 10. [↑](#footnote-ref-186)
187. EU Code of Practice on Disinformation 2018. [↑](#footnote-ref-187)
188. M. Klos, ‘Desinformatie over verkiezingen: verwijderen of labelen?’, 5 maart 2021, <https://www.nederlandrechtsstaat.nl/forum/id357/05-03-2021/gedragscode-politieke-advertenties-blog-3-desinformatie-over-verkiezingen-verwijderen-of-labelen?.html> [↑](#footnote-ref-188)
189. M. Klos, ‘Desinformatie over verkiezingen: verwijderen of labelen?’, 5 maart 2021, <https://www.nederlandrechtsstaat.nl/forum/id357/05-03-2021/gedragscode-politieke-advertenties-blog-3-desinformatie-over-verkiezingen-verwijderen-of-labelen?.html> [↑](#footnote-ref-189)
190. Nederlandse Gedragscode Transparantie Online Politieke Advertenties 2021, p. 4 [↑](#footnote-ref-190)
191. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement; Kamerstukken II, 30 821, 35 165, 118, p. 4-5 [↑](#footnote-ref-191)
192. S. Maasbommel, *Een gedragscode inzake politieke advertenties: meer dan goede intenties?*, 6 januari 2021, <https://www.europa-nu.nl/id/vle4mmj4s0xa/nieuws/een_gedragscode_inzake_politieke> [↑](#footnote-ref-192)
193. M. Klos, *Desinformatie over verkiezingen: verwijderen of labelen?*, 5 maart 2021, <https://www.nederlandrechtsstaat.nl/forum/id357/05-03-2021/gedragscode-politieke-advertenties-blog-3-desinformatie-over-verkiezingen-verwijderen-of-labelen?.html> [↑](#footnote-ref-193)
194. Van Hoboken e.a. 2019, p. 129-131 [↑](#footnote-ref-194)