



Het juridisch kader voor de verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties

Eindrapport, december 2019

Instituut voor Informatierecht (IViR),
Universiteit van Amsterdam, 2019

Een rapport voor het ministerie van
Binnenlandse Zaken en Koninkrijksrelaties



UNIVERSITEIT VAN AMSTERDAM



Instituut voor Informatierecht
Faculteit der Rechtsgeleerdheid
Universiteit van Amsterdam
Nieuwe Achtergracht 166
1018 WV Amsterdam

Het juridisch kader voor de verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties

Eindrapportage

Joris van Hoboken
Naomi Appelman
Ronan Ó Fathaigh
Paddy Leerssen
Tarlach McGonagle
Nico van Eijk (betrokken tot 31 oktober 2019)
Natali Helberger

Amsterdam, december 2019

Inhoudsopgave

1. Introductie	11
A. Algemene introductie	11
B. Nederlandse situering	12
C. Onderzoeksvragen	12
D. Tussenrapportage: desinformatie en politieke advertenties	13
E. Opzet van de studie	14
2. Desinformatie	15
A. Conceptuele inkadering	15
i. Definities	15
ii. Reikwijdte: type uitingen & juridische kwalificatie	18
iii. Actoren	19
B. Problematiek en feitelijke situatie	21
C. Context van desinformatie	24
i. Desinformatie en nieuws	24
ii. Desinformatie en hate speech	26
iii. Desinformatie en commerciële uitingen	26
iv. Desinformatie en buitenlandse invloeden	27
D. Desinformatie en politieke advertenties	27
E. Samenvatting & Conclusie	31
3. Rechtspositie relevante internetdiensten (tech bedrijven)	33
A. Definiëring relevante internetdiensten	33
B. Bedrijfsvormen en verdienmodellen	34
C. Handhavingsmodaliteiten van internetdiensten	35
D. Samenvatting	37
4. Vrijheid van meningsuiting	38
A. Artikel 10 EVRM en artikel 11 EU-Handvest	38
i. Positieve verplichtingen van de staat om pluralisme te garanderen	39
ii. Vrijheid van meningsuiting en onjuiste of misleidende informatie	40
iii. Artikel 10 EVRM & ruime definities van desinformatie	42
iv. Artikel 10 van het EVRM en schade voor het publiek	43
v. Commerciële uitingen	44
vi. Hate speech	45
vii. Politieke advertenties als een vorm van politieke meningsuiting	46
viii. De toelaatbaarheid van een verbod op politieke advertenties	47
ix. Internetdiensten en vrijheid van meningsuiting	49
x. Beperking van schaal, het bereik en de omvang van de publicatie	50
xi. Transparantie	51
xii. Buitenlandse invloeden	53
xiii. Beperken van onjuiste informatie tijdens verkiezingstijd	55
B. De Nederlandse Grondwet	56
C. Samenvatting & conclusie	58

5. Europees regelgevend kader	60
A. Richtlijn elektronische handel	60
B. Algemene Verordening Gegevensbescherming	63
C. Regulering van direct marketing	65
D. Richtlijn Audiovisuele Mediadiensten	67
E. Desinformatie & commerciële regelgeving	70
F. Huidige stand van zaken op het gebied van zelf- en co-regulering	74
G. Recente ontwikkelingen en voorstellen	76
H. Overzicht EU-kader	78
 6. Nationaal wettelijk kader	 79
A. Privaatrechtelijke normen	79
B. Strafrechtelijke normen	82
i. Onlinemanipulatie van verkiezingen	82
ii. Desinformatie & Computervredebreuk	88
iii. Desinformatie & verspreidingsdelicten	91
C. Bestuursrechtelijke normen	92
i. Regulering van advertenties	92
ii. Financiering politieke partijen	94
iii. Nationale veiligheid	95
iv. Vitale/kritische infrastructuur	97
D. Zelfregulering	97
E. Nationale politieke ontwikkelingen	102
i. Rapport Staatscommissie Parlementair Stelsel	102
ii. Wet op de politieke partijen	103
iii. Moties	104
iv. Bewustwordingscampagnenationale	105
v. Mediawijzer	105
vi. NL DIGIbeter 2019	106
vii. Toezegging minister Dekker	106
viii. Brief minister Ollongren	106
F. Overzicht nationale wetgeving	106
 7. Synthese	 108
A. Desinformatie	108
i. Landenstudies en beleidsvoorbeelden	108
ii. Verkiezingstoezicht en desinformatie	112
iii. Politieke advertenties en desinformatie	113
B. Beleidsniveaus	116
C. Landenstudies en beleidsvoorbeelden	118
 8. Samenvatting en conclusies	 122
A. Context & onderzoeksoopdracht	122
B. Samenvatting & conclusies	124
C. Aanbevelingen	129
 Literatuurlijst	 132

Bijlage: Landenstudies	149
A. Inleiding tot de landenstudies	149
B. Verenigd Koninkrijk	150
i. Algemene karakterisering	150
ii. Regulering van desinformatie	151
iii. Regelgeving inzake politieke advertenties	153
C. Frankrijk	154
i. Algemene kenmerken	154
ii. Regulering van desinformatie	154
iii. Politieke advertenties	156
D. Duitsland	157
i. Algemene kenmerken	157
ii. Regulering van desinformatie	158
iii. Politieke advertenties	159
E. Zweden	161
i. Algemene kenmerken	161
ii. Regulering van desinformatie	161
iii. Politieke advertenties	163
F. Verenigde Staten	163
i. Algemene kenmerken	163
ii. Regulering van desinformatie	164
iii. Politieke advertenties	165
G. Canada	167
i. Algemene kenmerken	167
ii. Regulering van desinformatie	168
iii. Politieke advertenties	168

1. Introductie

A. Algemene introductie

De verspreiding van desinformatie online en de mogelijk schadelijke gevolgen voor een vrije democratische samenleving zijn de afgelopen jaren onophoudelijk onderwerp geweest van politiek debat en wetenschappelijk onderzoek. De potentieel ondermijnende werking van desinformatie voor (het vertrouwen in) het democratische proces en de media is door een aantal internationale incidenten nadrukkelijk in het publieke bewustzijn gegrift.¹ De Europese Commissie stelt dat desinformatie het vertrouwen in de media en democratieën kan ondermijnen, burgers limiteert in hun vrije informatiegaring en een toename van radicale en extremistische ideeën kan veroorzaken.² Hiermee raakt de problematiek geassocieerd met desinformatie potentieel aan de kern van de Nederlandse samenleving, wat het noodzakelijk maakt het bestaande wettelijke kader en mogelijke waarborgen aan onderzoek te onderwerpen.

De problematiek rond desinformatie is ontstaan in de context van een in sterke mate veranderd medialandschap waarbij de traditionele, lineaire massamedia in toenemende mate aan invloed inboeten ten koste van veelal geïndividualiseerde onlinediensten zoals sociale media. De schadelijke gevolgen van desinformatie kunnen ook direct gekoppeld worden aan dit veranderde medialandschap, nu deze voornamelijk het gevolg zijn van de nieuwe mogelijkheid om desinformatie op grote schaal en op voorheen ondenkbare manieren te verspreiden.³ Maatschappelijke actoren die voordeel proberen te halen uit het verspreiden van onjuiste en misleidende informatie zijn immers van alle tijden. De snelle, gerichte, groot-schalige en vaak gepersonaliseerde verspreiding via internetdiensten is daarentegen wel nieuw.

In het veranderde medialandschap staat een relatief kleine groep internationaal opererende internetdiensten centraal, die hierdoor ook een grote impact op lokale democratische processen kunnen hebben.⁴ Wat vervolgens deze problematiek verder compliceert zijn de socio-technologische verspreidingsprocessen die bij de verspreiding van desinformatie via internetdiensten in het vizier komen. Hierbij kan gedacht worden aan mirco-targeting, astroturfing, de inzet van bots, trolls en andere online manipulatietechnieken.

De problematiek stelt overheden verder voor de uitdaging om desinformatie op zo een manier aan te pakken dat een open, vrije en democratische samenleving beschermd wordt maar tegelijkertijd fundamentele rechten zoals met name de vrijheid van meningsuiting niet onnodig wordt ingeperkt door deze maatregelen. Veel wetgevers zijn deze uitdaging aan gegaan en in reactie op deze problematiek rond desinformatie zijn op zowel Europees als nationaal niveau meerdere initiatieven ontwikkeld om aspecten van de verspreiding van desinformatie via deze internetdiensten te reguleren.⁵

¹ Bijvoorbeeld de Russische inmeninging via onder andere de "Internet Research Agency" in de presidentsverkiezingen van de Verenigde Staten in 2016, U.S. Department of Justice, Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller, III (DOJ, 2019).

² Europese Commissie, 'Tackling online disinformation: a European Approach, COM(2018) 236 final', par. 2.2.

³ Neudert, L.M.N., 'Computational Propaganda in Germany: A Cautionary Tale', Computational Propaganda Working Paper, 2017.7, Oxford: Oxford Internet Institute; Rogers, R., & Niederer, S. 'The politics of social media manipulation: A view from the Netherlands', 2019, p. 17; Bayer, J., et al., 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States', 2019, European Union, p. 22.

⁴ European Commission, 'Tackling online disinformation: a European Approach, COM(2018) 236 final', par. 2.2.

⁵ Bijvoorbeeld: 'Idemem; Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, Interim mission report - "Regulation of social networks – Facebook experiment," Submitted to the French Secretary of State for Digital Affairs, 2019, https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf; Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department, Online Harms White Paper (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

Echter, de complexiteit van de problematiek rond desinformatie en het belang van de nationale context voor regulering die raakt aan het publieke debat maakt dat een enkele maatregel niet afdoende zal zijn.

B. Nederlandse situering

De problematiek rondom desinformatie geniet ook in de Nederlandse context veel aandacht.⁶ Wat betreft de feitelijke situatie, is uit recent onderzoek gebleken dat er in Nederland sprake is van een in toeneemende mate polariserende mediasfeer. Daarnaast bleek dat het aan desinformatie gerelateerde concept van “junknieuws” wijdverspreid is in Nederland.⁷ Politiek gezien geniet het fenomeen ondertussen veel politieke aandacht met een groot aantal Tweede Kamermoties die de regering verzoeken specifiek desinformatie of gerelateerde problematiek te adresseren.⁸ Ook is de Nederlandse regering een bewustwordingscampagne gestart met betrekking tot desinformatie, en heeft de regering recentelijk haar desinformatiestrategie aan de Tweede Kamer gepresenteerd.⁹

Ondanks de uitgebreide aandacht voor het fenomeen en de verschillende reguleringsinitiatieven bestaan er nog veel vragen met betrekking tot de aanpak van desinformatie in de Nederlandse context. Zo is nog steeds niet volledig helder wat de omvang en de impact is van desinformatie op de Nederlandse samenleving. Daarnaast bestaan er ook vanuit juridisch perspectief veel onduidelijkheden. Zo kent “desinformatie” zelf geen eenduidige, laat staan een afgebakende, juridische definitie en is gezien de breedte van het fenomeen het toepasselijke wettelijke kader niet goed vastgesteld. Hieruit volgt ook dat niet altijd helder is waar de ruimte ligt voor nationale regulering binnen de Europese kaders. Hieraan nauw verwant is het feit dat ten aanzien van de verspreiding en de hoeveelheid desinformatie er een grote informatie asymmetrie bestaat tussen de internetdiensten enerzijds en de wetgever, onderzoekers en de bredere maatschappij anderzijds.

Deze onduidelijkheid die nog steeds heerst over de juridische kwalificatie van het fenomeen, het relevante wettelijk kader en de mogelijke reguleringsopties vormt samen met een deze Tweede Kamermoties de aanleiding voor dit juridische onderzoek. Hoewel het bredere medialandschap relevant is, wordt in dit onderzoek slechts gefocust op de verspreiding van desinformatie via internetdiensten. Het feit dat deze diensten een bijzondere rol spelen in het faciliteren van desinformatie, alsmede de vragen die spelen ten aanzien van hun verantwoordelijkheid en soms grote informatie asymmetrie ten aanzien van deze diensten, maakt dat deze focus voor de hand ligt. Het overkoepelende doel is om helderheid te scheppen in het relevante juridische kader met betrekking tot de verspreiding van desinformatie via internetdiensten in Nederland en om aan te geven waar eventueel ruimte voor regulering ligt.¹⁰

C. Onderzoeksvragen

Aan het onderzoek liggen een zevental door het ministerie voorgelegde onderzoeksvragen ten grondslag. De vragen variëren van heel algemeen naar zeer specifiek, maar hebben alle betrekking op de bredere problematiek rond desinformatie, het bestaande juridische kader en de mogelijkheid tot verdere regulering. Deze zeven vragen worden dan ook alle beantwoord in de context van de brede analyse in het rapport van het relevante wettelijk kader voor de verspreiding van desinformatie via internetdiensten en mogelijke reguleringsopties. De zeven onderzoeksvragen luiden als volgt:

⁶ Zie bijvoorbeeld: Tweede Kamer, vergaderjaar 2018-2019, 30821, nr. 51.

⁷ Rogers, R., & Niederer, S. *The politics of social media manipulation: A view from the Netherlands*, 2019, p. 16.

⁸ Zie bijvoorbeeld: Motie Asscher en Buitenweg, Tweede Kamer, vergaderjaar 2018-2019, 35 078, nr. 21; Motie Asscher- Van der Molen, Tweede Kamer, vergaderjaar 2018/19, 30821, nr. 60; Motie Kuiken en Verhoeven, Tweede Kamer, vergaderjaar 2018-2019, 32 761, nr. 145.

⁹ <https://www.rijksoverheid.nl/actueel/nieuws/2019/03/11/campagne-nepnieuws-vandaag-van-start>; zie ook: Tweede Kamer, vergaderjaar 2018-2019, 30 821, nr. 51, p. 5; Tweede Kamer, vergaderjaar 2019-2020, 30821, nr. 91 (mede op basis van de tussenrapportage).

¹⁰ Moties Asscher/Van Der Molen, Tweede Kamer, 2018/19, 30821, nr. 61, nr. 62, nr. 68.

1. Welke huidige wet- en regelgeving bestaat er gericht op/gerelateerd aan het tegengaan van verspreiding van (des)informatie, en specifiek voor/door tech bedrijven?
2. Welke eisen stelt de wet- en regelgeving aan de verspreiding van informatie? Zijn deze techniekonafhankelijk beschreven?
3. Hoe houdt de huidige wet- en regelgeving rekening met de transparantie van de herkomst van informatie op sociale mediaplatforms? Worden hier grenzen gesteld aan eventuele buitenlandse invloeden, bijv. t.a.v. het plaatsen van politieke advertenties (motie Asscher/Vd Molen)?
4. Welke toezichtmogelijkheden en sanctionering biedt de wet- en regelgeving ten aanzien van online manipulatie (motie Asscher/Vd Molen, 62)?
5. Zou bewuste online manipulatie onder de delictsomschrijvingen in het strafrecht inzake het manipuleren van verkiezingen kunnen worden gebracht? (motie Asscher- Van der Molen, Kamerstukken II, 2018/19, 30821, nr. 68).
6. Welke betekenis heeft de rechtsvorm voor de maatregelen die techbedrijven kunnen of moeten nemen t.a.v. content-moderatie, bevorderen van transparantie en bescherming rechten van burgers? Wat is de verantwoordelijkheid van techbedrijven voor de verspreiding via hun zoekmachines, sociale platforms e.d.?
7. Hoe zijn de rechten van burgers beschermd tegen bewuste misleidende informatie? Ook in het kader van gebruik van persoonsgegevens (privacy) en vrijheid van meningsuiting (ook t.a.v. verwijderen van content).

In plaats van “techbedrijven” wordt in dit onderzoek de term “internetdiensten” gebruikt. Juridisch gaat het om diensten van de informatiemaatschappij, elektronische communicatiediensten of audiovisuele mediadiensten. Dit omvat, onder andere, alle bekende sociale mediadiensten en de *direct messaging* diensten.

Omdat zoals gezegd vele andere landen in de afgelopen jaren al maatregelen getroffen hebben in het kader van desinformatie, is het de moeite waard om de keuzes die in deze landen zijn gemaakt te analyseren, om te kunnen bezien wat passend kan zijn voor de Nederlandse context. Daarom is als deel van het onderzoek een landenstudie uitgevoerd, waarbij de volgende landen zijn meegenomen: het Verenigd Koninkrijk, Frankrijk, Duitsland, Zweden, de Verenigde Staten, en Canada. De aanpak van desinformatie in deze landen zijn bekeken vanuit de mogelijkheid om de specifieke keuzes die in deze landen zijn gemaakt in te passen in het Nederlandse juridisch kader. De landenstudies zijn als bijlagen bij het rapport opgenomen. Door het rapport heen zal waar relevant aan de landenstudies gerefereerd worden.

D. Tussenrapportage: desinformatie en politieke advertenties

Dit onderzoek is in twee fases uitgevoerd. De eerste fase, en de behorende tussenrapportage, spitte zich toe op de eerste drie onderzoeksvragen en in het bijzonder de specifieke problematiek van politieke advertenties.¹¹ De aanvullende vraag die in de tussenrapportage centraal stond was wat het reguleringskader voor de verspreiding van politieke advertenties via internetdiensten is, en wat de mogelijkheden zijn met betrekking tot regulering (transparantie in het bijzonder) in het licht van de geldende normatieve kaders en de landenstudies. Deze huidige eindrapportage bouwt nadrukkelijk voort op de resultaten van de tussenrapportage en, hoewel dit rapport desinformatie in de volle breedte bespreekt, wordt de problematiek van desinformatie in relatie tot politieke advertenties nog integraal meegenomen.

De focus voor de tussenrapportage op politieke advertenties weerspiegelt dat de aanpak van desinformatie in het algemeen vaak wordt gekoppeld aan de mogelijke regulering van online politieke advertenties.

¹¹ Deze tussenrapportage is inmiddels gepubliceerd als bijlage bij de brief aan de Tweede Kamer van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, ‘Beleidsinzet bescherming democratie tegen desinformatie’, dd. 18 oktober 2019.

Ook in Nederland zijn stemmen opgegaan tot nieuwe regulering, in het bijzonder met betrekking tot online politieke advertenties.¹² Het idee is dat de advertentieproducten van internetdiensten een aan desinformatie gerelateerde problematiek faciliteren. De mogelijkheid gerichte en softwarematig gestuurde politieke campagnes te voeren, zonder de begrenzing door landsgrenzen of andere bij traditionele media geldende beperkingen, creëert openingen voor oneigenlijke beïnvloeding van het democratische proces. Online politieke advertenties kunnen bijvoorbeeld aan desinformatie raken wanneer er sprake is van oneigenlijke inmenging in het nationale politieke proces door buitenlandse actoren. Vervolgens roept ook het creëren van gerichte politieke advertenties (*“micro-targeting”*) vragen op over de mogelijkheid dat middels data-gestuurde campagnes het politieke debat op individueel niveau wordt gemanipuleerd. Echter, hoewel de verspreiding en impact van online politieke advertenties gerelateerd kan zijn aan de bredere problematiek van desinformatie, moeten de beide fenomenen zowel in praktische, als juridische zin onderscheiden worden. Daarom behandelt deze eindrapportage de problematiek rond desinformatie in de volle breedte, waarbij alle zeven onderzoeksvragen aan bod komen.

E. Opzet van de studie

Er is voor gekozen de studie om de structuur van het wettelijk kader te volgen. Binnen deze structuur lenen de onderzoeksvragen zich ervoor om in de loop van de rapportage heen beantwoord te worden. Waar noodzakelijk zal in de conclusies expliciet stilgestaan worden bij de beantwoording van een specifieke vraag.

Deze rapportage heeft de volgende structuur. Allereerst zullen een aantal cruciale begrippen gedefinieerd worden. In **hoofdstuk 2** zal het begrip “desinformatie” worden ontleed aan de hand van het geldend juridisch kader, beschikbare wetenschappelijke literatuur, rapporten en beleidsstukken. Vervolgens, in **hoofdstuk 3**, zal worden stilgestaan bij de verscheidenheid aan internetdiensten (tech bedrijven) die in de discussie over de problematiek van de verspreiding van desinformatie de aandacht behoeven. Het gaat hier om een breed scala aan verschillende diensten, waaronder sociale media, zoekmachines en communicatiediensten. In deze rapportage is de keuze gemaakt voor het gebruik van de term internetdiensten, in plaats van de term “tech bedrijven”. Na deze conceptuele inkadering van de centrale begrippen, geeft de rapportage inzicht in het voor Nederland geldende relevante juridisch kader voor de aanpak van desinformatie. Dit zal opgedeeld worden in drie delen. Eerst wordt stilgestaan bij de grondrechtelijke normering op Nederlands en Europees niveau (**hoofdstuk 4**), ten tweede wordt het Europeesrechtelijk geldende kader voor internetdiensten besproken (**hoofdstuk 5**) om ten derde een overzicht te bieden van de specifieke wetgeving en (zelf-)regulering in Nederland (**hoofdstuk 6**). Bij de bespreking van het Europeesrechtelijk kader wordt tevens aandacht besteed aan de relevante beleidsontwikkelingen op Europees niveau ten aanzien van desinformatie.

In het laatste deel van de rapportage worden de inzichten die de uitgevoerde analyse van de problematiek en het juridisch kader bieden op een rij gezet en met elkaar in verbinding gebracht (**hoofdstuk 7**). Daarbij worden ook de inzichten uit de landenstudies meegenomen. Deze landenstudies zijn opgenomen als bijlage. Afsluitend worden de relevante conclusies die uit het onderzoek volgen samenvattend besproken om te komen tot een eindconclusie met betrekking tot de onderzoeksvragen (**hoofdstuk 8**).

12 Motie Asscher- Van der Molen, Tweede Kamer, vergaderjaar 2018-2019, 30821, nr. 68; Motie Kuiken en Verhoeven, Tweede Kamer, vergaderjaar 2018-2019, 32 761, nr. 145; Motie Asscher en Buitengeweg, Tweede Kamer, vergaderjaar 2018-2019, 35 078, nr. 21; Staatscommissie parlementair stelsel, *‘Lage Drempels, Hoge Dijken. Democratie en rechtstaat in balans’* Den Haag, 2018, p. 18.

2. Desinformatie

- Desinformatie is 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;
- De term desinformatie is nuttig als beleidsterm maar niet als juridisch begrip.
- Het omvat veel bestaande juridische categorieën (illegaal & onrechtmatig) maar ook ongereguleerde schadelijke uitingen;
- Verschillende actoren zijn betrokken: de maker, het verspreidingsmedium en het publiek;
- De verspreiding wordt technologisch versterkt (micro-targeting / astroturfing etc.)
- Desinformatie komt in verschillende contexten voor met telkens unieke problematiek: o.a. nieuws, hate-speech, commercieel en politieke campagnes.

A. Conceptuele inkadering

Het begrip desinformatie (in het Engels: “disinformation”) is momenteel in beleidskringen het leidende begrip geworden onder de noemer waarvan een breed scala aan problemen op het gebied van de informatiekwaliteit en het medialandschap aangeduid worden. Het is de term die vanuit wetenschappelijk en normatief oogpunt de voorkeur verdient boven problematischeren termen zoals “nepnieuws”.¹³ Het blijft daarbij van groot belang, zeker in het geval van beleidsmaatregelen en/of nieuwe vormen van regulering, dat het begrip desinformatie en de onderliggende problematiek helder worden gedefinieerd, ingekaderd en empirisch onderbouwd. Deze conceptuele inkadering zal in deze sectie besproken worden, waarna ingegaan wordt op zowel de feitelijke problematiek als de verschillende contexten waarin desinformatie relevant is.

i. Definities

In de relevante literatuur is een verscheidenheid aan definities en beschrijvingen van desinformatie voorhanden. De volgende benaderingen zijn in het bijzonder invloedrijk geweest in het bieden van een conceptueel kader voor de problematiek.

In het rapport *Information Disorder* voor de Raad van Europa presenteren Wardle en Derakhshan een breed conceptueel kader waarin zij onderscheid maken tussen de begrippen desinformatie, misinformatie, en malinformatie. Ze benadrukken het belang van een onderscheid tussen juiste en onjuiste berichten, tussen berichten die gecreëerd, geproduceerd of verspreid worden door actoren die daarmee schade willen aanrichten, en berichten waarvoor dat niet het geval is. De door Wardle en Derakhshan gekozen specifieke definities luiden als volgt:

- “Dis-information. Information that is false and deliberately created to harm a person, social group, organization or country.
- Mis-information. Information that is false, but not created with the intention of causing harm.
- Mal-information. Information that is based on reality, used to inflict harm on a person, organization or country.”¹⁴

De Europese Commissie in haar mededeling uit 2018 getiteld “Bestrijding van online-desinformatie: een Europese benadering” kiest voor een verwante maar bredere definitie. De Commissie definieert

¹³ Zie McGonagle 2018. Zie ook McGonagle e.a. 2018.

¹⁴ Wardle, C., & Derakhshan, H. ‘Information Disorder. Toward an interdisciplinary framework of research and policymaking’, z.p., 2017 p. 20.

desinformatie als “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.”¹⁵ Twee opvallende verschillen zitten in de rol die de opzet van de actor speelt en of *economisch gewin* van belang is. De definitie van Wardle en Derakhshan vereist namelijk dat desinformatie altijd gecreëerd is met de opzet schade aan te richten. Terwijl in de definitie van de Commissie deze intentie daarentegen alleen een rol speelt wanneer het gaat om het bedriegen van het publiek en niet zodra er sprake is van economisch gewin. De definitie van de Commissie vereist slechts dat de informatie feitelijk onjuist of misleidend is om te kwalificeren als desinformatie waar Wardle en Derakhshan winstbelang in het geheel niet meenemen. De definitie van Commissie vormt in dit opzicht een duidelijke uitbreiding van het concept desinformatie. Onder de Commissie definitie vallen namelijk ook onjuiste of misleidende commerciële advertenties en onjuiste nieuwsberichten terwijl deze niet onder de definitie van Wardle en Derakhshan vallen. De waarde van een dergelijk brede definitie kan er in gelegen zijn dat de definitie erkent hoe het commerciële succes van onjuiste informatie mogelijk kwalitatief betere informatie naar de achtergrond drukt. De Commissie hanteert dezelfde definitie in de EU praktijkcode tegen desinformatie.¹⁶

De definitie van de Commissie is gebaseerd op de onafhankelijke door de Europese Commissie ingestelde High Level Expert Group (“HLEG”). Het rapport uit januari 2018, *“A multi-dimensional approach to disinformation”*, spreekt over “false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.”¹⁷ Hier speelt opzet dus ook geen rol zodra er economische overwegingen in spel zijn. Daarnaast voegt de HLEG hier nog aan toe dat debatten over “nepnieuws” “een spectrum van informatietypen omvatten”. Zij omvatten: “Vormen met een relatief laag risico, zoals eerlijke fouten van verslaggevers, politiek partijdige retoriek en het gebruik van “clickbait”-koppen, en vormen met een hoog risico, zoals bijvoorbeeld buitenlandse staten of binnenlandse groepen die het politieke proces in de Europese lidstaten en de Europese Unie zouden proberen te ondermijnen door het gebruik van verschillende vormen van kwaadwillige verzinsels, infiltratie van *grassroots* groepen en geautomatiseerde amplificatietechnieken”.¹⁸ Een recent verschenen rapport van Wardle bevat een uitvoerige bespreking van de verschillende vormen van desinformatie op een spectrum van “low harm” zoals satire en parodie tot “high harm” zoals gefabriceerde informatie.¹⁹

De *European Broadcasting Union* kiest voor een definitie die dicht bij die van Wardle en Derakhshan ligt. In hun position paper wordt desinformatie gedefinieerd als “inaccurate information [...] which is presented, promoted or disseminated by one or more actors in the chain with the intention to cause harm or make a profit.”²⁰ Verder bieden Bayer et al. in een recente studie van februari 2019 voor de LIBE-commissie van het Europees Parlement een gebalanceerde definitie waarin desinformatie benaderd wordt als fenomeen gekarakteriseerd door specifieke elementen. Desinformatie is informatie (i) ontworpen om foutief, manipulatief of misleidend te zijn, (ii) met de intentie om onzekerheid te creëren, sociale cohesie te verstoren, haat aan te wakkeren of om het democratische proces te ontwrichten, (iii) betreffende een onderwerp van maatschappelijk belang en (iv) veelal verspreid via geautomatiseerde technieken om de impact te vergroten.²¹ De nadruk die in deze definitie wordt gelegd op de methode van verspreiding is voornamelijk interessant.

15 Europese Commissie, ‘Bestrijding van online-desinformatie: een Europese benadering’, COM(2018) 236 final, par. 2.1. <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018DC0236&from=EN>

16 Europese Commissie, ‘EU praktijkcode tegen desinformatie’, preambule, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

17 HLEG, ‘A multi-dimensional approach to disinformation’, p. 10.

18 Idem.

19 Wardle, C. ‘Understanding Information Disorder’, First Draft, October 2019.

20 European Broadcasting Union, ‘Position Paper: Fake News and the Information Disorder’, 2018, https://www.ebu.ch/files/live/sites/ebu/files/Publications/Position%20papers/EBU-Position-EN-Fake_News_Disinformation-18.04.2018.pdf.

21 Bayer, J., et al., ‘Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States’, 2019, European Union, p. 18.

De door de Nederlandse overheid gehanteerde definitie van desinformatie is nauwer dan de definitie van de Europese Commissie. In de recente kamerbrief waar de regering haar beleidsinzet met betrekking tot desinformatie uiteenzet wordt desinformatie gedefinieerd als “het doelbewust, veelal heimelijk, verspreiden van misleidende informatie, met het doel om schade toe te brengen aan het publieke debat, democratische processen, de open economie of nationale veiligheid.”²² Opvallend aan deze definitie ten opzichte van de definitie van de Europese Commissie is dat slechts misleidende informatie onder de definitie valt en niet ook onjuiste (maar mogelijk niet misleidende) informatie. Verder ontbreekt het winstelement, hetgeen bijvoorbeeld betekent dat *clickbait* niet onder de definitie van de Nederlandse overheid valt, maar wel onder de definitie van de Europese Commissie.

Duidelijk is dat er geen éénduidige juridische kwalificatie van het concept desinformatie bestaat. Evenwel zijn er een aantal aspecten te identificeren die consistent in alle definities terugkomen: (i) de informatie moet **onjuist** of **misleidend** zijn. Verder (ii) komt in elke definitie ook het element **maatschappelijke schade** terug. Het is niet steeds helder of goed uitgewerkt welke rol dit schade criterium speelt. Moet de informatie daadwerkelijk schadelijk zijn, of is de intentie om op schadelijke wijze informatie te verspreiden voldoende? Verder is ook onduidelijk wat deze schadelijkheid inhoudelijk betekent. De Europese Commissie spreekt over “schade in het publieke domein” terwijl Wardle en Derakhshan kijken naar schade aan een persoon, sociale groep, organisatie of een land. In ieder geval blijft onduidelijk wat hier exact onder verstaan wordt. Deze breed en vaag gedefinieerde concepten van schade leveren een duidelijk spanningsveld op met de vrijheid van meningsuiting, waar immers in beginsel ook de publicatie en verspreiding van foutieve informatie door beschermd wordt.²³ Desinformatie is het doelbewust, veelal heimelijk, verspreiden van misleidende informatie, met het doel om schade toe te brengen aan het publieke debat, democratische processen, de open economie of nationale veiligheid.

Verder speelt ook (iii) de **intentie** of **opzettelijkheid** van de actor in elke definitie een rol. Echter, er bestaat ook hier geen eensgezindheid over het object van deze intentie. Bij de definitie van de HLEG moet de intentie zien op het aanbrengen van “public harm”, en ook bij de definitie van Wardle en & Derakhshan moet de opzet zien op het berokkenen van schade, terwijl bij de Commissie de opzet moet zien op het bedriegen van het publiek. Ten slotte (iv) speelt het **economisch gewin** van de actor veelal een rol, hoewel het geen onderdeel vormt van de definitie van Wardle en Derakhshan.

Dit onderzoek sluit aan bij de definitie van de Europese Commissie zoals geformuleerd in de Mededeling uit 2018: desinformatie is “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.”²⁴ Vanuit het oogpunt van beleidsvorming verdient het de voorkeur om deze gezaghebbende definitie te volgen waar men zich veelal in lijkt te kunnen vinden.²⁵ Waar nodig zal deze definitie verder gekwalificeerd worden langs de lijnen van de hierboven genoemde vier factoren, in het bijzonder ten aanzien van de maatschappelijke schade en de intentie van de actor. De specifieke invulling van voornamelijk deze twee factoren is namelijk bepalend voor een juridische kwalificatie in een concreet geval. Er is voor gekozen om de brede Europese definitie te volgen, en niet de meer beperkte Nederlandse definitie, omdat een analyse op basis van een bredere Europese definitie een meer omvattend beeld geeft van het regulatoire landschap. Om dezelfde reden wordt hieronder ook de keuze gemaakt om illegale uitingen en *hate speech* onder desinformatie te laten vallen waar veel onderzoeken dit niet doen.²⁶ Naast deze algemene definitie van desinformatie die de Europese Commissie hanteert, zal in dit rapport ook gebruik gemaakt worden van de driedeling van Wardle en Derakhshan. Aan hun

²² Tweede Kamer, 2019-2020, 30 821 nr. 91, dd. 18 oktober 2019 (kamerbrief) p. 3.

²³ Zie voor een bespreking: Tarlach McGonagle, ‘De Raad van Europa en online desinformatie: laveren tussen zorgen en zorgplichten?’, Mediaforum 2018-6, 180-184.

²⁴ Idem.

²⁵ Idem, p. 22; Marsden, C. & Meyer, T., ‘Regulating disinformation with artificial intelligence’, European Union, 2019.

²⁶ Zie paragraaf 2.A.ii.

definitie van desinformatie zal gerefereerd worden als “desinformatie in enge zin” en aan de definitie van de Europese Commissie als “desinformatie” of “desinformatie in brede zin”.

Desinformatie is “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.”²⁷

ii. Reikwijdte: type uitingen & juridische kwalificatie

Naast het feit dat er geen eenduidige juridische definitie voorhanden is, is ook duidelijk dat er bij iedere definitie een breed spectrum aan vormen van communicatie onder het begrip vallen. Zelfs wanneer slechts informatie in een digitale context in ogenschouw wordt genomen, omvat het begrip desinformatie een grote verscheidenheid aan media- en communicatievormen. Zo vallen onder de definitie van de Europese Commissie uitingen variërend van commerciële reclames, politieke betogen, nieuwsartikelen, medische claims, complottheorieën, blog posts, politieke advertenties, tot e-mails, posts op sociale media, vlogs en privéberichten via media zoals WhatsApp, Telegram of Facebook.

Deze verschillende verschijningsvormen hebben ook wijd uiteenlopende juridische kwalificaties. Veel van de uitingen die onder de noemer van desinformatie vallen, worden al wettelijk gereguleerd. In de eerste plaats kan hierbij gedacht worden aan de illegale en dus strafrechtelijk vervolgbare uitingen zoals smaad, laster, belediging, en bepaalde vormen van verkiezingsfraude. Vervolgens zijn er de onrechtmatige, via de privaatrechtelijke weg te adresseren, uitingen zoals misleidende reclames, oneerlijke handelspraktijken, inbreuken op intellectuele eigendomsrechten of onrechtmatige perspublicaties. In de derde plaats kan ook worden gedacht aan publiekrechtelijk gereguleerde uitingen zoals de verschillende reclame verboden en de mediaregulering in het algemeen.

Hoewel veel van de uitingen die onder het begrip desinformatie vallen dus al wettelijk gereguleerd worden, geldt dit niet in alle gevallen. Cruciaal hierbij is het onderscheid tussen illegale en onrechtmatige informatie enerzijds, en schadelijke informatie anderzijds. Hoewel deze begrippen vaak in één zin genoemd worden is het voor het juridisch kader van belang het onderscheid helder voor ogen te hebben.²⁸ Zoals uit het voorgaande blijkt zijn illegale en onrechtmatige informatie beide bij wet gesanctioneerd, waar schadelijke informatie dat in beginsel niet is. Bij illegale informatie is sprake van de overtreding van een strafrechtelijk verbod. Onrechtmatige informatie leidt tot privaatrechtelijke aansprakelijkheid of maatregelen. Daar staat tegenover dat schadelijke informatie niet wettelijk gereguleerd is en onder de bescherming van de vrijheid van meningsuiting valt. Met schadelijke informatie wordt veelal verwezen naar zaken die, hoewel binnen de grenzen van de wet, als maatschappelijk onwenselijk worden gezien. Hierbij kan gedacht worden aan gefabriceerde complottheorieën, extreme politieke denkbeelden, foutieve medische theorieën zoals bij de antivaccinatie beweging of misleidende nieuwsberichten. Benaadrukt moet worden dat veel van deze uitingen, die niet gereguleerd zijn maar wel als schadelijk ervaren worden, niet gereguleerd worden omdat ze in principe onderdeel vormen van een gezond maatschappelijk debat waar ook ruimte moet zijn voor foutieve informatie die beschermd wordt door de vrijheid van meningsuiting.²⁹ Onder de paraplu van desinformatie worden dus uitingen gebracht die wettelijk gereguleerd of verboden zijn maar ook ongereguleerde uitingen die de bescherming van het recht op vrijheid van meningsuiting genieten. Het begrip omvat hiermee zowel de klassieke leerstukken, ingekaderd door

²⁷ Idem.

²⁸ Zie bijvoorbeeld UK Government, ‘Online Harms White Paper’, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

²⁹ Zie verder hoofdstuk 4.

gedetailleerde jurisprudentie, zoals smaad en onrechtmatige perspublicaties, als niet genormeerde fenomenen zoals complottheorieën of foutieve persberichten.

In de literatuur wordt deze brede juridische classificatie niet altijd gevolgd. De HLEG sluit bijvoorbeeld expliciet alle illegale of onrechtmatige informatie uit van desinformatie,³⁰ om het concept verder aan te scherpen.³¹ Ook in de LIBE-studie van Bayer *et al.* valt *hate speech* bijvoorbeeld buiten de definitie van desinformatie, voornamelijk om de scope van het onderzoek te beperken.³² In dit rapport wordt wel expliciet de hierboven uiteengezette brede scope gehanteerd. Dit in de eerste plaats nu de onderzoeksvragen ook expliciet verlangen dat de juridische dimensies geduid worden en in de tweede plaats omdat deze brede discussie van desinformatie noodzakelijk is om te zien hoe verschillende rechtsgebieden en huidige reguleringsinstrumenten in elkaar grijpen of waar juist gaten vallen. Dit is ook waarom, zoals eerder uiteengezet, in deze rapportage de brede definitie van desinformatie gevolgd wordt.

De mogelijke aanpak en handhavinginstrumenten zijn afhankelijk van de juridische kwalificaties van het onderliggend handelen. Een complicerende factor in het een en ander is nog dat een daadwerkelijke vaststelling of sprake is van illegale en/of onrechtmatige informatie door daarvoor aangewezen instanties in veel gevallen niet plaatsvindt en eventuele acties ten aanzien van deze informatie door relevante diensten worden genomen op basis van de gebruiksvoorwaarden. Dit gegeven hangt uiteraard nauw samen met de wijze waarop desinformatie feitelijk verspreid wordt en zijn impact heeft.

iii. Actoren

Een van de definiërende eigenschappen van de problematiek rond desinformatie is de grote verscheidenheid van de betrokken actoren. Volgens Wardle en Derakhshan is de betrokkenheid van verschillende actoren in verschillende stadia van de verspreiding van desinformatie één van de drie kernelementen van desinformatie.³³ Wardle en Derakhshan onderscheiden drie fases: de creatie van de desinformatie, de productie waar de boodschap in een mediaproduct gevormd wordt en ten derde de verspreiding of distributie van de informatie.³⁴ In deze drie fases zijn verschillende actoren relevant: de maker of opdrachtgever tot de desinformatie, het medium via welke de desinformatie verspreid wordt en het publiek dat de desinformatie ontvangt en verder verspreidt.

De eerste categorie is de maker of opdrachtgever voor de desinformatie. Dit is de actor die, volgens de definitie van desinformatie, de intentie heeft om maatschappelijke schade aan te richten en moedwillig foutieve of misleidende informatie verspreidt. Zo breed als de problematiek zelf zijn ook de mogelijke actoren die achter de desinformatie kunnen zitten. Het kunnen bijvoorbeeld individuen, *trolls*, politieke partijen, statelijke actoren, maatschappelijke belangenorganisaties of commerciële bedrijven zijn.³⁵ Dit onderscheid is voornamelijk relevant nu de middelen die de verschillende partijen ter beschikking staan zeer wisselend zijn en de mogelijke regulering afgestemd moet zijn op de desbetreffende actor; dezelfde maatregelen voldoen niet voor een commercieel bedrijf en een statelijke actor. In de literatuur wordt veel aandacht besteed aan desinformatiecampagnes ontworpen door statelijke actoren, nu deze potentieel

30 HLEG, 'A multi-dimensional approach to disinformation', p. 12.

31 Volgens Renda, A., 'The legal framework to address "fake news": possible policy actions at the EU level' Policy Department for Economic, Scientific and Quality of Life Policies, 2018, p. 12.

32 Bayer, J. e.a., 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States', European Union, 2019, p. 16, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

33 Wardle, C., & Derakhshan, H. 'Information Disorder. Toward an interdisciplinary framework of research and policymaking', z.p., 2017 p. 25.

34 *Ibid.* P. 23.

35 HLEG, 'A multi-dimensional approach to disinformation', p. 10.

zeer veel impact kunnen hebben en vanuit democratisch perspectief bijzondere zorgwekkend kunnen zijn.³⁶ Een ander type actor dat in deze categorie geplaatst kan worden zijn de zogenaamde *trolls* die - al dan niet in opdracht - desinformatie verspreiden, om verdeeldheid te creëren en reacties uit te lokken.³⁷ Deze *trolls* zijn "(1) human accounts that post politically motivated, generally pro-government content, often for a fee, or (2) human accounts that post provocative (generally "anti-PC") content, often with graphic language and misogynistic content, either out of political conviction or simply for the "thrill" of doing so".³⁸ Om een maker van desinformatie correct te kunnen plaatsen kan nog gebruikt gemaakt worden van vijf factoren opgesteld door Wardle en Derakhshan: het type actor (statelijk, commercieel, politieke partij ect.), de organisatiegraad, motivatie, doelgroep desinformatie (nationaal, internationaal, specifieke etnische groep etc.) en het gebruik van geautomatiseerde technologie.³⁹ De European Association for Viewers Interests ("EAVI") heeft als mogelijke motivatiebronnen voor desinformatie geïdentificeerd: geld, politieke invloed, humor en passie of ideologische overtuiging.⁴⁰ Een van de grote uitdagingen met betrekking tot de maker van desinformatie is niet alleen dat de groep heel divers is, maar ook dat de misleiding juist vaak zit in wie de maker is. Misleiding ten aanzien van de spreker is één van de belangrijkste middelen die wordt ingezet bij desinformatie. Desinformatie wordt namelijk veelal verspreid onder een valse naam, door bijvoorbeeld valse accounts.⁴¹

Een tweede in de context van dit onderzoek zeer belangrijke actor is het kanaal via welke de desinformatie verspreid wordt. Binnen de reikwijdte van dit onderzoek zijn dit specifiek internetdiensten zoals platforms, *direct messaging* diensten of zoekmachines. Deze diensten, die gekenmerkt worden door een gebrek aan klassieke redactionele controle, faciliteren in veel gevallen ook de verspreiding van desinformatie via de kanalen voor gesponsorde inhoud. Deze kanalen zijn van belang omdat desinformatiecampagnes veelal op basis van dezelfde logica opereren als de klassieke advertentie industrie: het doel is om de aandacht van mensen zo lang mogelijk vast te houden en hun gedrag te beïnvloeden ten aanzien van een specifiek doel.⁴² Naast het gebruik van de gesponsorde kanalen, wordt desinformatie echter ook veelal verspreid via het reguliere kanaal van een dergelijke internetdienst. Het beleid van internetdiensten ten aanzien van advertenties of het gebruik van het reguliere kanaal kan hiermee dus zeer van invloed zijn op de mogelijkheden die de makers van desinformatie ter beschikking staan om desinformatie te verspreiden.

Vervolgens is een zeer cruciale actor voor de verspreiding van desinformatie het algemene publiek en de reguliere gebruikers van internetdiensten. De Europese Commissie geeft aan dat het feit dat de desinformatie op grote schaal door nietsvermoedende gebruikers gedeeld wordt een uniek aspect van de problematiek is.⁴³ Het algemene publiek is enerzijds de ontvanger en de doelgroep van de desinformatie, maar door de inrichting van de verschillende internetdiensten zijn zij in de meeste gevallen ook de verspreiders

36 Jeangène Vilmer, J.B. et. al, 'Information Manipulation: A Challenge for Our Democracies', Ministry for Europe and Foreign Affairs and the Ministry for the Armed Forces, 2018, p. 46-63, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf; Wardle, C., & Derakhshan, H. 'Information Disorder. Toward an interdisciplinary framework of research and policymaking', z.p., 2017 p. 30.

37 Phillips, W. 'This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture', MIT Press 2015.

38 Tucker, J. et al., 'Social media, political polarization and political disinformation: a review of the scientific literature'. Hewlett Foundation, March 2018, p. 8, <https://hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf>

39 Wardle, C., & Derakhshan, H. 'Information Disorder. Toward an interdisciplinary framework of research and policymaking', z.p., 2017 p. 25.

40 EAVI, 'Beyond 'fake news' 10 types of misleading news', 2017 https://eavi.eu/wp-content/uploads/2017/07/beyond-fake-news_COLOUR_WEB.pdf;

41 Camille François, 'Actors, Behaviours, Content: A Desinformation ABC. Highlighting three vectors of viral deception to guide industry & regulatory responses', Transatlantic working group, september 20, 2019.

42 Bayer, J. e.a., 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States', European Union, 2019, p. 31, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf); Ghosh, D., & Scott, B., 'Digital Deceit. The Technologies Behind Precision Propaganda on the Internet', 2018, p. 4 <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/>.

43 Europese Commissie, 'Mededeling: Bestrijding online desinformatie – een Europese aanpak' COM(2018) 236 definitief, p. 6. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>.

van de betreffende informatie door het te delen, liken, retweeten of anderszins.⁴⁴ Dit wordt ook wel het “participatoire karakter” van desinformatie genoemd, en vormt een van de grote uitdagingen voor de mogelijke aanpak van desinformatie.⁴⁵

Uit de verhoudingen tussen deze verschillende actoren blijkt ook hoe zeer de problematiek rond desinformatie samenhangt met de feitelijke technologische verspreidingsmiddelen. Dit vormt dan ook het aanknopingspunt om de conceptuele inkadering van desinformatie af te sluiten en over te stappen op de wijze waarop desinformatie in de praktijk verspreid wordt en wat de feitelijke maatschappelijke invloed is.

B. Problematiek en feitelijke situatie

Na deze conceptuele inkadering van het begrip desinformatie, op basis waarvan helder is hoe breed en veelomvattend het concept is, is het van belang de daadwerkelijke problematiek verder te duiden. In de eerdergenoemde mededeling uit 2018 identificeert de Europese Commissie een zestal mogelijke schadelijke gevolgen van de grootschalige verspreiding van desinformatie. Als belangrijkste is het gevaar dat desinformatie (i) het vertrouwen in de media vermindert en zo ook in onze democratie “doordat de burgers minder in staat zijn weloverwogen beslissingen te nemen.” Door deze invloed op de media kan desinformatie (ii) een impact hebben op de vrijheid van meningsuiting doordat mensen gelimiteerd worden in hun vrije informatiegaring. Ook kan het leiden tot (iii) verminderd vertrouwen in de wetenschap en (iv) grotere populariteit van radicale en extremistische ideeën en activiteiten. Vervolgens is desinformatie ook problematisch in een internationale context. Het kan door buitenlandse actoren ingezet worden (v) om specifieke maatschappelijke debatten te beïnvloeden of zelfs (vi) om het nationale verkiezingsproces te beïnvloeden en de nationale veiligheid in gevaar te brengen.⁴⁶

Deze schadelijke gevolgen komen niet direct voort uit de desinformatie als zodanig, maar voornamelijk door de grootschalige verspreiding ervan via internetdiensten.⁴⁷ Hier kan ook de verklaring gevonden worden voor de huidige politieke aandacht voor het fenomeen. Het soort uitingen zelf zijn over het algemeen geen nieuwe ontwikkeling. Dit blijkt al duidelijk uit het feit dat veel van de zaken die onder het begrip vallen al lang gereguleerd zijn. Het op grote schaal wegvallen van redactionele controle, alsmede de schaal waarop en de snelheid van de verspreiding van onjuiste of misleidende informatie, gemedieerd door internetdiensten en veelal versterkt door geautomatiseerde verspreidingsmethodes zijn daarentegen wel nieuw.⁴⁸ De snelle online verspreiding door middel van de normale kanalen van bijvoorbeeld sociale media, of artificieel versterkt door middel van geautomatiseerde bots maakt dat het veelal moeilijk is vast te stellen waar de desinformatie vandaan komt.⁴⁹ Op deze wijze vormen internetdiensten de centrale spil die een mediërende en faciliterende rol spelen in de verspreiding van desinformatie. Hierdoor zijn internetdiensten en de wijze waarop deze diensten vormgegeven worden, cruciaal voor de verspreiding en mogelijke impact van desinformatie.⁵⁰

44 Bayer, p. 35.

45 Asmolov G., ‘*The Disconnective Power of Disinformation Campaigns*’, Journal of International Affairs 71(1.5): Columbia, 18 September 2018, <https://jia.sipa.columbia.edu/disconnective-power-disinformation-campaigns>

46 Europese Commissie, ‘Tackling online disinformation: a European Approach, COM(2018) 236 final’, par. 2.2.

47 Vilmer, J-B. et al., ‘Information Manipulation: A Challenge for Our Democracies’, p. 39; Marsden, C. & Meyer, T., ‘Regulating disinformation with artificial intelligence’, European Union, 2019 p. 8.

48 Neudert, L.M.N., ‘Computational Propaganda in Germany: A Cautionary Tale’, Computational Propaganda Working Paper, 2017.7, Oxford: Oxford Internet Institute; Rogers, R., & Niederer, S. ‘The politics of social media manipulation: A view from the Netherlands’, 2019, p. 17; Bayer, J., et al., ‘Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States’, 2019, European Union, p. 22.

49 Bayer J. e.a., ‘Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States’, European Union, 2019, p. 30, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

50 Rogers, R., & Niederer, S. ‘*The politics of social media manipulation: A view from the Netherlands*’, 9 april 2019, p. 17.

In haar mededeling identificeert de Commissie drie categorieën van methodes die de verspreiding van desinformatie faciliteren:

- *“Op basis van algoritmen: (...) Doordat het delen van gepersonaliseerde inhoud onder gelijkgestemde gebruikers wordt gefaciliteerd, kunnen algoritmen indirect polarisatie vergroten en versterken ze de effecten van desinformatie;*
- *Op basis van reclame: het huidige model voor digitale reclame werkt vooral op basis van muiskliks, waardoor sensationele en virale inhoud wordt aangemoedigd. Het berust op reclamenetwerken die worden beheerd door agentschappen die zorgen voor real-time plaatsing van advertenties op basis van algoritmische besluitvorming. Daardoor worden gemakkelijker advertenties geplaatst op websites met sensationele inhoud die op de emoties van de gebruikers inspeelt, en op websites met desinformatie;*
- *Op basis van technologie: onlinetechnologieën zoals automatische diensten (“bots” genoemd) versterken kunstmatig de verspreiding van desinformatie. Deze mechanismen kunnen verder worden versterkt met gesimuleerde profielen (nepaccounts) waarachter geen authentieke gebruiker schuilgaat, die soms op enorme schaal worden georkestreerd (“troll factories” genoemd).”⁵¹*

Met betrekking tot de verspreiding van desinformatie op basis van reclame wordt zoals hiervoor al aangegeven gebruik gemaakt van de kanalen en technieken aangeboden door internetdiensten voor commerciële reclames (bijvoorbeeld gesponsorde content door middel van *real time bidding*), en wordt ook op basis van dezelfde logica geopereerd. Commerciële reclame en desinformatie hebben immers beide tot doel de aandacht van mensen te grijpen en hun gedrag te beïnvloeden.⁵² Zoals aangegeven hebben de verspreiders van desinformatie en sommige internetdiensten belangen die in elkaars verlengde liggen. Het feit dat de verspreiding van desinformatie via internetdiensten opereert op basis van dezelfde logica als de onlineadvertentie-industrie is ook deels een verklaring voor het succes van de verspreiding van desinformatie via deze diensten.⁵³

Ook wat betreft de verspreiding op basis van algoritmen maakt desinformatie dankbaar gebruik van de structuur van veel internetdiensten, voornamelijk sociale media, die er baat bij kunnen hebben voorrang te geven aan gepersonaliseerde of sensationele informatie. De verspreiders van desinformatie maken zo gebruik (of misbruik) van de organische verspreidingsmethodes via deze internetdiensten. Een voorbeeld hiervan is zoekmachineoptimalisatie waarbij de algoritmes op basis waarvan zoekresultaten weergegeven en gerangschikt worden, gemanipuleerd worden om bepaalde (des)informatie, het meest zichtbaar te maken.⁵⁴ Daarentegen kan bij het gebruik van bots en nepaccounts eerder gesteld worden dat misbruik gemaakt wordt van de structuur van een bepaalde internetdienst. Een voorbeeld van dergelijke technieken is *astroturfing*. Hierbij worden bots of nepaccounts ingezet om de schijn van een breed maatschappelijk draagvlak of van een *grassroots* beweging te creëren. Het achterliggende doel is veelal economisch gewin of het bevorderen van een politiek standpunt.⁵⁵ Deze drie categorieën methodes om de verspreiding van desinformatie te faciliteren brengt Neudert alle onder de noemer van “computationale propaganda”: “the assemblage of social media, autonomous agents and algorithms tasked with the

51 Europese Commissie, COM(2018) 236 final, par. 2.2.

52 Bayer, J. e.a., ‘Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States’, European Union, 2019, p. 31, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf); Ghosh, D., & Scott, B., ‘Digital Deceit. The Technologies Behind Precision Propaganda on the Internet’, 2018, p. 4 <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/>.

53 Ghosh, D., & Scott, B., ‘Digital Deceit. The Technologies Behind Precision Propaganda on the Internet’, 2018, p. 4 <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/>.

54 Bayer, J. e.a., ‘Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States’, European Union, 2019, p. 31, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

55 Zie Leiser, M., ‘Astroturfing, ‘CyberTurfing’ and other online persuasion campaigns’, European Journal of Law and Technology 2016, p. 2.

manipulation of opinion.”⁵⁶ Methodes die hieronder vallen zijn de genoemde micro-targeting, bots, troll fabrieken, astroturfing en zoekmachineoptimalisatie.⁵⁷

Uit dit overzicht van de verschillende technologisch gemedieerde en manipulatieve manieren waaruit desinformatie verspreid wordt, blijkt uit ook duidelijk de connectie met het begrip onlinemanipulatie. Het probleem van desinformatie hangt samen met nieuwe vormen van online manipulatie die de laatste tijd onder de aandacht zijn gekomen van onderzoekers en beleidsmakers. De Europese Commissie legt een specifiek verband tussen manipulatie en desinformatie, aangezien de desinformatie zich verspreidt door het manipulatieve gebruik van de infrastructuur van online platforms..⁵⁸ Wetenschappers hebben online manipulatie gedefinieerd als het gebruik van informatietechnologie “[to] covertly influence another person’s decision-making,” en online manipulatieve praktijken als toepassingen van informatietechnologie “[that] impose hidden influences on users, by targeting and exploiting their vulnerabilities”.⁵⁹ Een vorm van schade die door online manipulatie wordt veroorzaakt, is de ondermijning van de beslissingsbevoegdheid en de autonomie van een individu.⁶⁰ De essentiële elementen van problematische online manipulatie liggen besloten in de verborgen aard van de beïnvloeding en het spelen met de kwetsbaarheid van een persoon. Het Comité van ministers van de Raad van Europa (COM) heeft zich ook gericht op het subliminale karakter van online manipulatie. In de 2019 *Declaration on the Manipulative Capabilities of Algorithmic Processes*, maakt de COM een onderscheid tussen “permissible persuasion” en “unacceptable manipulation”. *Manipulation* is een vorm van beïnvloeding die “subliminal, exploits existing vulnerabilities or cognitive biases, and/or encroaches on the independence and authenticity of individual decision-making”.⁶¹ De COM wijst op de gevaren voor de democratische samenlevingen van online manipulatie en de omstandigheid dat online manipulatie wordt vergemakkelijkt door technologiebedrijven, met inbegrip van het feit dat zij niet alleen in staat zijn om keuzes te voorspellen, maar ook “[to] influence emotions and thoughts and alter an anticipated course of action, sometimes subliminally”.⁶² Dit kan ook de manipulatie van politiek gedrag omvatten. In het licht van dit gevaar benadrukt de COM dat de regelgevingskaders met betrekking tot politieke communicatie en verkiezingsprocessen moeten worden beoordeeld om de eerlijkheid en integriteit van verkiezingen zowel on- als offline te waarborgen overeenkomstig de gevestigde beginselen. Er moet met name voor worden gezorgd dat de kiezers toegang hebben tot vergelijkbare informatie over het gehele politieke spectrum. Daarnaast moeten kiezers bewust worden van de gevaren van politieke *redlining*, die zich voordoen wanneer politieke campagnes beperkt blijven tot degenen die het meest waarschijnlijk worden beïnvloed. Tot slot dienen kiezers doeltreffend te worden beschermd tegen oneerlijke praktijken en manipulatie.

Deze problematiek rondom desinformatie geniet ook in de Nederlandse context veel aandacht.⁶³ Wat betreft de feitelijke situatie in Nederland, is recentelijk door Rogers en Niederer onderzoek gedaan naar desinformatie en “junknieuws” op sociale media in Nederland. Dit onderzoek levert geen bewijzen op voor buitenlandse desinformatiecampagnes rondom de Provinciale Staten- en Europese parlementsverkiezingen van 2019. Wel bleek dat de Nederlandse mediasfeer in toenemende mate gepolariseerd is en ook dat zogenaamd “junknieuws” wijdverspreid is met betrekking tot kwesties zoals Zwarte Piet, MH17, het klimaat en de Europese Unie.⁶⁴ De term “junknieuws” die in het onderzoek gehanteerd wordt

56 Neudert, L.M.N., ‘Computational Propaganda in Germany: A Cautionary Tale’, Computational Propaganda Working Paper, 2017.7, Oxford: Oxford Internet Institute, p. 1.

57 Rogers, R., & Niederer, S. ‘The politics of social media manipulation: A view from the Netherlands’, 2019, p. 17.

58 European Commission, ‘Tackling online disinformation: a European Approach’, p. 2.

59 Susser, D., Roessler, B., Nissenbaum, H., ‘Online Manipulation: Hidden Influences in a Digital World’, Georgetown Law Technology Review, Forthcoming 2019, p. 24, <https://ssrn.com/abstract=3306006>.

60 Idem, p. 2.

61 Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, Decl(13/02/2019)1, par. 9.

62 Idem.

63 Zie bijvoorbeeld Tweede Kamer, vergaderjaar 2018-2019, 30821, nr. 51; Kamerbrief van de Minister van Justitie en Veiligheid, 21 december 2018, 2285167, ‘Aanpak online hate speech’.

64 Rogers, R., & Niederer, S. ‘The politics of social media manipulation: A view from the Netherlands’, 9 april 2019, p. 16; Howard, P.H. e.a., ‘Junk news and bots during the U.S. election: What were Michigan voters sharing over Twitter?’ Computational Propaganda Data Memo, Oxford: Oxford Internet Institute.

is breder dan de hier gehanteerde definitie van desinformatie en omvat ook sensationele informatie, click-bait en politiek sterk gekleurde uitingen, die niet verspreid wordt met de intentie maatschappelijke schade te veroorzaken.⁶⁵ Verder concludeert een onderzoek van het Rathenau Instituut in 2018 dat, voor alsnog, desinformatie geen grote negatieve impact op de Nederlandse samenleving heeft gehad.⁶⁶ Daarnaast is uit recent onderzoek voor het Commissariaat voor de Media ook gebleken dat de problematiek ten aanzien van door algoritmische processen versterkte “filter bubbels” in Nederland niet wijdverspreid is, hoewel er wel aanleiding is om de invloed van filtering technologieën op het medialandschap nauw in de gaten te houden. Het Nederlandse publiek maakt nog in overwegende mate gebruik van kanalen die nieuws aanbieden die niet via algoritmes gefilterd zijn.⁶⁷

C. Context van desinformatie

Aangezien desinformatie een breed scala aan onderwerpen omvat, is het waardevol verschillende vormen van desinformatie in een concrete context te plaatsen. Desinformatie wordt zo vaak gezien in verband met de verspreiding van nieuws, of junknieuws, in relatie tot *hate speech* en extremistische uitingen, gekoppeld aan commerciële uitingen en in de context van oneigenlijke buitenlandse invloeden. Dit zijn zeer verschillende contexten die allen een unieke maatschappelijke en beleidsmatige problematiek met zich meebrengen en een eigen verhouding tot de vrijheid van meningsuiting hebben.⁶⁸ Zo worden commerciële uitingen in mindere mate beschermd,⁶⁹ terwijl politieke uitingen, waaronder ook politieke advertenties, op de grootst mogelijke bescherming van de vrijheid van meningsuiting mogen rekenen.⁷⁰ *Hate speech* daarentegen, valt deels buiten de bescherming⁷¹ en ten aanzien van het medialandschap heeft de staat significante positieve verplichtingen tot bescherming van de pluriformiteit en de vrije nieuwsgaring.⁷² Wanneer over mogelijke regulering “van desinformatie” gesproken wordt is dus van belang om helder te hebben in welke specifieke context desinformatie besproken wordt. Aangezien de tussenrapportage zich toespitste op de relatie tussen desinformatie en politieke advertenties, worden deze apart in sectie 2.D besproken.

i. Desinformatie en nieuws

Veel van de discussie over en het bestaande onderzoek met betrekking tot desinformatie spitst zich toe op de productie, verspreiding en toegang tot nieuws. Dit is logisch gezien de cruciale rol die een vrije, onafhankelijke en kwalitatief hoogwaardige media speelt voor het functioneren van een democratie. Pluralisme en vrije nieuwsgaring zijn noodzakelijk voor het democratisch proces en de vrees is dat de verspreiding van desinformatie via nieuwsartikelen dit ondermijnt door, onder andere, het algemene vertrouwen in de media te ondergraven. Desinformatie in verband met nieuws wordt vaak aangeduid als “nepnieuws”. Deze term is echter in onderzoek en beleidskringen in onbruik geraakt. Dit is in de eerste plaats het geval omdat de problematiek die er mee geïd werd breder is dan slechts nieuws en beter gedekt wordt door de term desinformatie. In de tweede plaats is de term sterk geassocieerd met politieke en historische strategieën om journalisten in diskrediet te brengen.⁷³ Zoals hierboven besproken is

⁶⁵ Rogers, R., & Niederer, S. *The politics of social media manipulation: A view from the Netherlands*, 2019, p. 4 & p. 16.

⁶⁶ Keulen, I. van e.a. *Digitalisering van het nieuws—Online nieuwsgedrag, desinformatie en personalisatie in Nederland*, 2018, Den Haag: Rathenau Instituut.

⁶⁷ Moeller, J., Helberger, N. & Makhortykh, M., *Filterbubbels in Nederland* Instituut voor Informatierecht, 2019.

⁶⁸ Zie verder hoofdstuk 4.

⁶⁹ Markt intern Verlag GmbH and Klaus Beermann v. Germany, 20 November 1989; Krone Verlag GmbH & Co. KG v. Austria (No. 3), 11 December 2003, r.o. 31; artikel 7 lid 4 Grondwet.

⁷⁰ TV Vest As & Rogaland Pensjonistparti v. Noorwegen (no. 21132/05) 11 December 2008, r.o. 59.

⁷¹ Seurot v Frankrijk (no. 57383/00) 18 mei 2004.

⁷² Huseynova v. Azerbaijan (Application no. 10653/10) 13 April 2017, r.o. 120; and Dink v Turkey (Application nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09) 14 September 2010, r.o. 137.

⁷³ Wardle, C., & Derakhshan, H. 'Information Disorder. Toward an interdisciplinary framework of research and policymaking', z.p., 2017 p. 6; HLEG, 'A multi-dimensional approach to disinformation', p. 10; EBU, 'Position Paper: Fake news and the information disorder', 2018, p. 6; McGonagle, T. e.a., 'Inventarisatie methodes om “nepnieuws” tegen te gaan', Instituut voor Informatierecht, 2018, p. 10-11; Darnton, R., 'The True History of Fake News, New York Review of Books; Bayer J. e.a., 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States', European Union, 2019, p. 24, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

een andere term die wordt gebruikt om deze diverse problematiek van desinformatie in de context van nieuws te duiden "junk nieuws".⁷⁴

Er is veel literatuur voorhanden op het raakvlak van desinformatie en nieuws. Een breed spectrum aan nieuwsvormen zijn hierbij relevant, van blogposts, tabloid nieuws tot onderzoeksjournalistiek. Waar het steeds om gaat is dat berichtgeving zich voordoet als een betrouwbare bron van nieuws terwijl het eigenlijk een vorm van desinformatie betreft. Zie hiervoor bijvoorbeeld de definitie van McGonagle *et al.*: "Informatie die opzettelijk is gefabriceerd en verspreid met de intentie anderen te bedriegen en te misleiden om onwaarheden te geloven of controleerbare feiten in twijfel te trekken; het is desinformatie die als nieuws wordt gepresenteerd of waarschijnlijk als nieuws zal worden gezien."⁷⁵

Wat betreft de verschillende nieuwsvormen die hier onder kunnen vallen maakten Tandoc *et al.* in 2017 een typologie van alle definities van "nepnieuws" die in de afgelopen 15 jaar in omloop waren. De categorieën zijn nieuwsparodie, gefabriceerd nieuws, nieuwssatire, gemanipuleerde foto's, reclame en propaganda.⁷⁶ In hetzelfde jaar ontwikkelde EAVI een invloedrijke "infographic" waar verschillende typen misleidend nieuws in tien categorieën opgedeeld worden om vervolgens geanalyseerd worden naar motivatie en invloed. De tien categorieën die EAVI onderscheidt, zijn: propaganda, click-bait, gesponsorde content, satire en hoax, foutief nieuws, activistische berichtgeving, complottheorieën, pseudowetenschap, verkeerde informatie en onzin.⁷⁷ Ook Wardle geeft aan dat het van belang is de verschillende nieuwsuitingen die aan desinformatie kunnen relateren van elkaar te onderscheiden. Zij stelt de volgende categorieën voor: satire of parodie, misleidende informatie, oplichting, gefabriceerde informatie, gefingeerde connecties, valse context of gemanipuleerde informatie.⁷⁸ Vervolgens kan het rapport van de HLEG in herinnering gebracht worden waar benadrukt werd dat "nepnieuws" een spectrum van informatietypes omvat, die op een schaal van laag naar hoog risico geplaatst kunnen worden.⁷⁹ Wat duidelijk naar voren komt uit al deze verschillende typologieën is opnieuw hoe breed de problematiek is, zelfs wanneer toegespitst wordt op desinformatie in de context van het nieuws. Ook valt opnieuw op dat de verschillende verschijningsvormen ook uiteenlopende juridische kwalificaties kennen. Satire en parodie worden bijvoorbeeld expliciet beschermd door de vrijheid van meningsuiting.⁸⁰

Voor de empirische situatie in Nederland met betrekking tot de verspreiding van junk nieuws en de maatschappelijke invloed kan weer verwezen worden naar de studie van Rogers *et al.* en het onderzoek van het Rathenau Instituut waaruit bleek dat Nederland een in toenemende mate gepolariseerd medialandschap kent met brede verspreiding van junk nieuws, maar dat de impact op de Nederlandse samenleving tot nu toe beperkt lijkt.⁸¹

74 Tommaso, V. 'From Fake to Junk News, the Data Politics of Online Virality', in: Bigo, D. Isin, E. & Ruppert, E. (eds), 'Data Politics: Worlds, Subjects, Rights', London: Routledge, 2019, . <https://hal.archives-ouvertes.fr/hal-02003893>; Howard, P.H. e.a., 'Polarization, Partisanship and Junk News Consumption on Social Media During the 2018 US Midterm Elections' 2018, COMPROP Data Memo, Oxford: Oxford Internet Institute.

75 T. McGonagle e.a., 'Inventarisatie methodes om "nepnieuws" tegen te gaan', Instituut voor Informatierecht, 2018, p. 12 onder verwijzing naar: the Ethical Journalism Network: <http://ethicaljournalismnetwork.org/tag/fake-news>.

76 Edson, C. e.a., 'Defining "Fake News"', 2018, Digital Journalism.

77 EAVI, 'Beyond "fake news" 10 types of misleading news', 2017 https://eavi.eu/wp-content/uploads/2017/07/beyond-fake-news_COLOUR_WEB.pdf; T. McGonagle e.a., 'Inventarisatie methodes om "nepnieuws" tegen te gaan', Instituut voor Informatierecht, 2018, p. 8.

78 Wardle, C., 'Fake News. It's Complicated', <https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79>.

79 HLEG, 'A multi-dimensional approach to disinformation', p. 10.

80 Eon v. France, 14 March 2013; Kuliś and Różycki v. Poland, 6 October 2009; Alves da Silva v. Portugal, 20 October 2009. Vereinigung Bildender Künstler v. Austria, 25 January 2007

81 Rogers, R., & Niederer, S. 'The politics of social media manipulation: A view from the Netherlands', 2019, p. 4 & p. 16; Keulen, I. van e.a. 'Digitalisering van het nieuws—Online nieuwsgedrag, desinformatie en personalisatie in Nederland', 2018, Den Haag: Rathenau Instituut, p. 4.

ii. Desinformatie en *hate speech*

Vervolgens wordt de verspreiding van desinformatie via internetdiensten ook veelal gekoppeld aan de verspreiding van *hate speech*.⁸² Desinformatie kan immers zelf ook kwalificeren als *hate speech* en de combinatie van deze dynamiek in de praktijk kan buitengewoon gevaarlijk en schadelijk zijn. Opvallend is dat de HLEG in haar studie *hate speech* expliciet uitsluit van het begrip desinformatie. Zoals eerder aangegeven gaat de HLEG zelfs zo ver om alle vormen van illegale of onrechtmatige uitingen van desinformatie uit te sluiten.⁸³ Ook Bayer *et al.* betrekken *hate speech* expliciet niet in hun onderzoek. Ze sluiten het niet uit van de definitie van desinformatie zelf, slechts van de scope van hun onderzoek.⁸⁴ Wardle en Derakhshan beschouwen in hun rapport *hate speech* niet als onderdeel van desinformatie, maar scharen het onder misinformatie. Dit omdat bij *hate speech* doorgaans een op de werkelijkheid gebaseerd feit (bijvoorbeeld huidskleur, sekse, seksuele oriëntatie of geloofsovertuiging) gebruikt wordt om iemand te schaden.⁸⁵ De Commissie spreekt zich niet expliciet uit op dit punt, maar betreft wel nadrukkelijk ook illegale en onrechtmatige uitingen in haar definitie van desinformatie.⁸⁶

Hoewel het feit dat *hate speech* niet even consistent betrokken is in onderzoeken met betrekking tot desinformatie is het van belang de problematiek van desinformatie expliciet vanuit het perspectief van *hate speech* te bezien. Het is juist dit perspectief dat goed blootlegt hoe complex de juridische problematiek is en voor welke uitdagingen eventuele aanvullende regulering komt te staan. De grens tussen illegale of onrechtmatige *hate speech* enerzijds, en slechts schadelijke uitingen of schokkende uitingen anderzijds, is immers notoir moeilijk te trekken. Dit gecombineerd met de snelle verspreiding op schaal via internetdiensten maakt dat de combinatie van *hate speech* en desinformatie in een online context een bijzondere uitdaging vormt.

iii. Desinformatie en commerciële uitingen

Ook wordt niet altijd expliciet stil gestaan bij de koppeling tussen desinformatie en commerciële belangen, terwijl juist deze koppeling één van de grootste uitbreidingen vormt van het concept desinformatie in de definitie van de Europese Commissie. Bij deze koppeling moet gedacht worden aan de commerciële belangen van degene die de desinformatie verspreid (zie ook de rol van “economisch gewin” in de definitie van de Europese Commissie), maar ook aan de commerciële belangen van de internetdiensten die de verspreiding mediëren. De twee zijn nauw aan elkaar verbonden nu desinformatie verspreid kan worden voor commercieel gewin gebruikmakend van de gesponsorde kanalen van veel sociale media bedoeld voor commerciële reclame. Op deze manier zijn de onlineadvertentie-industrie en de verspreiding van desinformatie nauw aan elkaar gekoppeld.⁸⁷ Het is voornamelijk relevant om deze koppeling met commerciële belangen expliciet te maken, omdat het maakt dat regulering met betrekking tot handelspraktijken in het algemeen en commerciële advertenties in het bijzonder van toepassing kan zijn. Dit type regulering is specifiek voor de commerciële context, en vaak ook alleen van toepassing als er sprake is van handelspraktijken gericht op consumenten. Het is daarentegen bijvoorbeeld niet van toepassing op desinformatie in de context van nieuws-verspreiding en journalistiek.

82 L. Reppell & E. Shein, ‘Disinformation Campaigns and Hate Speech: Exploring the relationship and Programming Interventions’ International Foundation for Electoral Systems, 2019, https://www.ifes.org/sites/default/files/2019_ifes_disinformation_campaigns_and_hate_speech_briefing_paper.pdf; Khaliq, Nahid, ‘Striking a Balance: Hate Speech, Freedom of Expression and Non-Discrimination’, Tolley’s Journal of Media Law and Practice, vol. 15, no. 1, 1994, p. 27-28, <https://heinonline.org/HOL/P?h=hein.journal>.

83 HLEG, ‘A multi-dimensional approach to disinformation’, p. 10.

84 Zie ook de inleiding van dit rapport.

85 Wardle, C., & Derakhshan, H. ‘Information Disorder. Toward an interdisciplinary framework of research and policymaking’, z.p., 2017 p. 20.

86 Europese Commissie, ‘Bestrijding van online-desinformatie: een Europese benadering’, COM(2018) 236 final, par. 2.1. <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018DC0236&from=EN>

87 Tambini, D. (2017) How advertising fuels fake news. LSE Media Policy Project Blog, <http://blogs.lse.ac.uk/mediapolicyproject/2017/02/24/how-advertising-fuels-fake-news/>

iv. Desinformatie en buitenlandse invloeden

Er is momenteel bijzondere aandacht voor desinformatie en buitenlandse invloed, en volgens de Europese Commissie worden massale online desinformatiecampagnes gebruikt door “buitenlandse” actoren, “buitenlandse” regeringen en “derde landen”.⁸⁸ Het doel van deze campagnes is wantrouwen te wekken en maatschappelijke spanningen in landen te creëren, politieke beslissingen in de EU te beïnvloeden, het beleid te manipuleren, maatschappelijke debatten te voeren en deel uit te maken van hybride bedreigingen van de binnenlandse veiligheid, waaronder verkiezingsprocessen.⁸⁹ Zo zijn er op nationaal en Europees niveau beleidsdiscussies gaande over hoe desinformatie van buitenaf tegen te gaan en wordt er specifiek aandacht besteed aan buitenlandse invloed en discussie. In Nederland bijvoorbeeld is desinformatie door buitenlandse actoren een expliciet onderdeel van het nationale veiligheidsbeleid.⁹⁰ Zoals besproken in hoofdstuk 4, zijn er in het verleden periodes geweest waarin de angst voor buitenlandse invloed op de voorgrond trad, ook in verband met desinformatie en propaganda, en dat er lange discussies zijn geweest over de vrijheid van meningsuiting, met name in de periode van de Koude Oorlog. Dit geldt met name voor de omroepsector ten aanzien van het blokkeren van uitzendingen al vele jaren.

Gezien deze hernieuwde aandacht voor het *buitenlandse* element van desinformatie, worden in de “Joint Declaration on Fake News, Disinformation and Propaganda”, twee specifieke grondbeginselen in het kader van de internationale normen inzake de vrijheid van meningsuiting met betrekking tot de buitenlandse invloed herhaald: ten eerste wordt de vrijheid van meningsuiting gegarandeerd “regardless of frontiers” en beperken de normen inzake de vrijheid van meningsuiting de beperkingen, niet alleen binnen een rechtsgebied, “but also those which affect media outlets and other communications systems operating from outside of the jurisdiction of a State as well as those reaching populations in States other than the State of origin”.⁹¹ Ten tweede is het blokkeren van uitzendingen van een in een andere jurisdictie gevestigde omroeporganisatie of het intrekken van de heruitzendrechten voor de programma’s van die organisatie legitiem “only where the content disseminated by that broadcaster has been held by a court of law or another independent, authoritative and impartial oversight body to be in serious and persistent breach of a legitimate restriction on content”.⁹²

Binnen de internationale mensenrechtennormen is er dus zeer weinig ruimte om de verspreiding van informatie aan te pakken uitsluitend op grond van het feit dat deze van *buitenlandse* oorsprong is. Elke beperking van informatie uit het buitenland moet voldoen aan de zeer strenge toets van de normen voor de vrijheid van meningsuiting waarin de wet voorziet, een van de legitieme belangen dienen die in het internationale recht worden erkend en noodzakelijk en evenredig zijn voor de bescherming van dat belang.

D. Desinformatie en politieke advertenties

Binnen het huidige diverse debat over desinformatie is de specifieke kwestie van “politieke advertenties” een prominent onderdeel van het beleidsdebat geworden. Zo heeft de Europese Commissie in haar mededeling van 2018 getiteld “Communication on *Tackling online disinformation: a European Approach*”, de problematiek van desinformatie en politieke advertenties met elkaar in verband gebracht. De Europese Commissie betoogt dat onlineplatforms niet voldoende informatie maken over “the use of strategic dissemination techniques, such as paid human influencers and/or robots to market

⁸⁸ European Commission, ‘*Tackling online disinformation: a European Approach*’, COM(2018) 236 final, par. 1 & 3.5.

⁸⁹ Tweede Kamer, 2019-2020, 30 821 nr. 91, dd. 18 oktober 2019 (kamerbrief) p. 4.

⁹⁰ Kamerstukken II 2018/19, 30821, nr. 72.

⁹¹ United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint declaration on freedom of expression and “fake news”, disinformation and propaganda*, FOM.GAL/3/17, 3 March 2017, par. 1c.

⁹² Idem, par. 1h.

messages”, en dat zij niet “sufficient transparency on political advertising and sponsored content” hebben geboden.⁹³ De Europese Commissie heeft aanbevolen dat onlineplatforms “[need to s]ignificantly improve the scrutiny of advertisement placements, notably in order to reduce revenues for purveyors of disinformation, and restrict targeting options for political advertising”, en “[e]nsure transparency about sponsored content, in particular political and issue-based advertising”.⁹⁴ Wat bots betreft, moeten onlineplatforms “clear marking systems and rules” vaststellen om verwarring met menselijke interacties te voorkomen.⁹⁵

De Mededeling van 2018 bevat echter geen definitie van politieke advertenties en een aantal verschillende soorten geld-gestuurde methoden om politieke communicatie te verspreiden, zoals betaalde *influencers*, het gebruik van bots, gesponsorde inhoud, (gerichte) politieke advertenties en issue-based advertising, worden samengevoegd maar niet uitgelegd. Verder wordt in de Mededeling eerst een onderscheid gemaakt tussen politieke advertenties en gesponsorde inhoud, maar later worden politieke advertenties en issue-based advertising als voorbeelden van gesponsorde inhoud genoemd. Toch is uit de Mededeling niet duidelijk wat het precieze verband is tussen het specifieke probleem van de desinformatie en de politieke advertenties. Om die reden is het belangrijk om aan te geven wat kan worden verstaan onder politieke advertenties die door internetdiensten worden vergemakkelijkt of uitgevoerd. Omdat politieke advertenties noodzakelijkerwijs een *politieke* inhoud hebben, moet bij elke mogelijke regulering van politieke advertenties rekening worden gehouden met de omstandigheid dat politieke advertenties rechtmatig worden gebruikt door politieke partijen.

Politiek in het begrip politieke advertenties en politieke communicatie kan verschillende betekenissen hebben. Politiek kan in de enge zin van het woord worden opgevat als een verwijzing naar de communicatie van politieke partijen, met name tijdens de verkiezingen. In de engste zin zou dit betekenen dat politieke advertenties kandidaten voor verkiezingen promoten.. In bredere zin bestaan politieke advertenties uit betaalde politieke communicatie over kwesties van openbaar belang, bijvoorbeeld door middel van wat ook wel “issue ads” worden genoemd. Met name dit onderscheid is niet alleen een kwestie van inhoud, maar ook van de verscheidenheid aan betrokken actoren. Terwijl verkiezingsadvertising waarschijnlijk worden gesponsord door specifieke politieke partijen en/of kandidaten zelf, zijn er bij betaalde politieke communicatie veel meer actoren betrokken die betalen om hun standpunten en politieke interventies effectief te verspreiden. Als gevolg daarvan houdt ongepaste beïnvloeding en manipulatie van het democratische debat hoogstwaarschijnlijk verband met de laatste en ruimere gedefinieerde vorm van betaalde politieke communicatie. Vanuit juridisch oogpunt moeten alle definities van politieke advertenties (in tegenstelling tot commerciële advertenties) gebaseerd zijn op de relevante normatieve verschillen in de jurisprudentie van het Europees Hof voor de Rechten van de Mens, die in detail worden besproken in hoofdstuk 4. De Commissie deelt deze mening.

Een eerste type betaalde politieke communicatie dat kan worden onderscheiden is *sponsored en promoted content*. Dit is een onderscheid dat gebaseerd is op het betaalde communicatiekanaal dat door bepaalde internetdiensten wordt aangeboden, naast het kanaal voor “organische” content. Een klassiek voorbeeld is een politieke partij die een advertentie maakt die de kiezers informeert over haar beleid en het advertentieplatform van Google (Google Ads) gebruikt om impressies te genereren voor bezoekers van websites in het Google Ads netwerk, zoals via Google Zoekresultaten of YouTube. Andere voorbeelden zijn het betalen voor gesponsorde tweets op Twitter, of een gesponsorde post op Instagram of Facebook.

93 Idem, par. 3.1.1.

94 Idem, par. 3.1.1.

95 Idem, par. 2.1.

Dit soort reclame is in zekere zin vergelijkbaar met *betaalde* politieke advertenties in kranten of op televisie, waarbij de krant of omroepen advertentieruimte verkopen aan een politieke partij of groepering. Een onderscheidend kenmerk van internetdiensten is echter dat zij het mogelijk maken om door middel van political microtargeting veel specifiekere gerichte maatregelen en instrumenten te ontwikkelen door “creating finely honed messages targeted at narrow categories of voters” op basis van een analyse van de gegevens die “garnered from individuals demographic characteristics and consumer and lifestyle habits”.⁹⁶ Facebook Audience van Facebook maakt het bijvoorbeeld mogelijk om advertenties te targeten op basis van leeftijd, geslacht, levensstijl, opleiding, relatiestatus, functie, online aankopen en locatie. Er is een verscheidenheid aan geavanceerde hulpmiddelen voor het bereiken van doelgroepen op platforms ontstaan, waaronder *look-a-like targeting*.⁹⁷ Naast de extra exposure die kan worden behaald door gebruik te maken van dergelijke diensten, voorzien zij ook in de mogelijkheid om extra meetgegevens te gebruiken voor de latere blootstelling van het publiek. Hierdoor wordt het voor adverteerders gemakkelijker om zich programmatisch te engageren en data-gestuurde evaluaties uit te voeren. Targeting kan ook gebruikt worden door overheden om bepaalde gemeenschappen en diaspora's uit het buitenland te bereiken.⁹⁸

Politieke partijen en de daarmee samenhangende campagne-operaties kunnen informatie van kiezers die zij verzamelen of waarvoor zij betalen, combineren met informatie afkomstig van internetdiensten. Hoewel dergelijke datagestuurde praktijken het politieke proces en de politieke participatie kunnen vergemakkelijken, hebben deze praktijken een aantal duidelijke vragen opgeroepen en de aandacht van de regelgevers getrokken. Zo heeft de Information Commissioner's Office in zijn onderzoek naar het Cambridge Analytica-schandaal gedetailleerd uiteengezet hoe de politieke partijen “marketing lists and lifestyle information from data brokers”, hadden gekocht en hadden gecombineerd met “electoral data sets they hold”.⁹⁹ De kwestie van microtargeting houdt dus niet alleen in dat er betaald moet worden voor de diensten die door onlineplatformen worden aangeboden, maar ook dat er gegevens moeten worden gekocht van databrokers die vervolgens worden gecombineerd met verkregen verkiezingsgegevens om vervolgens campagnes en communicatie te optimaliseren. Political microtargeting brengt een aantal specifieke regelgevingskwesties met zich mee, variërend van gegevensbescherming en privacy tot manipulatie, politieke participatie en het waarborgen van de integriteit van verkiezingen.¹⁰⁰

Ten tweede is er de politieke communicatie die zich als *organische inhoud* verspreidt. Bijvoorbeeld doordat een politieke partij zelf een campagnevideo maakt en deze op haar YouTube-kanaal publiceert, of een tweet van een eigen Twitter-account, of het posten van een campagneboodschap op Facebook. Cruciaal is dat bij politieke campagnes, met of zonder het gebruik van gesponsorde inhoud, bepaalde amplificatiestechnieken kunnen worden toegepast, die een groot en legitiem onderdeel vormen van moderne politieke campagnes. Bij *organisch* bereik verspreiden campagnevoerders hun boodschappen via Facebook, Instagram en Twitter, en moedigen campagnevoerders hun supporters aan om deze te delen met hun vrienden, familie en volgers. Sommige van deze praktijken zullen gepaard gaan met de inzet van financiële middelen om activiteiten van eindgebruikers te financieren en/of te betalen voor gespecialiseerde diensten, waarvan sommige door relevante internetdiensten als niet legitiem kunnen worden beschouwd of zelfs als onrechtmatig vanuit een juridisch perspectief, maar het is veel moeilijker

96 Gorton, W. 'Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy', New Political Science, 2016, <https://doi.org/10.1080/07393148.2015.1125119>, p. 61-80, p. 62; geciteerd in Zuiderveen Borgesius et al., 'Online Political Microtargeting: Promises and Threats for Democracy', Utrecht Law Review 2018.

97 Voor een bespreking van enkele van deze instrumenten en hoe ze tot discriminatie kunnen leiden, zie Amit, D., Makagon, J., Mulligan, D.C., & Tschantz, M.C., 'Discrimination in Online Personalization: A Multidisciplinary Inquiry' 2018, p. 20-34.

98 Zie Wong, S.L, Shepherd, C. & Liu, Q., 'Old messages, new memes: Beijing's propaganda playbook on the Hong Kong protests', Financial Times, 2019.

99 Information Commissioner's Office, 'Investigation into the use of data analytics in political campaigns: A report to Parliament' 2018, p. 24, <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>. Zie ook: Gibney, E. 'The scant science behind Cambridge Analytica's controversial marketing techniques', Nature, 2018, <https://www.nature.com/articles/d41586-018-03880-4>.

100 Zie de bespreking hieronder in deel 5(b) over de AVG.

om een onderscheid te maken tussen organische inhoud die gepaard gaat met betaling en “normale” organische inhoud.

Het optimaliseren van het organische bereik van relevante inhoud kan plaatsvinden door middel van een grote verscheidenheid aan technieken, instrumenten en praktijken. Botsoftware kan worden gebruikt, en over het gebruik van bots in politieke campagnes heeft de Britse verkiezingscommissie verklaard dat zij niet denkt “that there is anything wrong with campaigners using bots to post messages telling voters about their policies and political views”, of campagnevoerders die het personeel vertellen om campagneboodschappen te posten.¹⁰¹ Het wordt echter problematisch wanneer deze technieken worden gebruikt “[to] deceive voters about a campaigner’s identity or their true level of support, or used to abuse people”.¹⁰² Sommige jurisdicties hebben transparantieregels ingevoerd voor het gebruik van bots om een verkiezing te beïnvloeden.¹⁰³ Zoals Williams echter heeft opgemerkt, moeten goedbedoelde voorstellen voor transparantie in beide gevallen “zorgvuldig worden opgesteld”, anders kunnen ze zorgen voor “censorship and silence less powerful communities, threaten online anonymity, and the takedown of lawful human speech expression”.¹⁰⁴

Een voorbeeld van een problematische techniek is *astroturfen*, waarbij gebruik wordt gemaakt van social media bots, nepaccounts en betaalde trollen (of *influencers*) om campagneboodschappen te “versterken”, wat de “schijn van steun onder de bevolking” creëert, met als doel een campagne populair te maken onder het publiek.¹⁰⁵ *Astroturfen* is namelijk ontworpen om de valse indruk te wekken dat een campagne zich *organisch* heeft ontwikkeld.¹⁰⁶ Een belangrijke overweging bij het onderzoek naar astroturfen of andere vormen van bedrieglijke politieke communicatie is dan ook of de regels voor verkiezingsuitgaven van toepassing zijn, aangezien politieke partijen en groepen moeten aangeven hoe het geld wordt besteed aan het voeren van campagnes. Een daarmee samenhangende vraag is of astroturfen als een vorm van een politieke advertentie moet worden beschouwd en in de relevante regelgeving als zodanig moet worden gedefinieerd. Bij politieke advertenties hoeft het niet te gaan om een betaling aan een technologiebedrijf zoals Facebook of Twitter, maar het kan ook gaan om het betalen van anderen om een politieke boodschap te verspreiden en te versterken via bijvoorbeeld Facebook of Twitter.

Tot slot is een andere vorm van organische inhoud gewoonweg het *rechtstreeks* sturen van een politieke boodschap naar een bepaald individu, bijvoorbeeld via een *direct message* via een berichtendienst, zoals WhatsApp of Facebook Messenger. Dit kan onderdeel zijn van een virale politieke campagne, inclusief een politieke *crowdfunding*.¹⁰⁷ Sommige internetdiensten stellen gebruikers in staat om betalingen van andere gebruikers te innen, iets wat vrij populair is in bepaalde door gebruikers gecreëerde inhoudscategorieën zoals gaming, waardoor nieuwe verstrengelingen tussen online media en geld ontstaan.¹⁰⁸ Verder kunnen politieke berichten rechtstreeks via een berichtendienst worden verzonden via een valse account of door middel van het gebruik van een valse identiteit.

Gezien deze methoden van gesponsorde en organische inhoud, rijst de vraag wat als politieke advertentie kan worden aangemerkt. Vanuit juridisch oogpunt heeft het Europees Hof voor de Rechten van de Mens

101 The Electoral Commission, ‘Digital campaigning: Increasing transparency for voters’ 2018, par. 26, https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Digital-campaigning-improving-transparency-for-voters.pdf.

102 Idem.

103 Zie Country studies, deel 1(e) - United States.

104 Zie Williams, J., ‘Cavalier Bot Regulation and the First Amendment’s Threat Model’, Knight First Amendment Institute, 21 augustus 2019, <https://knightcolumbia.org/content/cavalier-bot-regulation-and-the-first-amendments-threat-model>.

105 Idem, par. 24.

106 Zie Leiser, M., ‘AstroTurfing, ‘CyberTurfing’ and other online persuasion campaigns’, 7 European Journal of Law and Technology 2016, p. 2; Electoral Commission, ‘Digital campaigning: Increasing transparency for voters’, 2018, p. 15.

107 International Institute for Democracy and Electoral Assistance, ‘Online Political Crowdfunding’, 2018, <https://www.idea.int/sites/default/files/publications/online-political-crowdfunding.pdf>.

108 Dergelijke betalingen kunnen zeer problematisch worden als ze worden veroorzaakt door illegale en schadelijke uitlatingen en communicatie, zoals *hate speech*.

("EHRM") de kwestie van *betaalde* politieke advertenties in zijn jurisprudentie op nuttige wijze onderzocht.¹⁰⁹ Het EHRM heeft weliswaar geen harde en snelle definitie vastgesteld, maar in plaats daarvan een brede kijk op wat een betaalde politieke advertentie is. Hieronder valt niet alleen een betaalde advertentie van een politieke partij die op zoek is naar stemmen, maar ook een betaalde advertenties van een campagnegroep over kwesties van algemeen belang. Het EHRM heeft benadrukt dat er niet is voldaan aan het *betaalde* element wanneer wordt een publicatie een gewone journalistieke uiting is.

Het cruciale element is dus het betalingsvereiste wat betekent dat gesponsorde content onder de definitie van politieke advertenties valt. De meer complexe vraag is hoe naar *organic content*, amplificatie- en virale campagnetechnieken moet worden gekeken. Deze kunnen alle ook in ruil voor betaling geschieden, bijvoorbeeld in de vorm van politiek campagnepersoneel, softwarediensten voor bots, of werknemers van "trol-fabrieken". Vervolgens is naast deze problematiek ook het klassieke onderscheid tussen redactionele en commerciële-inhoud moeilijker te maken door het gebrek aan redactionele controle aan de zijde van relevante internetdiensten. Het zou kunnen worden beargumenteerd dat dergelijke vormen van reclame slechts een extra manieren zijn om het publiek te bereiken, met extra tools en efficiëntie. Met andere woorden: reclameproducten van internetdiensten stellen gebruikers in staat om extra *exposure* te kopen, bovenop de mogelijkheden voor normale gebruikers van de dienst.

E. Samenvatting & Conclusie

Desinformatie is een breed en ingewikkeld begrip met veel verschillende definities in omloop. Alle definities omvatten echter in enigerlei vorm van (i) informatie die **onjuist** of **misleidend** is, (ii) informatie die **schade** veroorzaakt en (iii) de **bedoeling met betrekking tot** deze schade of de contra feitelijke aard van de informatie speelt een rol. Tot slot, (iv) speelt **economische winst** een belangrijke rol in de meeste definities. Door de definitie van de Europese Commissie te volgen, definieert dit verslag desinformatie als volgt:

Desinformatie is "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."¹¹⁰

Een van de complicerende aspecten van de verspreiding van desinformatie is de vele verschillende mogelijke actoren die hierbij betrokken kunnen zijn. In de eerste plaats lopen de verschillende actoren waar de desinformatiecampagne vandaan kan komen uiteen van een individu, tot een politieke partij, tot en met de overheidsactoren. Ten tweede speelt het kanaal waarlangs de desinformatie wordt verspreid, de internetdienst, een belangrijke rol in de impact die desinformatie kan hebben. Ten derde fungeert het publiek zowel als ontvanger van desinformatie als verspreider daarvan door de specifieke inhoud te waarderen of te delen. Ten vierde, kan de manier waarop traditionele en redactionele media reageren op bepaalde gevallen van desinformatie de impact ervan sterk beïnvloeden.

In dit alles spelen mogelijke vormen van sociaal-technische amplificatie van desinformatie een belangrijke rol. In veel gevallen is de desinformatie zelf niet de kern van het probleem, maar de grootschalige verspreiding via relevante internetdiensten, die doorgaans geen redactionele controle opleggen. Deze sociaal-technische amplificatie van desinformatie omvat een verscheidenheid aan technieken en processen, waaronder gebruikersactiviteit (liken, delen), data-gestuurde *targeting* en het gebruik van geautomatiseerde betrokkenheid via platforms (bots). Het gebruik van deze technologische en manipu-

¹⁰⁹ Zie hoofdstuk 4, voor een diepgaande discussie.

¹¹⁰ European Commission, 'Tackling online disinformation: a European Approach', COM(2018) 236 final, par. 3.1.1, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>.

latieve methoden maakt desinformatie nauw verbonden met het concept van online manipulatie, dat kan worden gedefinieerd als het gebruik van informatietechnologie om “heimelijk de besluitvorming van een ander te beïnvloeden”, en online manipulatieve praktijken zoals toepassingen van informatietechnologie die “verborgen invloeden opleggen aan gebruikers, door zich te richten op hun kwetsbaarheid”.

Desinformatie doorbreekt dus veel van de traditionele rechtsgebieden en kan, vanuit het perspectief van de inhoud van de communicatie, zowel schadelijke, onwettige als illegale inhoud bevatten. Het bestrijkt een breed scala aan verschillende uitdrukkingen die in verschillende bestaande juridische categorieën kunnen vallen. Zoals weergegeven in onderstaande tabel kan het brede scala aan verschillende soorten uitingen die desinformatie kunnen bevatten, vaak worden genuanceerd ten opzichte van een bestaande juridische categorie zoals laster of misleidende reclame, of vallen ze onder de categorie van schadelijke spraak die niet gereguleerd is.

Mogelijke juridische kwalificatie van desinformatie				
Gereguleerde spraak				vrije meningsuiting
Misleidende reclame	Onwettige perspublicatie	Direct messaging	Discriminatie	Onware nieuwsartikelen
Laster	Illegaal commercieel gedrag	Hate speech	Oneerlijke handelspraktijken	Samenzwerings-theorieën
Verkiezings-fraude	Intellectuele eigendom	Illegale gezondheids-claims		Hyper partisan speech
Soorten of uitdrukkingen				
Persoonlijk	Handels-praktijken	Nieuwsberichten	Politiek	reclame

Tabel 1

Bovendien wordt desinformatie als fenomeen meestal niet geïsoleerd besproken, maar in relatie tot een specifieke context. Met name desinformatie wordt besproken in relatie tot nieuws, haat zaaiende uitlatingen, commerciële communicatie, buitenlandse invloed of politieke advertenties. In elk van deze contexten heeft desinformatie een eigen logica en zijn er verschillende actoren bij betrokken. In het kader van deze studie is het van belang op te merken dat het toepasselijke wettelijke kader verschuift afhankelijk van de context waarin de desinformatie wordt besproken.

De algemene conclusie die uit deze analyse van het begrip desinformatie kan worden getrokken is dat het fenomeen breed is en dat het een groot aantal uitdrukkingsvormen bevat en een breed scala aan actoren raakt. Om die reden is het niet altijd mogelijk een precieze en duidelijke definitie te geven. Met name wat betreft de schade van desinformatie verschillen de huidige definities van elkaar en bevatten relatief vage en open termen als “maatschappelijke” of “publieke” schade. Om die reden moet “desinformatie” meer als een beleidsterrein dan als een juridische categorie worden beschouwd. Een tweede conclusie is dat het begrip desinformatie dwars door vele rechtsgebieden heen gaat en een grote groep van verder los van elkaar staande juridische categorieën omvat. Desinformatie heeft met name betrekking op uitdrukkingen die momenteel niet gereguleerd zijn en beschermd worden door het recht op vrijheid van meningsuiting. Ten derde laat de discussie over desinformatie duidelijk zien hoe het probleem en de mogelijke schade van desinformatie gelokaliseerd is in de grootschalige en sociaal-technologische verspreiding van informatie. Ten slotte is, omdat het concept zo breed is, veel verschillende actoren erbij betrokken zijn, voor een groot deel afhankelijk van individueel gedrag (delen, liken, etc.) en de maatschappelijke impact niet op alle punten duidelijk is, is empirisch onderzoek naar de verspreiding en prevalentie van desinformatie in Nederland noodzakelijk om de verdiensten van mogelijke beleidsopties goed te kunnen beoordelen.

3. Rechtspositie relevante internetdiensten (tech bedrijven)

- Juridische kwalificaties van internetdiensten die relevant zijn voor desinformatie zijn:
 - diensten van de informatiemaatschappij;
 - elektronische communicatiediensten; en
 - audiovisuele mediadiensten.
- Deze diensten hebben verschillende bedrijfsvormen: (i) opslag- en verspreidingsdiensten, (ii) diensten voor netwerken, collaboratieve productie en koppelingen, en (iii) diensten voor selectie, zoeken en verwijzingen.
- Onderscheid in handhavingsmodaliteit al naar gelang:
 - de vormgeving van de specifieke dienst;
 - het beleid van de dienst zelf; en
 - daadwerkelijke handhaving door de dienst.

De problematiek van desinformatie speelt met betrekking tot een breed scala aan verschillende internetdiensten. Zo kan er sprake zijn van de verspreiding van desinformatie via sociale media met een openbaar of semi-openbaar karakter, maar ook via nieuwe communicatiediensten met een besloten karakter zoals WhatsApp. Zoekmachines spelen ook een belangrijke rol op het gebied van de distributie en relatieve toegankelijkheid van informatie via internet, mede middels gesponsorde resultaten. Daarnaast zijn er online mediaplatformen, zoals YouTube, mediadiensten die op gamers zijn gericht, zoals Twitch, de recent bij jongeren populair geworden mobiele app TikTok, en discussieplatforms zoals Reddit en 4chan, die een belangrijke rol kunnen spelen in het populariseren van informatie en bij de verspreiding van desinformatie. Bij een specifieke focus op advertenties zijn daarnaast advertentiediensten van belang, in het bijzonder diensten die een rol spelen in de koppeling van aanbod van advertentieruimte op websites en adverteerders (advertentienetwerken).

Voor deze studie worden gezien hun gebrek aan, of zeer beperkte relevantie voor het vraagstuk van de aanpak van desinformatie een aantal internetdiensten buiten beschouwing gelaten. Zo wordt bijvoorbeeld niet stilgestaan bij infrastructurele diensten (zoals *cloud computing*), diensten op het gebied van domeinnamen, diensten voor het optimaliseren van de effectieve aflevering van online inhoud, diensten op het gebied van *cybersecurity*, de aanbieders van besturingssystemen of browser software, en de producenten van software en voor het internet relevante hardware.

A. Definiëring relevante internetdiensten

Vanuit juridisch perspectief geldt dat de relevante internetdiensten voor de beleidsproblematiek van desinformatie niet eenvoudig of eenduidig te positioneren zijn. Vanuit het perspectief van de aanpak van desinformatie en de regulering van politieke advertenties zijn de relevante juridische definities van verschillende internetdiensten te vinden op Europeesrechtelijk niveau. Het gaat specifiek om de volgende definities:

- diensten van de informatiemaatschappij. Hieronder vallen diensten die via internet een relevant aanbod leveren, bijvoorbeeld middels een website of mobiele applicatie;
- elektronische communicatiediensten;
- audiovisuele mediadiensten.

Daarbij geldt voor al deze diensten dat zij ook kunnen kwalificeren als internet tussenpersoon, in het bijzonder als internet *hosting of mere conduit* dienst. Hoewel er sprake is van relevante implementatiewetgeving in Nederland zijn er met betrekking tot deze definities geen relevante aanvullende of afwijkende Nederlandse bepalingen. Wel worden er naast deze juridische definities op Europees niveau beleidskaders voor online platformen ontwikkeld. Het gaat hier om een relatief rekbaar begrip dat nog geen duidelijke juridische inkadering kent maar wel, afhankelijk van de specifieke definitie die wordt gevolgd, de meeste van de voor desinformatie relevante internetdiensten omvat.

De richtlijn elektronische handel bevat het leidende juridische kader voor diensten van de informatiemaatschappij.¹¹¹ Dit kader bevat regels met betrekking tot de transparantie van commerciële communicatie, alsmede de regeling met betrekking tot de beperking van aansprakelijkheid van internet tussenpersonen.¹¹² Deze laatste regeling is van bijzonder belang gezien het feit dat veel van de relevante internetdiensten, gezien het gebrek aan redactionele controle, een beroep zullen kunnen (of in elk geval willen) doen op de beperking van aansprakelijkheid voor internet hosting diensten. Daarnaast zijn er diensten, zoals *instant messaging* diensten, die zullen gelden als elektronische communicatiediensten en als zodanig juridisch zijn ingekaderd op Europees niveau in de telecomunicatieregelgeving. Als laatste is vervolgens het juridisch kader voor audiovisuele diensten mede van toepassing op bepaalde voor desinformatie relevante internetdiensten zoals YouTube.

B. Bedrijfsvormen en verdienmodellen

De kernactiviteit van internetdiensten die een centrale rol spelen in de verspreiding van desinformatie is veelal dat zij derden de mogelijkheid bieden te communiceren. Daarmee is er al snel sprake van een bedrijfsvorm die raakt aan de problematiek van de aansprakelijkheid en verantwoordelijkheid voor illegale en schadelijke inhoud en communicatie. In lijn met een recente studie voor de Europese Commissie over dit onderwerp kunnen in dit kader de onderstaande diensten onderscheiden worden, in drie brede categorieën.¹¹³

Category 1: Storage & Distribution

1. **Web hosting:** The classic hosting intermediary: providing the possibility to host a website or other internet-based offering. Customers can publish their website through the services managed by the hosting company. Web hosting can vary in the extent to which it provides pre-installed web hosting and publishing features, such as analytics, programming environments, databases, etc. Examples of providers operating in this market are Leaseweb, WIX.com and Vautron Rechenzentrum AG.
2. **Online media sharing platforms:** services, that provide an open platform for online publications as well as the consumption of those publications, including images and video (Youtube, Vimeo, Photobucket), blogging and journalism (Medium, Wordpress) and other forms of media and for specialized contexts. Often, media sharing platforms will also involve a social element through comments sections or a discussion forum.
3. **File storage and sharing:** Services that offer users the ability to store and share different forms of files online (including video, audio, image, software and text documents). These services range from offering individual file storage solutions, with limited functionality to share, to services that incorporate more social features to facilitate sharing of materials between users and/or with third parties, turning them into online media sharing platforms discussed above. Examples of providers offering file storage and sharing services are Dropbox, box.com and WeTransfer.

¹¹¹ Richtlijn 2000/31/EG.

¹¹² Zie paragrafen 5.A en 6.A.

¹¹³ Zie https://www.ivir.nl/publicaties/download/hosting_intermediary_services.pdf.

4. **IaaS/PaaS:** Infrastructure as a Service and Platform as a Service cloud computing services.

Category 2: Networking, collaborative production and matchmaking

1. **Social networking and discussion forums:** services, like Facebook, LinkedIn, Twitter, Reddit and 4chan that allow people to connect and communicate publicly or semi-publicly.
2. **Collaborative production:** services that allow users to collaboratively create documents and other forms of media, and make these available to a broader audience.
3. **Online marketplaces:** services, like eBay, Marktplaats, eBid and Craigslist, offering the ability to place advertisements, and sell and buy goods, including second hand goods.
4. **Collaborative economy:** services that allow supply and demand relating to various goods and services to connect, for instance with respect to mobility (Lyft, BlaBlaCar), labor (Twizzi), travel/real estate (Airbnb, Homestay), and funding (Kickstarter).
5. **Online games:** services offering online multi-user gaming environments (with communication features), such as Xbox Live, Fortnite and World of Warcraft.

Category 3: Selection, search and referencing

1. **search tools:** online search services, such as Google Search, Yandex, or Baidu, that provide the possibility to navigate the online environment and search for online accessible information and offerings and directories such as dmoz and startpagina.
2. **Rating and review services:** online services, like Yelp, that provide the possibility to rate and review third-party offerings of various kinds.

In aanvulling hierop zijn, zoals eerder aangegeven, communicatiediensten relevant. In het bijzonder via internet aangeboden “*over the top*”-diensten (OTT’s) spelen een belangrijke rol.

De verdienmodellen van de bovengenoemde internetdiensten lopen uiteen en zijn het beste te classificeren door naar deze diensten te kijken vanuit het perspectief van de meerzijdige platformmarkten. Daarbij kan vervolgens onderscheid worden gemaakt tussen inkomsten aan de vraag- en aanbodkant, alsmede mogelijke inkomsten vanuit adverteerders. Het genereren van inkomsten via het aanbieden van gesponsorde communicatiemogelijkheden, al dan niet via daarvoor specifiek gecreëerde kanalen, is een belangrijke vorm van inkomsten voor veel van deze diensten. Er zijn ook vele internetdiensten waarbij in het geheel geen sprake is van advertenties, zoals bijvoorbeeld het geval is bij de meeste elektronische communicatiediensten. Daarentegen bestaan er ook andere inkomstenbronnen, bijvoorbeeld inkomsten uit betalingen door eindgebruikers.

C. Handhavingsmodaliteiten van internetdiensten

De daadwerkelijke mogelijkheden van internetdiensten om op te treden tegen desinformatie verschillen van dienst tot dienst. In het algemeen kan gesteld worden dat er vaak sprake zal zijn van een gebrek aan effectief toezicht en redactie op de inhoud vooraf. Dit is in het bijzonder het geval met betrekking tot de vraag of de informatie en communicatie die door derden via de dienst verspreid worden, voldoet aan de daarvoor door de dienst gestelde of op grond van de wet geldende regulering en beperkingen. Van een vergelijkbaar gebrek aan toezicht kan sprake zijn bij de inrichting en het daaropvolgende gebruik van gebruiksprofielen (accounts). Hier dient voorop te staan dat over het algemeen geen sprake is van het verplicht gebruik van identificerende gegevens bij het gebruik van internetdiensten. Om die reden is het redelijk eenvoudig om een hele reeks accounts aan te maken en hiermee te communiceren met door anderen gedeelde inhoud.

Het gebrek aan controle vooraf betekent uiteraard niet dat er geen mogelijkheden tot controle en handhaving voor handen zijn. Er kan hier een onderscheid gemaakt worden tussen drie verschillende modaliteiten van controle. Ten eerste is van belang de wijze waarop de relevante dienst is vormgegeven, waaronder eventuele specifieke mogelijkheden voor het verspreiden van gesponsorde (politieke) communicatie. Bij het ontwerp van de dienst moet zeker ook gedacht worden aan de relevante gebruiksin-terfaces via welke eindgebruikers en adverteerders van de dienst gebruik kunnen maken. Zo speelt bij communicatiediensten bijvoorbeeld de vraag hoe makkelijk het is om informatie verder te delen, of hoe-veel mensen tegelijkertijd een bericht kan worden gestuurd. Verder kan een dienst zo worden ingericht dat bijvoorbeeld verklaringen van gebruikers worden afgedwongen bij het gebruik van een bepaalde dienst, hetgeen de effectieve handhaving van bepaalde regels kan bevorderen (zogenaamde “regulering middels ontwerp”). Met betrekking tot gesponsorde communicatie is er tegenwoordig sprake van een veelheid aan verschillende mogelijkheden (data en overige analytische instrumenten) om advertenties op specifieke groepen mensen te richten. Deze mogelijkheden worden deels door de betreffende internet-diensten zelf aangeboden en deels door overige dienstverleners.

Ten tweede is vervolgens het beleid van de dienst zelf relevant, hetgeen via richtlijnen en gebruiksvoor-waarden zal worden opgelegd aan gebruikers. In dergelijke voorwaarden zijn doorgaans een veelheid aan beperkingen en voorwaarden opgelegd met betrekking tot de inhoud van communicatie, alsmede het gebruik van de dienst. Onder invloed van voortschrijdend inzicht over de maatschappelijke verant-woordelijkheid, reguleringsdruk en juridische ontwikkelingen vinden in gebruiksvoorwaarden verder geregeld aanpassingen plaats. De toegankelijkheid van de dienst voor, en de voorwaarden met betrek-king tot het kunnen tonen van politieke advertenties zijn momenteel in Nederland voornamelijk op deze wijze genormeerd.

Het verdient hier aandacht dat de mogelijkheden tot de verspreiding van politieke advertenties via internetdiensten aan duidelijke beperkingen onderhevig is. Veel relevante diensten, zoals advertentie-netwerkdiensten, staan geen politieke advertenties toe. Microsoft en meer recentelijk ook Twitter, bij-voorbeeld, staat niet langer betaalde politieke advertenties toe op internetdiensten.¹¹⁴ LinkedIn verbiedt politieke advertentie, inclusief advertenties die een bepaalde kandidaat of politiek standpunt in een ver-kiezing promoot, of anderszins tot doel heeft de uitkomst van een verkiezing te beïnvloeden. De dienst Reddit staat ook geen betaalde politieke advertenties toe buiten de Verenigde Staten.¹¹⁵ De in de markt bestaande incentives om advertentiekanalen voor politieke communicatie open te houden zijn gezien de gevoeligheden van dergelijke communicatie en de betrekkelijk beperkte markt, blijkbaar relatief beperkt. Facebook houdt vooralsnog vast aan een brede toegankelijkheid voor politieke advertenties, waarbij het er ook voor kiest om geen *fact checking* toe te passen op politieke advertenties.¹¹⁶

Zonder effectieve controle en handhaving, de derde modaliteit van controle, is er uiteraard mogelijk slechts een beperkte invloed van dit beleid. Het kan zijn dat deze controle plaatsvindt door de dienst zelf. In het geval dat het (mede) gaat om een wettelijke beperking, kan er sprake zijn van toezicht door derden of de overheid. Er wordt veel gebruik gemaakt van notificatieprocessen (*notice and action*), meer informeel via speciale knoppen voor gebruikers, en meer formeel indien sprake is van daarvoor ingerichte juridische procedures (zoals Notice en Takedown codes en in het geval van de Duitse NetzDG wetgeving).

114 Microsoft, ‘Disallowed Content Policies - Political and religious content’, <https://about.ads.microsoft.com/en-us/resources/policies/disallowed-content-policies> (“Advertising for election related content, political parties, candidates, and ballot measures is not allowed. Fundraising for political candidates, parties, PACs, and ballot measures is not allowed.”); Conger, K., ‘Twitter will ban all political ads, C.E.O. Jack Dorsey says’, The New York Times, 30 October 2019, available at: <https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html>.

115 Reddit, ‘Reddit Advertising Policy - Political Advertisements’, <https://www.reddithelp.com/en/categories/advertising/policy-guidelines/reddit-advertising-policy> (“Reddit does not accept advertisements pertaining to political issues, elections, or candidates outside the United States.”).

116 Vaidhyanathan, S. ‘The Real Reason Facebook Won’t Fact-Check Political Ads’, The New York Times, 2 November 2019.

Ten aanzien van mogelijke onrechtmatigheid of onregelmatigheid met betrekking tot informatie en communicatie, kunnen tenslotte de volgende vormen van actie onderscheiden worden. Naast het toestaan of verwijderen van communicatie is het de-prioriteren via relevante *ranking* en *recommendation* mechanismes van bijzonder belang. Deze vormen van controle over informatiestromen is van steeds groter belang voor het uitoefenen van controle op de informatiekwaliteit. Daarnaast wordt er door de meeste internetdiensten gebruik gemaakt van mogelijkheden om toegangsbeperkingen op te leggen aan specifieke gebruikers. Tenslotte is bij een aantal diensten sprake van de integratie van en/of samenwerking met zogenaamde fact-checkers. Bij dit laatste is het van belang stil te staan bij de vraag naar de effectiviteit van deze methoden van controle op desinformatie. Uit sociaalwetenschappelijk onderzoek blijkt dat omdat fact-checkers vaak komen uit ideologisch en maatschappelijk tegengestelde groepen, er sprake kan zijn van een gebrek aan vertrouwen bij de daadwerkelijke doelgroep. Dit kan ervoor zorgen dat het gebruik hiervan maar weinig effectief is of zelfs averechts kan werken.¹¹⁷

D. Samenvatting

Een groot aantal verschillende internetdiensten zijn relevant voor de mogelijke regulering van politieke advertenties. Deze verschillende diensten kunnen beschouwd worden op basis van hun juridische kwalificatie, bedrijfspvormen en verdienmodellen of op basis van de handhavingsmodaliteiten die een specifieke dienst ter beschikking staat. Vanuit juridisch perspectief zijn de volgende typen diensten relevant: diensten van de informatiemaatschappij, elektronische communicatiediensten en audiovisuele mediadiensten. Ook is het begrip *hosting service provider* uit de richtlijn elektronische handel van belang gezien de mogelijkheid van veel van de relevante diensten deze beperking van aansprakelijkheid in te roepen.

Wat betreft de verschillende bedrijfspvormen is het nuttig een onderscheid te maken tussen (i) opslag- en verspreidingsdiensten, (ii) diensten voor netwerken, collaboratieve productie en koppelingen, en (iii) diensten voor selectie, zoeken en verwijzingen. De verdienmodellen kunnen opgedeeld worden in diensten die inkomsten halen uit de vraag- of aanbodzijde, via adverteerders of betalingen door eindgebruikers.

Voor de handhaving moet ten slotte gekeken worden naar de volgende drie modaliteiten van controle voor de internetdienst: ten eerste de vormgeving van de specifieke dienst, ten tweede het (gestelde) beleid van de dienst zelf, en ten derde in hoeverre en hoe de dienst zijn uiteindelijke beleid, bijvoorbeeld ten aanzien van beperkingen op de inhoud, de wijze van gebruik en de politieke advertenties, (effectief) handhaaft.

¹¹⁷ Zie Harambam, J., 'De/politisering van de Waarheid'. Sociologie, 2017/13(1), p. 73-92.

4. Vrijheid van meningsuiting

- Vrijheid van meningsuiting brengt voor de staat een positieve verplichting met zich mee om pluralisme te garanderen.
- Het reguleren van desinformatie louter op grond van het feit dat informatie onjuist of misleidend is, zonder aanvullende eisen, kan een schending opleveren van het recht op vrijheid van meningsuiting.
- Betaalde politieke reclame is een politieke meningsuiting in de zin van het recht op vrijheid van meningsuiting.
- Transparantie is essentieel voor de bevordering en bescherming van mensenrechten zoals het recht op vrijheid van meningsuiting.
- Rechtsregels voor betaalde politieke reclame moeten ervoor zorgen dat het publiek een betaalde politieke reclame als zodanig kan herkennen.

Het recht op vrijheid van meningsuiting is een essentieel element bij het reguleren van politieke advertenties, aangezien de vrijheid om een politieke mening te uiten één van de meest gekoesterde democratische waarden is. De Nederlandse regering zet dit grondrecht daarom centraal bij haar beleid ter bescherming van de democratie tegen desinformatie. Het eerste uitgangspunt van dit beleid zijn de rechtsstatelijke waarden en grondrechten, waaronder de vrijheid van meningsuiting en vrijheid van de pers. De doelstelling van dit beleid is “de stabiliteit en kwaliteit van onze democratische rechtsorde en onze open samenleving te beschermen, met inbegrip van de vrijheid van meningsuiting en pers.”¹¹⁸

Het recht op vrijheid van meningsuiting is niet alleen een negatief recht dat wordt uitgeoefend tegen overheidsinmenging. Het legt staten ook een aantal positieve verplichtingen op om pluralisme te garanderen.¹¹⁹ In dit hoofdstuk wordt het mensenrechtelijk kader dat van toepassing is op vrijheid van meningsuiting en dat relevant is voor de discussie over de regulering van de politieke advertenties uiteengezet. Specifiek de relevante jurisprudentie en literatuur in verband met artikel 10 van het Europees Verdrag voor de Rechten van de Mens (“EVRM”) en artikel 11 van het Handvest van de grondrechten van de Europese Unie (“EU-Handvest”) wordt onder 4.a besproken. In 4.b wordt artikel 7 van de Nederlandse Grondwet besproken.

A. Artikel 10 EVRM en artikel 11 EU-Handvest

Het recht op vrijheid van meningsuiting wordt gewaarborgd door artikel 10 van het EVRM. Het Europees Hof voor de Rechten van de Mens (“EHRM”) is belast met de interpretatie van artikel 10 EVRM. Het EHRM heeft een aantal uitspraken gedaan over de vrijheid van meningsuiting en politieke advertenties, onlineplatforms en informatie van buitenlandse oorsprong. Deze uitspraken kunnen als leidraad dienen voor de in artikel 10 EVRM neergelegde beginselen die van toepassing zijn op alle toekomstige regelgeving inzake politieke advertenties die door internetdiensten worden gefaciliteerd.

De vrijheid van meningsuiting wordt ook gewaarborgd door artikel 11 van het EU-Handvest, dat wordt uitgelegd door het Hof van Justitie van de Europese Unie (“HvJEU”). Wat betreft de verhouding tot het EVRM bepaalt het EU-Handvest dat alle rechten “die corresponderen met rechten welke zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele

¹¹⁸ Tweede Kamer, 2019-202, 30 821, nr. 91 Kamerbrief ‘beleidsinzet bescherming democratie tegen desinformatie’.

¹¹⁹ Zie Tarlach McGonagle, ‘Positive Obligations Concerning Freedom of Expression: Mere Potential or Real Power?’ in Andreotti, O. (ed), *Journalism at Risk: Threats, Challenges and Perspectives* (Council of Europe Publishing 2015), p. 9-35.

vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend". Het HvJEU heeft zich tot op heden echter niet gebogen over vrijheid van meningsuiting in de context van politieke advertenties. Als zodanig heeft de onderstaande discussie voornamelijk betrekking op de jurisprudentie van het EHRM.

i. Positieve verplichtingen van de staat om pluralisme te garanderen

Het EHRM heeft benadrukt dat staten op grond van artikel 10 EVRM de positieve verplichting hebben "[to] create a favourable environment for participation in public debate by all the persons concerned".¹²⁰ Zoals McGonagle heeft opgemerkt, vereist deze verplichting dat staten pluralisme binnen het media-ecosysteem garanderen.¹²¹ Het EHRM heeft benadrukt dat de staten zelfs verplicht zijn een passend wetgevend en administratief kader te creëren om op effectieve wijze pluralisme te waarborgen.¹²² De redenen hiervoor zijn tweeledig. Enerzijds is er "no democracy without pluralism" en anderzijds moeten staten "the ultimate guarantor of pluralism" zijn.¹²³

Bij de regulering van online politieke advertenties moet om reeds genoemde redenen rekening worden gehouden met de positieve verplichting van de staat om pluralisme te garanderen wat kan betekenen dat de staat actief moet ingrijpen om op effectieve wijze pluralisme te garanderen. De noodzaak van positieve maatregelen kan liggen in twee aspecten gerelateerd aan de regulering van politieke advertenties. Ten eerste kan het nodig zijn om politieke advertenties te reguleren om te voorkomen dat geldstromen een te grote en te versturende invloed hebben op zowel het democratische debat als de democratische participatie. Het EHRM heeft het belang van een "plurality of voices" benadrukt voor wat betreft onderwerpen van publiek belang. Bovendien heeft het EHRM benadrukt dat het van belang is dat iedereen, waaronder individuen en kleine actiegroepen, effectief moet kunnen deelnemen aan het publiek debat.¹²⁴ Grote partijen mogen om die reden het publiek debat niet domineren of verstoren. Het kan mogelijk zijn dat vrijwillige maatregelen om bepaalde vormen van politieke advertenties te beperken, met name wanneer zij worden genomen door dominante internetdiensten, het vermogen van bepaalde groepen om doeltreffend te communiceren onnodig beperken waardoor ook het pluralisme wordt geschaad.¹²⁵ Eerder heeft het EHRM geoordeeld dat een gebrek aan procedurele billijkheid en gelijkheid aanleiding kan geven tot een schending van artikel 10 EVRM.¹²⁶

In het meest recente arrest over politieke advertenties, dat hieronder wordt besproken, heeft het EHRM een verband gelegd tussen pluralisme en de regulering van politieke advertenties. Het EHRM heeft aanvaard dat wanneer machtige financiële groepen "competitive advantages in the area of paid advertising" verkrijgen, dit kan leiden tot een beperking van "a free and pluralist debate" en de staat de positieve verplichting kan hebben om in te grijpen om op effectieve wijze pluralisme te garanderen.¹²⁷ De leden van de Raad van Europa hebben krachtens Protocol nr. 1 EVRM de aanvullende verplichting om verkiezingen te houden "onder voorwaarden die de vrije meningsuiting van het volk

120 Huseynova v. Azerbaijan (Application no. 10653/10) 13 April 2017, r.o. 120; and Dink v. Turkey (Application no. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09) 14 September 2010, r.o. 137.

121 Tarlach McGonagle, 'Fake news': False fears or real concerns? Netherlands Quarterly of Human Rights 2017, p. 203-209.

122 Centro Europa 7 S.r.l. and Di Stefano v. Italy [GC] (Application no. 38433/09) 7 June 2012, r.o. 134.

123 Manole and Others v. Moldova (Application no. 13936/02) 19 September 2009, r.o. 95-99.

124 Steel and Morris v. the United Kingdom (Application no. 668416/01) 15 February 2005, r.o. 89. Zie ook Dink v. Turkey, reeds aangehaald.

125 Zie verder: Angelopoulos, C. et al., 'Study of fundamental rights limitations for online enforcement through self-regulation', Institute for Information Law (IViR) 2015; McGonagle, T., 'The Council of Europe and Internet Intermediaries: A Case-Study of Tentative Posturing', in Jorgensen, R., 'Private Actors and Human Rights in the Online Domain', (MIT Publishing, forthcoming 2019).

126 Steel and Morris v. the United Kingdom, op. cit., r.o. 95.

127 Animal Defenders International v. the United Kingdom (Application no. 48876/08) 22 April 2013, r.o. 112.

bij het kiezen van de wetgevende macht waarborgen”,¹²⁸ met inbegrip van de verplichting voor de staat om positieve maatregelen te nemen “[to] secure pluralism of views”.¹²⁹

Hierbij moet men niet vergeten dat politieke advertenties mogelijkheden scheppen voor verstorende effecten voor het publieke debat. Bij gebrek aan redactionele controle bestaan dergelijke effecten echter ook door het gebruik van niet-gesponsorde communicatiekanalen en bijbehorende optimalisatietechnieken.

ii. Vrijheid van meningsuiting en onjuiste of misleidende informatie

Om te beginnen moet worden opgemerkt dat een specifieke regeling voor desinformatie die louter gebaseerd is op het feit dat de informatie onjuist of misleidend is, zonder aanvullende eisen, zoals het schaden van iemands reputatie of de rechten van een ander, moeilijk te rijmen valt met het recht op vrijheid van meningsuiting. Volgens de internationale normen voor de vrijheid van meningsuiting is het duidelijk dat “[g]eneral prohibitions” op de verspreiding van “false news” of “non-objective information” niet verenigbaar zijn met de internationale normen voor beperkingen van de vrijheid van meningsuiting en “should be abolished”.¹³⁰ Dit is ook de unanieme mening van de vier *special international mandates for protecting freedom of expression*, namelijk: de UN Special Rapporteur on Freedom of Opinion and Expression; de Organization for Security and Co-operation in Europe Representative on Freedom of the Media; de Organization of American States Special Rapporteur on Freedom of Expression; en de African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression and Access to Information.

Evenzo heeft de U.N. Human Rights Committee in niet mis te verstane bewoordingen verklaard dat vervolging “for the crime of publication of false news merely on the ground, without more, that the news was false, [is] in clear violation in clear violation of [freedom of expression].”.¹³¹ Regionale mensenrechtshoven nemen hetzelfde standpunt in: het Inter-Amerikaanse Hof voor de Rechten van de Mens heeft geoordeeld dat een “system that controls the right of expression in the name of a supposed guarantee of the correctness and truthfulness of the information that society receives can be the source of great abuse,” en “violates the right to information that this same society has.”¹³² Het EHRM heeft unaniem geoordeeld dat een vervolging wegens “verspreiding van valse informatie” een schending van het recht op vrijheid van meningsuiting inhoudt, waarbij het EHRM heeft geoordeeld dat “artikel 10 van het Verdrag als zodanig de bespreking of verspreiding van ontvangen informatie niet verbiedt, ook al bestaat er een sterk vermoeden dat deze informatie niet naar waarheid is verstrekt”.¹³³

En toch handhaven landen nog steeds wetten op het gebied van valse informatie en wetten die van oudsher bekend staan als “valse nieuwswetten”. In Frankrijk is er bijvoorbeeld een verbod op de publicatie van “*nouvelles fausses*” (“vals nieuws”) in het kader van de Persvrijheidswet 1881.¹³⁴ Als gevolg daarvan hebben hooggerechtshoven en constitutionele hoven over de hele wereld wetten inzake onjuiste of misleidende informatie overwogen en verschillende schendingen van de vrijheid van meningsuiting vastgesteld, waaronder het Hooggerechtshof van Canada, het Hooggerechtshof van Zimbabwe en het

128 Protocol bij het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, artikel 3 (“De Hoge Verdragsluitende Partijen verbinden zich om met redelijke tussenpozen vrije, geheime verkiezingen te houden onder voorwaarden die de vrije meningsuiting van het volk bij het kiezen van de wetgevende macht waarborgen.”).

129 Communist Party of Russia and Others v. Russia, no. 29400/05, 19 June 2012, r.o. 126.

130 United Nations Special Rapporteur, ‘Joint declaration on freedom of expression and “fake news”’, FOM.GAL/3/17, 2017, <https://www.osce.org/fom/302796?download=true>.

131 Slotopmerkingen van de Mensenrechtencommissie: Kameroen, CCPR/C/79/Add.116, 4 november 1999, par. 24, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2F79%2FAdd.116&ang=en.

132 Verplicht lidmaatschap van een vereniging voor de journalistieke praktijk, advies OC-5/85, voorgeschreven door de wet. Serie A, nr. 5, 13 november 1985.

133 Salov v. Ukraine (App. no. 65518/01), 6 September 2005.

134 Loi du 29 juillet 1881 sur la liberté de la presse, article 27, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722>.

Hooggerechtshof van Oeganda. De specifieke bepalingen die in de landen in kwestie aan de orde zijn, zoals hieronder besproken, vertonen een opvallende gelijkenis met de huidige concepten van desinformatie die worden voorgesteld.

Een van de belangrijkste arresten is die van het Hooggerechtshof van Canada, dat artikel 181 van het Wetboek van Strafrecht ("spreading false news") overwoog, dat "wilfully publish[ing] a statement, tale or news that he knows is false and that causes or is likely to cause injury or mischief to a public interest."¹³⁵ Het Hof oordeelde dat de wet in strijd is met het recht op vrijheid van meningsuiting, waarbij het doel van de vrijheid van meningsuiting zich uitstrekt tot "the protection of minority beliefs which the majority regard as wrong or false," en een wet "which forbids expression of a minority or "false" view on pain of criminal prosecution and imprisonment, on its face, offends the purpose of the guarantee of free expression."¹³⁶ Verder kan "[e]xaggeration - even clear falsification - may arguably serve useful social purposes linked to the values underlying freedom of expression."¹³⁷ Ook het Hooggerechtshof van Zimbabwe heeft unaniem geoordeeld dat de valse informatieverstrekking door Zimbabwe het recht op vrijheid van meningsuiting schendt.¹³⁸ De wet stelde namelijk "any false statement, rumour or report which is likely to cause fear, alarm or despondency among the public or any section of the public; or is likely to disturb the public peace" strafbaar. Het Hof oordeelde dat de wet "has the effect of overriding the most precious of all the protected freedoms, resting as it does at the very core of a democratic society - fails for want of proportionality between its potential reach on the one hand and the "evil" to which it is claimed to be directed on the other."¹³⁹ Het Hooggerechtshof van Oeganda heeft zich eveneens gebogen over artikel 50 van het Oegandese Wetboek van Strafrecht (publicatie van vals nieuws), dat "publish[ing] any false statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace" strafbaar stelt. Het Hof oordeelt dat de wet een schending is van het recht op vrijheid van meningsuiting en vindt dat de wet "imposes an unacceptable chilling effect on the freedom of the press".¹⁴⁰ En in 2018 overwoog het Hof van Justitie van de Economische Gemeenschap van West-Afrikaanse Staten veroordelingen op grond van de valse nieuwswet van Gambia, die het een strafbaar feit maakte voor een persoon om een "statement, rumour or report which is likely to cause fear and alarm to the public or disturb the public peace, knowing or having reason to believe that the statement, rumour or report is false".¹⁴¹ De Rekenkamer constateerde dat de bepaling "amounts to censorship on publication".¹⁴²

De belangrijkste zaak over de valse uitdrukking van het Amerikaanse Hooggerechtshof is *United States v. Alvarez*, waar het Hof oordeelde dat een federale wet die het "falsely claim[ing] receipt of military decorations or medals" strafbaar stelt, het recht op vrijheid van meningsuiting schendt.¹⁴³ Het Hof oordeelde dat de federale wet "rejects the notion that false speech should be in a general category that is presumptively unprotected".¹⁴⁴ Verder zou "[p]ermitting the government to decree this speech to be a criminal offense", "endorse government authority to compile a list of subjects about which false statements are punishable," en "[o]ur constitutional tradition stands against the idea that we need Oceania's Ministry of Truth."¹⁴⁵ Het Hof concludeert dat "[t]he remedy for speech that is false is speech that is true. This is the ordinary course in a free society."¹⁴⁶

135 R. v. Zundel, 27 augustus 1992, 2 S.C.R. 731, www.canlii.org/en/ca/scc/doc/1992/1992canlii75/1992canlii75.html.

136 Idem, p. 753.

137 Idem, p. 754.

138 Chavunduka and others v Minister of Home Affairs and another, 20 mei 2000, SC36/2000, <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2017/08/Chavunduka-v-Minister-of-Home-Affairs-Zimbabwe9610.pdf>.

139 Idem, p. 24.

140 Charles Onyango Obbo en Anor tegen procureur-generaal ((Constitutioneel beroep nr. 2 van 2002)). UGSC 1 (10 februari 2004), blz. 48 (Odoki, CJ), <https://ulii.org/ug/judgment/supreme-court/2004/1>.

141 Federation of African Journalists (FAJ) and others v. The Gambia, Judgment No: ECW/CCJ/JUD/04/18. 13 March 2018, <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/04/FAJ-and-Others-v-The-Gambia-Judgment.pdf>.

142 Idem, p. 40.

143 *United States v. Alvarez*, 567 U.S. 709 (2012).

144 *United States v. Alvarez*, 567 U.S. 709 (2012), r.o. 722.

145 *United States v. Alvarez*, 567 U.S. 709 (2012), r.o. 723.

146 *United States v. Alvarez*, 567 U.S. 709 (2012), r.o. 727.

iii. Artikel 10 EVRM & ruime definities van desinformatie

Krachtens artikel 10 EVRM moeten wetten die de vrijheid van meningsuiting aantasten, met “sufficient precision” worden geformuleerd, zodat personen in algemene zin de gevolgen van hun handelen kunnen voorzien.¹⁴⁷ Wanneer de wetgeving te ruime of vage bepalingen bevat, heeft het EHRM schendingen van artikel 10 EVRM vastgesteld aangezien deze een voortdurende bedreiging voor de vrijheid van meningsuiting kunnen vormen. Daarom kan het nuttig zijn om voor mogelijke regulering van desinformatie de door de Europese Commissie gegeven definitie te onderzoeken in het licht van artikel 10 EVRM. De definitie van de Europese Commissie is natuurlijk niet bedoeld als een modeldefinitie voor wetgeving, maar een analyse ervan in het kader van de normen voor de vrijheid van meningsuiting kan valkuilen in verband met mogelijke regelgeving aan het licht brengen.

Als we kijken naar de definitie van desinformatie van de Europese Commissie in het licht van de hierboven genoemde internationale normen voor de vrijheid van meningsuiting, dan is er één belangrijke opmerking die moet worden gemaakt. Opvallend is dat de definitie gelijkenis vertoont met de hierboven genoemde fake news” wetten, die door een reeks van hooggerechtshoven in de hele wereld in overweging zijn genomen. Hieronder zijn vier voorbeelden opgenomen uit het strafrecht, waar nationale hooggerechtshoven, naast de definitie van de Commissie, schendingen van de vrijheid van meningsuiting hebben vastgesteld:

1. “false or misleading information which is disseminated for economic gain or to intentionally deceive the public, and may cause public harm” (European Commission)
2. “false statement, rumour or report which is likely to cause fear, alarm or despondency among the public or any section of the public; or is likely to disturb the public peace” (Zimbabwe Criminal Code) (declared unconstitutional by Zimbabwe Supreme Court).
3. “wilfully and knowingly publishes any false news or tale whereby injury or mischief is or is likely to be occasioned to any public interest” (Canada Criminal Code) (declared unconstitutional by Canadian Supreme Court).
4. “false statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace” (Uganda Penal Code) (declared unconstitutional by Uganda Supreme Court).
5. “statement, rumour or report which is likely to cause fear and alarm to the public or disturb the public peace, knowing or having reason to believe that the statement, rumour or report is false” (the Gambia Criminal Code) (violated freedom of expression, Court of Justice of the Economic Community of West African States).

Sommige van deze definities bevatten strengere eisen dan de definitie van de Europese Commissie, zoals de eis van een “*waarschijnlijke*” verstoring van de vrede, terwijl de Commissie alleen eist dat valse informatie het publiek schade “*kan*” toebrengen. En toch zijn deze definities van “fake news” in strijd met de vrijheid van meningsuiting. Gezien de bovengenoemde duidelijke internationale normen voor de vrijheid van meningsuiting en de gelijkenis tussen de definitie van de Europese Commissie van desinformatie en “fake news” wetgeving die wordt beschouwd als een schending van de vrijheid van meningsuiting, is het duidelijk dat elke poging om wetgeving te creëren om desinformatie in de vorm van onjuiste of misleidende informatie te verbieden, ernstige problemen met betrekking tot de vrijheid van meningsuiting met zich mee zou brengen.

Ten tijde van zijn uitspraak merkte het Hooggerechtshof van Canada op dat toen de Canadese regering de wet op de verspreiding van valse informatie probeerde te rechtvaardigen, de regering “no other

¹⁴⁷ Altuğ Taner Akçam v. Turkey (Application no. 27520/07) 25 October 2011, r.o. 87.

free and democratic country with criminal legislation of this type” kon aanwijzen.¹⁴⁸ Dit is veranderd. Sinds 2016 hebben landen als Kameroen, Rusland, Maleisië, en Singapore nieuwe “fake news” wetten ingevoerd met onheilspellende titels zoals de Maleisische Anti-Fake News Act 2018 of de Singapore’s Protection from Online Falsehoods and Manipulation Act 2019, en zijn ze bekritiseerd op grond van internationale normen voor vrijheid van meningsuiting.¹⁴⁹ Veel landen criminaliseren nog steeds de publicatie van valse informatie, zoals het Bahreinse wetboek van strafrecht of de federale wet van de Verenigde Arabische Emiraten.¹⁵⁰

Kortom, brede, vage of algemene termen mogen niet worden gebruikt als basis voor het beperken van de vrijheid van meningsuiting. Het gebruik van dergelijke termen in het kader van de regulering van de meningsuiting brengt het risico met zich mee dat deze termen te breed of willekeurig worden geïnterpreteerd en toegepast, wat op zijn beurt een *chilling* effect heeft op de vrijheid van meningsuiting en leidt tot zelfcensuur. Brede en vage termen die een reeks verschillende soorten uitingen bestrijken, moeten worden beoordeeld in het licht van de reikwijdte van het recht op vrijheid van meningsuiting, zoals dat wordt gewaarborgd door het internationale recht op het gebied van de mensenrechten en de beperkingen en verboden die het recht toestaat en voorschrijft.¹⁵¹

iv. Artikel 10 van het EVRM en schade voor het publiek

Aangezien de vrijheid van meningsuiting “taken en verantwoordelijkheden met zich meebrengt”, kan zij krachtens artikel 10, lid 2, EVRM alleen worden beperkt op grond van een aantal specifiek opgesomde redenen, zoals de bescherming van de reputatie of de persoonlijke levenssfeer van een persoon, de “prevention of disorder or crime”, enz.¹⁵² Wetgeving zoals regelgeving over smaad beperken valse informatie die de reputatie van een persoon kan schaden; of wetten die zien op het aanzetten tot geweld die bedoeld zijn om wanorde te voorkomen.

In de definitie van de Europese Commissie van desinformatie omvat echter ook valse informatie die “may cause *public harm*,” met inbegrip van “threats to democratic political and policymaking processes”.¹⁵³ De vraag rijst dus of er op grond van artikel 10 EVRM een legitieme reden is om valse informatie te reguleren op grond van het feit dat deze *het publiek schade* kan berokkenen, in tegenstelling tot valse informatie die de reputatie of de orde kan schaden.

Belangrijk is dat het EHRM in *Perinçek v. Zwitserland* het standpunt verwierp dat artikel 10 EVRM een uitzondering bevatte voor de bescherming van “de openbare orde”, zoals wanneer het “is often taken to refer to the body of political, economic and moral principles essential to the maintenance of the social structure”.¹⁵⁴ Het Hof oordeelde dat de term “voorkoming van ordeverstoring” in artikel 10 betekent dat “vormen van verstoring van de openbare orde” worden voorkomen.¹⁵⁵ In een arrest van 2019, waarbij de Russische regering een sociale mediapost blokkeerde om de “openbare veiligheid” te beschermen, stelde

148 R. v. Zundel, 27 augustus 1992, 2 S.C.R. 731, www.canlii.org/en/ca/scc/doc/1992/1992canlii75/1992canlii75.html.

149 Zie Artikel 19 Anti-Fake News Act 2018 <https://www.article19.org/wp-content/uploads/2018/04/2018.04.22-Malaysia-Fake-News-Legal-Analysis-FINAL-v3.pdf>; and Artikel 19 New law on “online falsehoods” a grave threat to freedom of expression 2019, <https://www.article19.org/resources/singapore-new-law-on-online-falsehoods-a-grave-threat-to-freedom-of-expression/>

150 Zie Bahrain Penal Code, 1976, artikel 168, https://www.unodc.org/res/cld/document/bhr/1976/bahrain_penal_code_html/Bahrain_Penal_Code_1976.pdf.

151 UN Human Rights Committee, General Comment No. 34, para. 46.

152 Article 10(2) ECHR (The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary).

153 Europese Commissie, ‘EU praktijkcode tegen desinformatie’, preambule, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

154 *Perinçek v. Switzerland* (App. no. 27510/08) 15 October 2015 (Grand Chamber), r.o. 146.

155 *Perinçek v. Switzerland* (App. no. 27510/08) 15 October 2015 (Grand Chamber), r.o. 152.

het EHRM een schending van artikel 10 EVRM vast en zei het heel definitief: “neither Article 10 nor Article 11 allows for restrictions aimed at maintenance, or protection, of public order”.¹⁵⁶

Op grond van artikel 10 EVRM zou het dus zeer problematisch zijn om valse informatie te verbieden louter op grond van het feit dat deze “publieke schade” kan veroorzaken. Elke regeling van desinformatie zou alleen gericht moeten zijn op informatie op basis van de bescherming van de rechten van anderen (bv. reputatie, privacy, waardigheid) of een legitiem overheidsbelang, zoals het voorkomen van wanorde (bv. verstoring van de openbare orde). Een vaag belang zoals publieke schade lijkt niet onder artikel 10 EVRM te vallen.

In plaats van te streven naar een nieuwe inhoudelijke regulering van desinformatie op basis van nieuwe en betwiste vormen van overheidsbelangen, zoals publieke schade, zou het garanderen van mediapluralisme en een faciliterende omgeving voor de vrijheid van meningsuiting op het internet een geschiktere basis zijn om desinformatie aan te pakken, en zou het een basis vormen voor de aanpak van desinformatie die gefundeerd is op mensenrechtennormen.

v. Commerciële uitingen

Een bijzonder kenmerk van de definitie van de Europese Commissie van desinformatie is dat deze slechts kan bestaan uit onjuiste of misleidende informatie “disseminated for economic gain”, en niet meer dan dat. Dit doet de vraag rijzen of het mogelijk is om regelgeving op te stellen die gericht is op desinformatie die specifiek wordt verspreid met een winstoogmerk, in plaats van om redenen van algemeen belang (hoewel de meeste Europese mediaorganisaties zoals uitgevers, kranten, nieuwswebsites en omroepen een winstoogmerk hebben). Belangrijk is dat het EHRM specifiek heeft geoordeeld dat artikel 10 EVRM van toepassing is ook wanneer het nagestreefde doel “profit-making” is, waarbij wordt gesteld dat de expliciete formulering van artikel 10 EVRM de vrijheid van meningsuiting voor “eenieder” waarborgt en “[n]o distinction is made in it according to whether the aim pursued is profit-making or not”.¹⁵⁷ De uitoefening van de vrijheid van meningsuiting voor uitsluitend commercieel of economisch gewin wordt dus beschermd door artikel 10 EVRM. Pogingen om onjuiste of misleidende informatie te reguleren op grond van het feit dat deze met het oog op economisch gewin wordt verspreid, zouden dus ook problematisch zijn in het kader van artikel 10 van het EVRM. Het zou zeer moeilijk zijn om op deze basis wetgeving te creëren, aangezien de meeste online-nieuwsorganisaties een winstoogmerk hebben. Daarom zou een poging om de definitie van onjuiste of misleidende informatie te beperken door zich te richten op informatie die wordt verspreid met een winstoogmerk, niet alle problemen oplossen die in de vorige paragraaf zijn beschreven. Bovendien is regulering van onjuiste of misleidende informatie dus niet verenigbaar met de internationale normen voor vrijheid van meningsuiting.

Door zich te concentreren op de verspreiding van desinformatie verspreid met een winstoogmerk probeert de Commissie het probleem aan te pakken van de zogenaamde click-bait-artikelen die opzettelijke leugens uitlokken en enkel bedoeld zijn om de reclame-inkomsten te maximaliseren. Dergelijke artikelen kunnen problematisch zijn voor het openbare debat, maar het zou vrij moeilijk zijn om in het kader van artikel 10 EVRM een voldoende duidelijke en strikt op maat gesneden wet te formuleren die niet ook het risico met zich meebrengt dat de wet onterecht op volstrekt legitieme politieke uitingen wordt toegepast. Een meer geschikte manier kan zijn om wetten te formuleren die erop gericht zijn het vermogen van de distributiekkanalen om te profiteren van de verspreiding van desinformatie aan te pakken.

Vervolgens kan er worden beargumenteerd dat onjuiste of misleidende informatie die met het oog op economisch gewin wordt verspreid, moet worden gekwalificeerd als een onjuiste of misleidende

¹⁵⁶ *Kablis v. Russia* (App. nos. 48310/16 and 59663/17) 30 April 2019, r.o. 87.

¹⁵⁷ *Zie, Casado Coca v. Spain* (Application no. 15450/89) 24 February 1994, r.o. 35; and *Autronic AG v. Switzerland* (Application no. 12726/87) 22 May 1990, r.o. 47.

commerciële uiting. Het EHRM heeft op nuttige wijze uiteengezet wat het EHRM als commerciële uitdrukking beschouwt, namelijk “inciting the public to purchase a particular product”,¹⁵⁸ of “product marketing”.¹⁵⁹ Commerciële reclame is een middel “to discover the characteristics of services and goods offered”.¹⁶⁰ In een van zijn laatste uitspraken over commerciële uitingen herhaalde het EHRM dat de lidstaten over een “broad margin of appreciation in the regulation of speech in commercial matters or advertising” beschikken.¹⁶¹ Hoewel reclame soms kan worden beperkt, met name om onjuiste of misleidende reclame te voorkomen, moeten dergelijke beperkingen “closely scrutinised by the Court, which must weigh the requirements of those particular features against the advertising in question”.¹⁶² Het zou dus moeilijk zijn om desinformatie te reguleren als een misleidende commerciële uiting, aangezien er geen sprake is van product- of dienstenmarketing. Zelfs wanneer sprake is van een commerciële uitdrukking, kan de regering een dergelijke uitdrukking alleen beperken op basis van het kader van artikel 10 EVRM, d.w.z. wettelijk voorgeschreven, een legitiem doel nastrevend, en noodzakelijk in een democratische samenleving. De overheid heeft weliswaar een beoordelingsmarge om commerciële uitingen te reguleren, maar heeft geen vrije hand.

vi. Hate speech

In sommige literatuur over desinformatie wordt de kwestie van *hate speech* als een onderscheidend kenmerk van desinformatiecampagnes opgenomen. Onderzoek heeft uitgewezen dat de amplificatie van *hate speech* een van de vele tactieken is die in desinformatiecampagnes worden toegepast.¹⁶³ De EU-ambtenaren hebben in één adem gesproken over het feit dat de problematiek van haatzaaiing en desinformatie een grote uitdaging voor de EU vormt.¹⁶⁴ Het is daarom heel belangrijk om de EVRM-normen inzake haatzaaiing duidelijk vast te stellen. Het kan onze discussie ook helpen om te kijken naar specifieke vereisten inzake de *intentie* en de *schade* voor wanneer de wetgeving zich richt op valse informatie die bepaalde minderheidsgroepen kan schaden.

De ontwikkeling van de jurisprudentie van het EHRM over *hate speech* is enigszins onduidelijk en heeft aanleiding gegeven tot vragen over de consistentie daarvan.¹⁶⁵ Het EHRM heeft zich echter de laatste tijd effectief beziggehouden met de kwestie van *hate speech* op sociale media.¹⁶⁶ Het EHRM heeft unaniem bevestigd dat het de benadering in het kader van de internationale normen voor de vrijheid van meningsuiting volgt die “essential elements” bevat om te bepalen of een uiting een (illegale) aansporing tot haat vormt: “(a) real and imminent danger of violence resulting from the expression; (b) intent of the speaker to incite discrimination, hostility or violence; and (c) careful consideration by the judiciary of the context in which hatred was expressed.” Toen het EHRM de vervolging van een blogger wegens het aanzetten tot haat herzag, kwam het EHRM unaniem tot de conclusie dat er sprake was van een schending van artikel 10 EVRM, aangezien er geen bewijs was dat de uitingen van de blogger onwettige handelingen zouden kunnen uitlokken, of dat het “posed a clear and imminent danger”. Het EHRM waarschuwde dat het van essentieel belang is dat strafrechtelijke bepalingen die gericht zijn op haatzaaiing “clearly and precisely define[s] the scope of relevant offences,” en dat de uitingen “strictly construed in order to avoid a

158 *VgT Verein gegen Tierfabriken v. Switzerland* (Application no. 24699/94) 28 June 2001, r.o. 57.

159 *TV Vest As & Rogaland Pensjonistparti v. Norway* (Application no. 21132/05) 11 December 2008, r.o. 64.

160 *Casado Coca v. Spain* (Application no. 15450/89) 24 February 1994, r.o. 51.

161 *Sekmadienis Ltd. v. Lithuania* (Application no. 69317/14) 30 January 2018, r.o. 73.

162 *Casado Coca v. Spain* (Application no. 15450/89) 24 February 1994, r.o. 51.

163 Reppell, L. & Shein, E., ‘*Disinformation Campaigns and Hate Speech: Exploring the Relationship and Programming Interventions*’, International Foundation for Electoral Systems, 2019, p. 1, https://www.ifes.org/sites/default/files/2019_ifes_disinformation_campaigns_and_hate_speech_briefing_paper.pdf.

164 Guérend, H.E.V., ‘*EU-Indonesia Seminar on Addressing Hate Speech and Disinformation with a Rights-Based Approach*’, 2018, https://eeas.europa.eu/delegations/indonesia/52263/indonesia-and-eu-discuss-tackling-hate-speech-and-disinformation_en.

165 Zie: McGonagle, T., ‘*The Council of Europe against online hate speech: Conundrums and challenges*’, Expert paper, Doc. No. MCM 2013(005), 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’, Belgrade, 7-8 November 2013.

166 *Savva Terentyev v. Russia* (Application no. 10692/09) 28 August 2018.

situation where the State's discretion to prosecute for such offences becomes too broad and potentially subject to abuse through selective enforcement."¹⁶⁷

Het EHRM is zich ervan bewust dat kwetsbare minderheden, groepen met een geschiedenis van onderdrukking en groepen die te maken hebben met diepgewortelde vooroordelen, vijandigheid en discriminatie, in principe beter beschermd moeten worden tegen beledigingen en laster.¹⁶⁸ Elke inhoudelijke regeling die gericht is op het aanpakken van valse informatie die geweld, haat of intolerantie aanwakert, bevordert of rechtvaardigt, moet echter voldoen aan de essentiële elementen van artikel 10 EVRM, waaronder de *intentie van de spreker* om aan te zetten tot discriminatie, vijandigheid of geweld. In een ander recent arrest heeft het EHRM benadrukt dat het "vitally important" is voor overheden om een "cautious approach" erop na te houden om de omvang van "hate speech" misdrijven vast te stellen.¹⁶⁹ Een goed uitgewerkte, inhoudelijk neutrale regeling, die bijvoorbeeld voorschrijft dat gebruikers schadelijke (maar niet illegale) haatzaaiing en desinformatie moeten melden, zou minder zorgwekkend zijn in het kader van artikel 10 EVRM.

vii. Politieke advertenties als een vorm van politieke meningsuiting

Bij het overwegen van politieke advertenties en vrijheid van meningsuiting heeft het EHRM een nuttige uiteenzetting gegeven van wat het EHRM als politieke advertenties beschouwt, hoewel er geen specifieke definitie is vastgesteld. Het EHRM overweegt dat een politieke advertentie tegen betaling kwalificeert als een politieke meningsuiting in de zin van artikel 10 EVRM. Zo werd bijvoorbeeld een televisiereclame van een politieke partij die de kijkers aanspoorde om voor de partij te stemmen gekwalificeerd als meningsuiting met een "indisputa[ble] political nature", ongeacht "the fact that it was presented as a paid advertisement". De "political nature of the advertisements" vereist een "strict scrutiny" aan de zijde van het EHRM. Ook heeft het EHRM geoordeeld dat een televisiereclame van een dierenbond die de kijkers aanspoorde om minder vlees te eten, kwalificeert als een politieke advertentie omdat de advertentie "[contained] controversial opinions pertaining to modern society in general and also lying at the heart of various political debates" en "fell outside the regular commercial context inciting the public to purchase a particular product". Het EHRM oordeelde dat de advertentie als "political speech by the applicant association" kwalificeerde. Tot slot heeft het EHRM verklaard dat politieke advertenties ook advertenties omvat voor "matters of broader public interest", in het kader van een procedure om een televisiereclame van een dierenrechtenvereniging die de kijkers aanmoedigde om apenmisbruik te stoppen.

Hieruit volgt dat het EHRM een ruime opvatting van politieke advertenties heeft. Deze opvatting omvat advertenties van politieke partijen die meer kiezers voor zich willen winnen, alsook advertenties over zaken van algemeen belang van actiegroepen. Deze laatste vorm worden "issue ads" genoemd in beleidsdiscussies. Beiden vormen worden beschouwd als politieke uitingen in de zin van artikel 10 EVRM.

In het bijzonder heeft het EHRM geoordeeld dat er sprake is van een schending van artikel 10 EVRM in situaties waarin de toets van een betalingsvereiste ontbreekt. Bijvoorbeeld in 2017 toen een Russische krant een boete opgelegd kreeg. De Russische regering betoogde dat een partijdig krantenartikel tijdens een verkiezing in feite een politieke advertentie was en om die reden onderworpen was aan campagnevoorschriften. Het EHRM benadrukte dat het ontbreken van enige betaling in deze zaak cruciaal is: om die reden kwalificeert het artikel journalistieke uiting in verkiezingstijd. Door te focussen op het betalingsvereiste kan een overijverige toepassing van de regels voor politieke advertenties op politieke uitingen in het kader van artikel 10 EVRM worden voorkomen.

¹⁶⁷ Ibid., para. 85.

¹⁶⁸ Savva Terentyev v. Russia (Application no. 10692/09) 28 August 2018, r.o. 76.

¹⁶⁹ Stomakhin v. Russia (Application no. 52273/07) 9 May 2018, r.o. 117.

Het kan ook nuttig zijn om nogmaals te bekijken hoe het EHRM commerciële advertenties definieert. Het gaat volgens het EHRM om advertenties “inciting the public to purchase a particular product”, of “product marketing”. Bovendien is dergelijke reclame voor consumenten een middel om de “characteristics of services and goods offered” te ontdekken. In een recentere uitspraak over commerciële meningsuitingen herhaalde het EHRM dat de lidstaten beschikken over een “broad margin of appreciation in the regulation of speech in commercial matters or advertising”. Hoewel advertenties soms mogen worden beperkt, met name om vormen van “untruthful or misleading advertising” te voorkomen, moeten dergelijke beperkingen als volgt worden afgewogen: “closely scrutinised by the Court, which must weigh the requirements of those particular features against the advertising in question”.

Samenvattend oordeelt het EHRM dat politieke advertenties tegen betaling een politieke uiting zijn in de zin van artikel 10 EVRM en dat commerciële advertenties daarentegen noodzakelijkerwijs betrekking hebben op het op de markt brengen van goederen en diensten, en eerder aan beperkingen kunnen worden onderworpen.

viii. De toelaatbaarheid van een verbod op politieke advertenties

Hoewel het EHRM politieke advertenties als een vorm van een politieke meningsuiting beschouwt, betekent dit niet dat politieke advertenties niet mogen worden beperkt. Het EHRM heeft in dit kader twee tegenstrijdige arresten gewezen. Enerzijds oordeelde het EHRM dat een verbod op politieke advertentie op televisie in Zwitserland en Noorwegen in strijd is met artikel 10 EVRM. Anderzijds, oordeelde het EHRM dat een verbod in het Verenigd Koninkrijk geen schending van artikel 10 EVRM oplevert.

In de eerste zaak, *VgT v. Switzerland*,¹⁷⁰ wilde een dierenrechtenorganisatie een reclame uitzenden met daarin de levensomstandigheden van varkens in *factory farms*. De Zwitserse Radio- en Televisiewet bevat een verbod op “politieke advertenties” en de Zwitserse rechtbanken stonden het uitzenden van de advertentie niet toe. Om die reden wendde de vereniging zich tot het EHRM met een beroep op artikel 10 EVRM.

Het EHRM heeft de door de Zwitserse regering naar voren gebrachte argumenten voor de handhaving van een politieke advertentieverbod in overweging genomen, namelijk: (a) het voorkomen van een verstoring van het publieke debat door financieel machtige groepen en (b) dat omroepmedia mag onderworpen worden aan meer overheidsregulering omdat het invloedrijke media zijn. Het EHRM concludeert echter dat deze redenen weliswaar relevant zijn, maar dat deze “general reasons” niet volstaan om het verbod te handhaven jegens een kleine dierenrechtenorganisatie die geen bedreiging voor enige verstoring van het publieke debat vormt. Het EHRM oordeelt dat er sprake is van een schending van artikel 10 EVRM. Het EHRM voegt daaraan toe dat het “cannot exclude” dat een verbod op “political advertising may be compatible with the requirements of Article 10 of the Convention in certain situations; but the reasons must be “relevant” and “sufficient” in respect of the particular interference with the rights under Article 10”.¹⁷¹

De uitspraak in *VgT v. Switzerland* was niet verrassend, gezien de bescherming die politieke uitingen gewoonlijk op grond van 10 EVRM genieten. *TV Vest v. Norway* is een vergelijkbare uitspraak: een Noorse politieke partij betoogt dat een verbod op politieke advertenties op televisie in de aanloop naar verkiezingen een schending van artikel 10 EVRM oplevert. Het EHRM oordeelt in het voordeel van de politieke partij. Het EHRM erkent dat er relevante redenen kunnen zijn voor een verbod op politieke advertenties, zoals het voorkomen dat “financially powerful [parties]” een “undesirable advantage” krijgen in het publiek debat en teneinde een “a level playing field in elections” te waarborgen. Het EHRM

¹⁷⁰ *VgT Verein gegen Tierfabriken v. Switzerland* (Application no. 24699/94) 28 June 2001.

¹⁷¹ *Idem*, r.o. 75.

oordeelt echter dat de betrokken politieke partij, een kleine partij van gepensioneerden, nauwelijks werd genoemd in de televisie-uitzendingen in de aanloop naar de verkiezingen en dat betaalde televisiereclame voor de partij “the only way” is om haar boodschap aan het publiek over te brengen. Bovendien viel de partij niet in de categorie van partijen waarop het verbod was gericht, namelijk financieel sterke partijen die een “unfair advantage” zouden kunnen behalen. Het EHRM oordeelde derhalve dat de algemene “objectives” van het advertentieverbod geen rechtvaardiging kunnen vormen voor de toepassing ervan op desbetreffende politieke partij, en aldus een schending oplevert van artikel 10 EVRM.

Anderzijds heeft het EHRM in 2013 in de *Grand Chamber* met 17 rechters (vanwege het belang van de zaak) in *Animal Defenders International v. UK* geoordeeld dat een verbod op betaalde politieke advertenties op televisie in het Verenigd Koninkrijk geen schending oplevert van artikel 10 EVRM. Voor het eerst heeft het EHRM op grond van artikel 10 EVRM geoordeeld dat een bepaald type regulering, die het EHRM bestempelt als “general measure”, kan worden opgelegd “consistently with the Convention”, zelfs wanneer dit leidt tot “individual hard cases” die tarten aan het recht op vrijheid van meningsuiting. Het EHRM introduceert een driestappentoets om te bepalen of een zogenaamde “general measure” in overeenstemming is met artikel 10 EVRM: “a) asses the legislative choices underlying the general measure, (b) the quality of the parliamentary review of the necessity of the measure, and (c) any risk of abuse if a general measure is relaxed”.

Vervolgens heeft het EHRM de driestappentoets toegepast op het verbod op politieke advertenties op televisie in de UK: ten eerste worden de “legislative choices” onderzocht die aan het verbod ten grondslag liggen. Het EHRM erkent in het kader hiervan dat het noodzakelijk is om het “risk of distortion” van het publieke debat door financieel sterke partijen met een ongelijke toegang tot politieke advertenties te voorkomen, mede vanwege het “immediate and powerful effect of the broadcast media”. Ten tweede merkt het EHRM op dat zij, met betrekking tot de kwaliteit van de parlementaire controle, veel waarde hecht aan “extensive pre-legislative consultation” onder verwijzing naar een aantal parlementaire organen die het betreffende verbod hadden onderzocht. Ten derde, met betrekking tot het risico van misbruik van een versoepeling van de regeling (zoals een financieel plafond voor de uitgaven aan politieke advertenties), oordeelt het EHRM dat de vrees van de regering dat een versoepeling van de regeling niet haalbaar was, gezien het risico van misbruik door financieel sterke partijen met agenda’s “being “fronted” by social advocacy groups”, wat zou leiden tot onzekerheid en juridische procedures. Het EHRM oordeelt dan ook dat het totaalverbod op politieke televisieadvertenties in overeenstemming is met artikel 10 EVRM.

Het is niet volledig duidelijk hoe het EHRM de regulering van online politieke advertenties zou zien in het licht van de verschillende conclusies in *VgT v. Switzerland*, *TV Vest v. Norway* en *Animal Defenders v. UK*. In het bijzonder heeft het EHRM in *Animal Defenders v. UK* een onderscheid gemaakt tussen omroep en internet. Volgens het EHRM had het internet en sociale media in 2013 niet dezelfde “synchronicity or impact” als de omroep die een “immediate and powerful effect [within the] intimacy of the home” heeft.¹⁷² Het EHRM oordeelde destijds dat er “no evidence of a sufficiently serious shift” in de invloeden van de nieuwe media is om de noodzaak van een politiek advertentieverbod in de omroepsector te ondermijnen.¹⁷³

172 Idem, r.o. 119. Zie verder, Cees Plaizier, *Micro-Targeting Consent: A Human Rights Perspective On Paid Political Advertising On Social Media*, LL.M. Thesis, Informatierecht, University of Amsterdam (2018), <http://www.scriptsionline.uva.nl/scriptie/650580>.

173 Idem.

Als *Animal Defenders* in de toekomst echter wordt behandeld als het belangrijkste arrest van het EHRM, kan regulering van online politieke advertenties worden opgelegd, als aan vier criteria wordt voldaan:

- a. Ten eerste, als kan worden aangetoond dat regulering van online politieke advertenties noodzakelijk is om het *risico van verstoring van het publieke debat* te voorkomen, zoals financieel sterke partijen die ongelijke toegang hebben tot online politieke advertenties;
- b. Ten tweede, als er aanwijzingen zijn dat online politieke advertenties *onmiddellijk en krachtig* genoeg effect hebben;
- c. Ten derde, als er een *uitgebreide prelegislatieve raadpleging plaatsvindt* over de regulering van online politieke advertenties; en
- d. Ten vierde, als er een *risico bestaat van misbruik of willekeur* in de situatie zonder de maatregelen, zoals het risico dat financieel sterke partijen met agenda's belangenverenigingen oprichten, en het risico dat financiële plafonds voor advertenties worden omzeild door die financieel sterke partijen door de oprichting van een grote hoeveelheid belangenverenigingen.

Uiteraard ging het in deze gevallen om een *totaalverbod* op betaalde politieke advertenties. Er zijn minder restrictieve regelgevingsopties dan een totaalverbod, zoals transparantieregels, uitgavenbeperkingen of beperkingen die slechts gelden ten tijde van verkiezingen.

ix. Internetdiensten en vrijheid van meningsuiting

Elke regeling die aan internetdiensten wordt opgelegd met betrekking tot politieke advertenties moet in overeenstemming zijn met artikel 10 EVRM. In dit verband heeft het EHRM geoordeeld dat ondernemingen die online platforms en sociale mediaplatforms exploiteren, zelf ook recht hebben op vrijheid van meningsuiting. Zo heeft het EHRM in 2017 bevestigd dat Google Inc. zelf een "recht op vrijheid van meningsuiting" krachtens artikel 10 EVRM geniet,¹⁷⁴ dat verschilt van de rechten gebruikers, gezien de rol van Google Inc. "as the provider of a platform for the free exchange of information and ideas".¹⁷⁵ Het EHRM heeft het belang van online platforms voor de vrijheid van meningsuiting benadrukt. Zo is YouTube volgens het EHRM een "unique platform" en een belangrijk middel voor vrije expressie waar "political content ignored by the traditional media" wordt gedeeld.¹⁷⁶ Ook andere diensten van Google die "the creation and sharing of websites within a group" mogelijk maken zijn volgens het EHRM een middel om vrijheid van meningsuiting uit te oefenen.¹⁷⁷ Het EHRM heeft bij de bespreking van Instagram-posts nogmaals gewezen op de belangrijke rol die het internet speelt bij "enhancing the public's access to news and facilitating the dissemination of information in general".¹⁷⁸

Wanneer internetdiensten een platform bieden voor de uitwisseling van informatie en ideeën, het doorgeven en ontvangen van informatie door anderen, of het creëren en delen van informatie binnen een groep, genieten deze bedrijven op grond van artikel 10 EVRM het recht op vrijheid van meningsuiting. Dit is gebaseerd op het idee dat artikel 10 EVRM de vrijheid van meningsuiting voor "eenieder" garandeert en "[i]t makes no distinction according to the nature of the aim pursued or the role played by natural or legal persons in the exercise of that freedom".¹⁷⁹ Het EHRM heeft dit beginsel bijna drie decennia geleden voor het eerst vastgesteld, toen het de opvatting verwierp dat een vennootschap met winstoogmerk niet de bescherming van artikel 10 EVRM geniet. Artikel 10 EVRM is namelijk van toepassing op iedereen, waaronder "profit-making corporate bodies".¹⁸⁰

174 Tamiz v. the United Kingdom (Application no. 3877/14) 19 September 2017 (dec.), r.o. 87 en 90.

175 Cengiz and Others v. Turkey (Application nos. 48226/10 and 14027/11) 1 December 2015, r.o. 52.

176 Ahmet Yıldırım v. Turkey (Application no. 3111/10) 18 December 2012, r.o. 49.

177 Einarsson v. Iceland (Application no. 24703/15) 7 November 2017, r.o. 46.

178 Idem.

179 Kablis v. Russia (Application nos. 48310/16 and 59663/17) 30 April 2019, r.o. 80.

180 Autronic AG v. Switzerland (Application no. 12726/87) 22 May 1990, r.o. 47.

x. Beperking van schaal, het bereik en de omvang van de publicatie

Eén van de problemen in verband met internetdiensten is de versterkte impact van *content* en de snelle verspreiding ervan. Een mogelijke regulerende maatregel om de amplificatie aan banden te leggen zou kunnen bestaan in regels die de schaal, het bereik en de omvang van de verspreiding beperken. In dit verband heeft het EHRM zich gebogen over de vraag of het bereik en de omvang van de publicatie van *wettige* informatie kan worden beperkt. De belangrijkste zaak is de uitspraak in

Satakunnan Markkinapörssi Oy & Satamedia Oy v. Finland,¹⁸¹ waar een krant de namen en inkomsten van meer dan een miljoen Finse belastingbetalers publiceerde in alfabetische lijsten, gerangschikt naar gemeente en inkomenscategorie. De krant verzamelde de informatie bij de Finse belastingautoriteiten, aangezien deze informatie openbaar toegankelijk was op grond van de Finse wet op de openbaarmaking van informatie. In 2009, na zes jaar procederen, heeft de Finse Raad voor Gegevensbescherming een besluit uitgevaardigd waarin werd vastgesteld dat het publiceren van fiscale gegevens "[was] not prohibited", maar dat het de krant wel verboden was de gegevens te publiceren "in the manner and to the extent" zoals in het onderhavige geval.¹⁸²

Toen de zaak het EHRM bereikte, oordeelde het EHRM dat er geen sprake was van een schending van de vrijheid van meningsuiting, zelfs al was de informatie in kwestie "publicly accessible".¹⁸³ Cruciaal is dat het EHRM oordeelde dat de publicatie geen openbaarmaking van "information, opinions and ideas" vormde, maar veeleer een verspreiding van "masse raw data in unaltered form". Vanwege de lay-out, vorm, inhoud en omvang van de openbaar gemaakte gegevens, kon het ontsluiten van de informatie niet kwalificeren als "contribute to a debate of public interest", noch als "political speech". Het Hof merkte op dat het de uitgever niet is verboden om "taxation data" te publiceren, en hoewel de beperkingen die werden opgelegd ten aanzien van de "quantity of the information" ertoe zou leiden dat de zakelijke activiteiten mogelijk minder rendabel zouden zijn, was dit "not, as such, a sanction within the meaning of the case-law of the Court."

Benadrukt moet worden dat de verspreiding in kwestie geen uiting was van openbaar belang. Het is niet duidelijk hoe het EHRM zou oordelen over een regel die beperking vormt op het bereik, de omvang en de kwantiteit van een politieke advertenties. *Satakunnan Markkinapörssi Oy & Satamedia Oy v. Finland* suggereert echter dat het soms in overeenstemming is met artikel 10 EVRM om de schaal, het bereik en de omvang van de verspreiding te beperken, zelfs wanneer de onderliggende inhoud zelf legaal is.

Het EHRM heeft zich ook gebogen over de amplificatie van het bereik van *content* door bepaalde internetdiensten. In het recente arrest van *M.L. & W.W. v. Germany* heeft het EHRM geoordeeld dat zoekmachines een "amplifying effect on the dissemination of information" kunnen hebben en dat omdat "[the] nature of the activity underlying the publication of information" op individueel niveau, de "obligations of search engines towards the individual who is the subject of the information may differ from those of the entity which originally published the information".¹⁸⁴ Het EHRM erkent dus dat internetdiensten, zoals zoekmachines, verspreiding vergemakkelijken en impact vergroten en dat hun verplichtingen op basis van de aard van hun activiteiten kunnen verschillen.

Met betrekking tot verzoeken om verwijdering van informatie is het EHRM zich ervan bewust is dat "balancing of the interests at stake may result in different outcomes depending on whether a request for deletion concerns the original publisher of the information, whose activity is generally at the heart of what freedom of expression is intended to protect, or a search engine whose main interest is not in

¹⁸¹ *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (App. no. 931/13) 27 June 2017 (Grand Chamber).

¹⁸² *Idem*, r.o. 13.

¹⁸³ *Idem*, r.o. 120.

¹⁸⁴ *M.L. and W.W. v. Germany* (App. nos. 60798/10 and 65599/10) 28 June 2018, r.o. 97.

publishing the initial information about the person concerned, but in particular in facilitating identification of any available information on that person and establishing a profile of him or her".¹⁸⁵ Het EHRM erkent dus wel degelijk een onderscheid tussen een internetdienst, zoals een zoekmachine, en de oorspronkelijke uitgever van informatie, wiens activiteit de kern van de vrijheid van meningsuiting vormt.

xi. Transparantie

De huidige discussies over desinformatie en politieke advertenties in het bijzonder, benadrukken de noodzaak van transparantie. Het Comité van Ministers van de Raad van Europa heeft in zijn Aanbeveling CM/Rec(2018)1 over mediapluralisme en transparantie van media-eigendom het belang van mediapluralisme en diversiteit van de media-inhoud als tegenwicht voor desinformatie onderstreept.¹⁸⁶ In de aanbeveling worden de staten opgeroepen om "encourage social media, media, search and recommendation engines and other intermediaries which use algorithms, along with media actors, regulatory authorities, civil society, academia and other relevant stakeholders to engage in open, independent, transparent and participatory initiatives that:

- improve the transparency of the processes of online distribution of media content, including automated processes;
- assess the impact of such processes on users" effective exposure to a broad diversity of media content."¹⁸⁷

In de Aanbeveling wordt ook een duidelijk standpunt ingenomen over het belang van transparantie met betrekking tot media-inhoud in het gehele multimediale ecosysteem:

"Diversity of media content can only be properly gauged when there are high levels of transparency about editorial and commercial content: media and other actors should adhere to the highest standards of transparency regarding the source of their content and always indicate clearly when content is provided by political sources or involves advertising or other forms of commercial communications, such as sponsoring and product placement. This also applies to hybrid forms of content, including branded content, native advertising, advertorials and infotainment. In cases where these obligations are not fulfilled, provision should be made for proportionate measures to be applied by the competent regulatory authorities."¹⁸⁸

In de Aanbeveling wordt vervolgens een reeks gedetailleerde transparantie-eisen vastgesteld voor media eigendom, organisatie en financiering. De Aanbeveling onderzoekt ook de synergiën tussen transparantie en media-educatie en alfabetisering.

Met betrekking tot politieke advertenties is het belangrijk om op te merken dat er een breed scala aan transparantieregels wordt besproken, waaronder regels voor de herkenbaarheid van betaalde politieke advertenties als zodanig, de informatie over de persoon of groep achter een betaalde politieke advertentie, de informatie over de uitgaven voor betaalde politieke advertenties, de informatie over de criteria die worden gebruikt bij de verspreiding van betaalde politieke advertenties, en de eis dat openbare registers van betaalde politieke advertenties kunnen worden geraadpleegd.¹⁸⁹

¹⁸⁵ Idem.

¹⁸⁶ Raad van Europa, Aanbeveling CM/Rec(2018)1 van het Comité van ministers van de Raad van Europa aan de lidstaten inzake mediapluralisme en transparantie van media-eigendom (7 maart 2018).

¹⁸⁷ *Ibid.*, para. 2.5.

¹⁸⁸ *Ibid.*, para. 2.7.

¹⁸⁹ Zie European Commission, *Tackling online disinformation: a European Approach*, COM(2018) 236 final, para. 3.1.1; and European Commission, *Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*, C(2018) 5949 final, 12 September 2018.

De vraag rijst of, en zo ja, welk soort transparantieregels voor betaalde politieke advertenties in overeenstemming zouden zijn met de vrijheid van meningsuiting. Transparantie is essentieel voor de bevordering en bescherming van mensenrechten, met inbegrip van de vrijheid van meningsuiting.¹⁹⁰ Het EHRM heeft lange tijd de nadruk gelegd op het “right of the public to be properly informed”.¹⁹¹ Hoewel het EHRM zich niet rechtstreeks heeft uitgesproken over de transparantieregels voor betaalde politieke advertenties, heeft het Comité van Ministers in verschillende aanbevelingen, die door het EHRM worden aangehaald, aan de lidstaten het belang van transparantie in het kader van betaalde politieke advertenties benadrukt.¹⁹² Zo wordt in de *Recommendation on media coverage of election campaigns* uit 1999 aanbevolen dat de regelgevingskaders voor betaalde politieke advertenties ervoor moeten zorgen dat het publiek zich ervan bewust is dat een boodschap onderdeel is van een betaalde politieke advertentie,¹⁹³ terwijl in de aanbeveling van 2007 wordt gesteld dat de regelgevingskaders ervoor moeten zorgen dat betaalde politieke advertenties als zodanig gemakkelijk herkenbaar moet zijn.¹⁹⁴ Dezelfde redenering volgend heeft de *Venice Commission* van de Raad van Europa aanbevolen dat de regelgeving moet voorschrijven dat betaalde politieke advertenties “clearly labelled” moet zijn.¹⁹⁵ De *Venice Commission* heeft onlangs een belangrijk rapport over digitale technologieën en verkiezingen goedgekeurd, waarin wordt benadrukt hoe belangrijk het is dat de “[a]ccountability of internet intermediaries in terms of transparency and access to data enhancing transparency of spending, specifically for political advertising” wordt gewaarborgd.¹⁹⁶ En zelfs in de Verenigde Staten, waar de bescherming van de vrijheid van meningsuiting onderworpen is aan een notoir strikt kader, heeft de *Supreme Court* geoordeeld dat de regels inzake de herkenbaarheid van betaalde politieke advertenties -de zogenaamde disclaimers- in overeenstemming zijn met de vrijheid van meningsuiting. Volgens de *Supreme Court* is het mogelijk dat herkenbaarheidsregels “may burden the ability to speak, but they do not prevent anyone from speaking”.¹⁹⁷ In plaats daarvan zorgen dergelijke regels ervoor dat “voters are fully informed about the person or group who is speaking”.¹⁹⁸

Niet alleen zijn transparantieregels in overeenstemming met de regels ten aanzien van vrijheid van meningsuiting, het kan zelfs de plicht zijn van de regering om transparantieregels op te stellen voor betaalde politieke advertenties in enge zin (verkiezingsadvertenties) om de vrijheid van meningsuiting te waarborgen. De *UN Special Rapporteur on the right to freedom of opinion and expression* heeft bijvoorbeeld verklaard dat staten in het kader van verkiezingen zelfs *verplicht zijn* om maatregelen te treffen die ervoor zorgen dat “in all circumstances, paid political advertising is identified as such and not disguised as news or editorial coverage, and that the origin of its financial backing is evident.”¹⁹⁹ De reden hiervoor is dat “informed political debate requires transparency, with respect to the conduct of political organizations, the financing and promotion of political campaigns”,²⁰⁰ en dat elk regelgevend kader voor verkie-

190 Zie UN Human Rights Committee, General comment No. 34, CCPR/C/GC/34, 12 September 2011, para. 1; and generally, Joseph A. Cannataci et al., *Privacy, free expression and transparency* (UNESCO, 2016), <https://unesdoc.unesco.org/ark:/48223/pf0000246610>; en Dirk Voorhoof, ‘Freedom of journalistic news-gathering, access to information and protection of whistleblowers under Article 10 ECHR and the standards of the Council of Europe’ in Onur Andreotti (ed), *Journalism at Risk: Threats, Challenges and Perspectives* (Council of Europe Publishing 2015), p. 106.

191 Zie bijvoorbeeld *The Sunday Times v. the United Kingdom* (Application no. 6538/74) 26 April 1979, r.o. 66.

192 *Animal Defenders International v. the United Kingdom* (Application no. 48876/08) 22 April 2013, para. 73-75; *Orlovskaya Iskra v. Russia* (Application no. 42911/08) 21 February 2017, r.o. 53.

193 Recommendation No. R (99) 15 of the Committee of Ministers to member States on measures concerning media coverage of election campaigns, 9 September 1999.

194 Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of election campaigns, 7 November 2007, section I.6.

195 European Commission for Democracy Through Law, *Compilation of Venice Commission Opinions and Reports concerning Media and Elections*, CDL-PI(2018)006, 4 July 2018, p. 14, [https://www.venice.coe.int/webforms/documents/?pdf=CDL-PI\(2018\)006-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2018)006-e).

196 Joint Report of the Venice Commission and of the Directorate of Information Society and Action Against Crime of the Directorate General of Human Rights and Rule of Law (DGI) on *Digital Technologies and Elections*, CDL-AD(2019)016, 24 June 2019, p. 39, [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2019\)016-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-e).

197 *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010), 366 (interne citaten weggelaten).

198 *Citizens United tegen Federal Election Commission*, 558 U.S. 310 (2010), 368.

199 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Human Rights Council, A/HRC/26/30, 2 July 2014, par. 82, <https://undocs.org/A/HRC/26/30>.

200 *Idem*, par. 5.

zingsprocessen “must have as a key objective the achievement of transparency in all facets of political life and discourse”.²⁰¹

Reeds genoemde beginselen hebben met name betrekking op betaalde politieke advertenties ter bevordering van politieke kandidaten of groepen (verkiezingsadvertenties). Of deze beginselen ook moeten worden toegepast op *issue-based ads* tijdens en buiten de verkiezingsperiode is een nog onbeantwoorde vraag.²⁰² Het is duidelijk dat transparantieregels geen gemakkelijke vangnetformule zijn om alle mogelijke kwalen te verhelpen die met betaalde politieke advertenties gepaard gaan. Bovendien zijn er moeilijke beleidskwesties verbonden aan elk type regulering. Zo heeft het verplicht stellen van openbare registers voor betaalde politieke advertenties, ook wel *ad libraries* genoemd, een aantal vragen opgeworpen.²⁰³ Zoals de vraag of de kopers van de advertenties moeten worden verplicht om advertenties in te dienen voor archivering, of in plaats daarvan een verplichting zou moeten worden opgelegd aan internetdiensten om betaalde politieke advertenties te registreren.²⁰⁴ Dit heeft er soms zelfs toe geleid dat grote internetdiensten een einde hebben gemaakt aan het faciliteren van betaalde politieke advertenties om de complexiteit van de implementatie van reclamebibliotheken te vermijden.²⁰⁵

Uit de bovengenoemde standaarden inzake de vrijheid van meningsuiting volgt dat transparantieregels voor politieke advertenties die specifiek gericht, voldoende duidelijk geformuleerd en proportioneel (d.w.z. bij wet voorzien en noodzakelijk in een democratische samenleving) zijn, in overeenstemming zijn met artikel 10 EVRM. Zoals reeds besproken, moeten goedbedoelde wetsvoorstellen “meticulously crafted” zijn. Zo niet, dan kunnen wetsvoorstellen “enable censorship and silence less powerful communities, threaten online anonymity, and result in the takedown of lawful”.²⁰⁶

xii. Buitenlandse invloeden

In de huidige discussie over desinformatie en politieke advertenties gaat het vooral om desinformatie van “foreign governments”,²⁰⁷ en “foreign actors”.²⁰⁸ De Franse regering betoogt dat de nieuwe Franse Wet op de manipulatie van informatie noodzakelijk was vanwege de “widespread and extremely rapid dissemination of fake news” via “channels offered by social networks and media outlets influenced by foreign states”.²⁰⁹ Een belangrijke overweging in deze discussie is dan ook of het richten van maatregelen op door buitenlandse actoren verspreide informatie in overeenstemming is met artikel 10 EVRM.²¹⁰

Het recht op vrijheid van meningsuiting geldt ongeacht grenzen. Staten mogen de vrije, grensoverschrijdende informatie- en expressiestromen alleen beperken met inachtneming van de strikte beperkingen en verboden waarin de internationale en Europese mensenrechtenwetgeving voorziet. In zijn jurisprudentie inzake grensoverschrijdende uitzendingen heeft het EHRM zijn standaardtest toegepast om na te gaan

²⁰¹ Idem, par. 61.

²⁰² Het opleggen van transparantieregels voor *issue-based ads* buiten de verkiezingstijd werpt ook de vraag op of het mogelijk is om anonieme uitingen te doen, vooral bij kleine campagne groepen. Zie bijvoorbeeld Article 19, *Right to Online Anonymity: Policy Brief* (2015), https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf.

²⁰³ Zie Paddy Leerssen, Jef Ausloos, Brahim Zarouali, Natali Helberger and Claes de Vreese, ‘Platform Ad Archives: Promises and Pitfalls’, 2019, <https://ssrn.com/abstract=3380409>.

²⁰⁴ Het verdient opmerking dat de richtlijn inzake elektronische handel, besproken in deel 5 onder a, de lidstaten verbiedt om bepaalde dienstverleners een algemene verplichting op te leggen om toezicht te houden op de informatie die zij doorgeven of opslaan, dan wel een algemene verplichting om actief op zoek te gaan naar feiten of omstandigheden die op illegale activiteiten wijzen.

²⁰⁵ Zie de landenstudies hieronder, deel 1.

²⁰⁶ Zie Jamie Lee Williams, ‘Cavalier Bot Regulation and the First Amendment’s Threat Model’, Knight First Amendment Institute, 21 August 2019.

²⁰⁷ Report of the independent High level Group on fake news and online disinformation, *A multi-dimensional approach to disinformation* (European Commission, 2018), p. 11.

²⁰⁸ European Commission, *Tackling online disinformation: a European Approach*, COM(2018) 236 final, par. 3.5.

²⁰⁹ Service d’information du Gouvernement, ‘Combating the manipulation of information’, <https://www.gouvernement.fr/en/combating-the-manipulation-of-information>.

²¹⁰ Zie Sue-Lin Wong, Christian Shepherd, and Qianer Liu, ‘Old messages, new memes: Beijing’s propaganda playbook on the Hong Kong protests’, *Financial Times*, 4 September 2019..

of een verbod op buitenlandse uitzendingen een schending van het recht op vrijheid van meningsuiting vormt, waarbij het EHRM ook rekening houdt met overwegingen van pluralisme in de media.²¹¹

De traditionele nadruk van het internationale mensenrechtenrecht op het belang van de grensoverschrijdende dimensie van de vrijheid van meningsuiting wordt in de huidige geglobaliseerde communicatie-omgeving nog belangrijker. Toch heeft de angst voor buitenlandse invloeden in de nationale politiek de discussie over de reikwijdte van de vrijheid van meningsuiting altijd levendig gehouden. Zulke discussies hebben de neiging zich te richten op de vraag hoe journalistiek, media en meer recentelijk sociale media, kunnen bijdragen aan dergelijke invloeden. De opstelling van het EVRM, het IVBPR en de OSCE-verbintenissen inzake de vrijheid van meningsuiting en de vrijheid van de media zijn duidelijk ingegeven door de vrees voor buitenlandse invloed en inmenging.²¹²

Zo werd bij het opstellen van het IVBPR voorgesteld om te erkennen dat de vrijheid van meningsuiting kan worden beperkt ten aanzien van: "The systematic diffusion of deliberately false or distorted reports which undermine friendly relations between peoples and States".²¹³ Hoewel de voorgestelde formulering uiteindelijk niet in de definitieve tekst van artikel 19 IVBPR is opgenomen, geeft zij aan dat de bezorgdheid over desinformatie zeer merkbaar was. Deze bezorgdheid werd verergerd door de verdeeldheid en het wantrouwen in de verdelingen van de Koude Oorlog en de politieke bezorgdheid over de gevaren van oorlogspropaganda en politieke ideologieën.²¹⁴

Artikel 10 EVRM garandeert het recht "[to] receive and impart information and ideas without interference by public authority and *regardless of frontiers*". In dit verband heeft het EHRM geoordeeld dat het recht om informatie te ontvangen een regering in wezen verbiedt om een persoon te beperken in het ontvangen van informatie die anderen hem of haar informatie willen of kunnen geven.²¹⁵ Het beperken van informatie afkomstig uit het buitenland is een inmenging in de vrijheid van meningsuiting, zoals blijkt uit de *Association Akin v. France* uitspraak. In die uitspraak stond een Franse wet centraal die publicaties van "buitenlandse oorsprong" verbood.²¹⁶ Het EHRM oordeelde dat een verbod op de publicatie van een boek in strijd is met artikel 10 EVRM en dat "[s]uch legislation appears to be in direct conflict with the actual wording of paragraph 1 of Article 10 of the Convention, which provides that the rights set forth in that Article are secured regardless of frontiers."²¹⁷

Dit betekent echter niet dat er geen beperkingen mogen worden opgelegd aan informatie uit het buitenland. In het bijzonder gaat het hierbij om informatie die geen legitieme bijdrage levert aan het publiek debat en informatie die bedoeld is om het democratisch proces te verstoren; zolang de beperking maar voldoet aan de vereisten van artikel 10 lid 2 EVRM. Artikel 10 lid 2 EVRM vereist namelijk dat een beperking bij wet is voorzien en noodzakelijk is in een democratische samenleving. In dit verband is de volgende bron bijzonder nuttig: *Committee of Ministers' Recommendation to member states on the free, transboundary flow of information on the Internet*.²¹⁸ In deze aanbeveling wordt verduidelijkt dat de lidstaten verplicht zijn om ervoor te zorgen dat het blokkeren van vermeende illegale inhoud of diensten in overeenstemming is met artikel 10 EVRM; en dat maatregelen ter bestrijding van illegale inhoud of activiteiten op het internet niet mogen leiden tot onnodige en onevenredige gevolgen buiten de grenzen

211 Zie bijvoorbeeld *Groppera Radio AG and Others v. Switzerland*, 28 March 1990, Series A no. 173; *Autronic AG v. Switzerland*, 22 May 1990, Series A no. 178; *Informationsverein Lentia and Others v. Austria*, 24 November 1993, Series A no. 276.

212 OSCE Representative on Freedom of the Media, *Propaganda and Freedom of the Media*, Non-paper, 2015..

213 Voor details, zie: Tarlach McGonagle, 'The development of freedom of expression and information within the UN: leaps and bounds or fits and starts?' in Tarlach McGonagle & Yvonne Donders, Eds., *The United Nations and Freedom of Expression and Information: Critical Perspectives* (Cambridge University Press, 2015), p. 1-51, p. 16.

214 Idem, p. 12.

215 Khurshid Mustafa and Tarzibachi v. Sweden (Application no. 23883/06) 16 December 2008, r.o. 41.

216 Association Ekin v. France (App. no. 39288/98) 17 July 2001, r.o. 26.

217 Idem, r.o. 62.

218 Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet, 1 April 2015, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f20.

van die staat. Voorts moeten de staten er naar streven om maatregelen te ontwikkelen die het minst ingrijpend en het minst verstorend zijn. Deze maatregelen moeten vervolgens ten uitvoer gelegd worden in een transparante en verantwoordelijke procedure.²¹⁹

Een andere beleidsoptie zou kunnen zijn om uitgavenbeperkingen op te leggen voor de verspreiding van bepaalde informatie of de aankoop van politieke advertenties, met name van buitenlandse personen of groepen. Het EHRM heeft zich gebogen over de kwestie van de beperking van de verkiezingsuitgaven in *Bowman v. The United Kingdom*.²²⁰ De zaak betrof een activist die in de aanloop naar een verkiezing 25.000 pamfletten had verspreid en was vervolgd op grond van een bepaling in de Kieswet die de uitgaven voor publicaties "promoting or procuring the election of a candidate" beperkte tot slechts 5 pond voor onbevoegde personen, dat wil zeggen niet-kandidaten of partijen.

Het EHRM oordeelt dat dit uitgavenlimiet "does not directly restrain freedom of expression", maar dat het wel "amounted to a restriction on freedom of expression".²²¹ Het EHRM oordeelde dat de beperking een onevenredige inperking van de vrijheid van meningsuiting was en aldus in strijd met artikel 10 EVRM. De reden hiervoor is dat het uitgavenlimiet was vastgesteld op "as low as £5" en dat de bepaling "operated, for all practical purposes, as a total barrier to [the applicant] publishing information with a view to influencing the voters".²²² Het EHRM was "not satisfied" dat het noodzakelijk zou zijn om de uitgaven te beperken tot 5 pond om het legitieme doel van gelijkheid tussen de kandidaten te bereiken.

De *Bowman* uitspraak bevestigt dat uitgavenlimieten een inmenging vormen op het recht van vrijheid van meningsuiting en dat deze geen volledige belemmering mogen vormen voor de publicatie van informatie tijdens verkiezingen. Het EHRM heeft verklaard dat het in beginsel noodzakelijk kan worden geacht om tijdens verkiezingsperioden het recht op vrijheid van meningsuiting te beperken op een manier die "would not usually be acceptable", teneinde de "free expression of the opinion of the people in the choice of the legislature" te waarborgen.²²³ Er kunnen dus bepaalde beperkingen op het recht van vrijheid van meningsuiting in de zin van artikel 10 EVRM tijdens de verkiezingsperiode worden opgelegd die buiten de verkiezingsperiode misschien niet gepast zouden zijn.

xiii. Beperken van onjuiste informatie tijdens verkiezingstijd

Zoals besproken in de landenstudies, heeft Frankrijk een wet uitgevaardigd die zich richt op onjuiste informatie tijdens de verkiezingen. De Wet op de manipulatie van informatie uit 2018 bepaalt dat een rechtbank gedurende de drie maanden voorafgaand aan een verkiezing een online platform kan gelasten om "*des allégations ou imputations inexactes ou trompeuses d'un fait*" (onnauwkeurige of misleidende beschuldigingen of beschuldigingen van feiten) te verwijderen, die "de oprechtheid van een aanstaande stemmingsronde kunnen veranderen", en op massale schaal "opzettelijk, kunstmatig of geautomatiseerd worden verspreid".²²⁴ Bij het verzoek tot een dergelijk bevel moet de rechter binnen 48 uur na de indiening van dit verzoek om verwijdering oordelen. Men zou kunnen stellen dat een dergelijke bepaling nauwer is dan algemene verbodsbepalingen inzake valse informatie, aangezien het belang dat men wil beschermen specifiek de integriteit van de verkiezingen is.

Opmerkelijk is echter dat het EHRM drie unanieme uitspraken heeft gedaan over een bepaling in de Poolse Kieswet op grond waarvan verkiezingskandidaten bij een regionale rechtbank een verzoek kunnen

219 Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet, 1 April 2015, Principles for the free, transboundary flow of information on the Internet, deel 2.

220 *Bowman v. the United Kingdom* (Application no. 24839/94) 19 February 1998.

221 *Idem*, r.o. 33.

222 *Idem*, r.o. 47.

223 *Idem*, r.o. 43.

224 Artikel 1 Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information,, <https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte>. Zie Blocman, A., 'Law on manipulation of information, validated by the Constitutional Council, is published', IRIS, 2019 <http://merlin.obs.coe.int/iris/2019/2/article11.en.html>.

indienen om de publicatie van campagnemateriaal of verklaringen die “onjuiste gegevens of informatie” bevatten, te beperken, waarbij de rechtbank de aanvraag binnen 24 uur moet onderzoeken.²²⁵ Met name heeft het EHRM in alle drie de arresten, alsook in een arrest van 2019, vastgesteld dat verschillende procedures op grond van deze bepaling in strijd zijn met artikel 10 EVRM.²²⁶ In de zaak *Brzeziński v. Poland* heeft het EHRM bijvoorbeeld unaniem een schending van artikel 10 vastgesteld, aangezien de nationale rechtbanken de verklaringen van een plaatselijke politicus tijdens een verkiezing “onmiddellijk als leugens” hadden aangemerkt en “[b]y following such an approach the domestic courts effectively deprived [the politician] of the protection afforded by Article 10”.²²⁷ Voorts heeft het EHRM in de zaak *Kwiecień v. Poland* ernstige tekortkomingen vastgesteld in het kader van een procedure wegens “onjuiste informatie” tijdens een verkiezing, en heeft het EHRM zelfs geoordeeld dat “[the] fairness of the proceedings may be called into question”.²²⁸ Evenzo heeft het EHRM in de zaak *Kita v. Poland* unaniem een schending van artikel 10 EVRM vastgesteld in verband met “untrue information”, omdat het van oordeel was dat de rechtbanken “unreservedly qualified all of [the statements] as statements which lacked any factual basis” en dat de “standards applied” door de rechtbank niet “compatible with the principles embodied in Article 10” zijn.²²⁹ Om die redenen kan in het algemeen worden geconcludeerd dat er ernstige twijfels bestaan over de verenigbaarheid van wetgeving die gericht is op onjuiste informatie maar die geen onderzoek mogelijk maakt naar de vraag of er sprake is van reputatieschade of de persoonlijkheidsrechten van de betrokkenen.

B. De Nederlandse Grondwet

De bescherming van de vrijheid van meningsuiting is naast het EVRM ook vastgelegd in artikel 7 van de Nederlandse Grondwet (“GW”). Dit artikel beschermt niet de uitings- of ontvangstvrijheid als zodanig, maar het biedt een specifieke bescherming tegen voorafgaand verlof (censuur) door de overheid. De bepaling maakt een onderscheid in de bescherming die het biedt al naar gelang het medium waarmee de uiting geopenbaard wordt. Artikel 7 GW biedt bescherming voor op “gedachten en gevoelens” geopenbaard via: de drukpers (lid 1), de radio en televisie (lid 2) en alle overige media zoals theater, spraak of dans (lid 3). In het vierde lid wordt handelsreclame volledig van bescherming uitgesloten.

In de huidige Nederlandse rechtspraak wordt hoofdzakelijk aangesloten bij de Europese jurisprudentie op basis van het EVRM en mist de Grondwet vaak toepassing. Wel nog interessant voor de regulering van desinformatie en een begrip van de veranderde context waarin overheden zich bevinden ten aanzien van nieuwe verspreidingsmiddelen op internet, is de verspreidingsleer. Op basis van dit leerstuk kan de verspreiding van geschriften in de publieke ruimte op decentraal niveau gereguleerd worden. Het is volledig in jurisprudentie ontwikkeld, met als expliciet doel deze normering op gemeentelijk niveau mogelijk te maken.²³⁰ Lokale regulering wordt namelijk noodzakelijk geacht voor het handhaven van de openbare orde.²³¹

In de kern komt de verspreidingsleer op het volgende neer. Om decentrale regulering constitutioneel mogelijk te maken, wordt in het leerstuk een principieel onderscheid gemaakt tussen de openbaringsvrijheid enerzijds, en de vrijheid tot verspreiding anderzijds. Waar de drukpersvrijheid uit artikel 7 lid 1 GW expliciet de openbaringsvrijheid beschermt, wordt de verspreidingsvrijheid als connex recht bij de

²²⁵ Zie *Brzeziński v. Poland* (Application no. 47542/07) 25 July 2019, r.o. 28.

²²⁶ Zie *Kwiecień v. Poland* (Application no. 51744/99) 9 January 2007; *Kita v. Poland* (Application no. 57659/00) 8 July 2008; and *Brzeziński v. Poland* (Application no. 47542/07) 25 July 2019.

²²⁷ *Brzeziński v. Poland* (Application no. 47542/07) 25 July 2019, r.o. 58.

²²⁸ *Kwiecień v. Poland* (Application no. 51744/99) 9 January 2007, r.o. 55.

²²⁹ *Kita v. Poland* (Application no. 57659/00) 8 July 2008, r.o. 51.

²³⁰ Kistenkas, F., *Vrije straatcommunicatie. De rol van de lokale overheid bij de regulering van de uitingsvrijheid in rechtsvergelijkend perspectief*, Deventer/Arnhem: Kluwer/Gouda Quint 1989 p. 26.

²³¹ De Meij, J.M. e.a., *'Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief'*, Amsterdam: Cramwinckel 2000 p. 112; R.E. de Winter, *'De heersende leer: honderd jaar verspreidingsjurisprudentie: 1892-1992'*, Den Haag: SDU 1993 p. 18.

openbaringsvrijheid ingelezen. Het doel indachtig is het verschil tussen het “hoofdrecht” van de openbaringsvrijheid en het “afgeleide recht” tot verspreiding logischerwijs te vinden in de beperkingsmogelijkheden: de openbaring zelf kan slechts bij formele wet beperkt worden, maar de verspreiding ook bij materiële wet.

De formulering “volgens de wet” van het openbaringsrecht in het eerste lid van artikel 7 maakt namelijk dat de openbaring slechts bij formele wet beperkt kan worden. Het connexe recht tot verspreiding kan daarentegen door een wet in materiële zin beperkt worden, nu het losgemaakt is van het openbaringsrecht en dus de formulering uit artikel 7 GW. De tijd, plaats en wijze van verspreiding kan hierdoor in lagere regelgeving genormeerd worden.²³² Relevant om te bedrukken op dit punt is dat deze openbaringsvrijheid uit artikel 7 GW in tegenstelling tot artikel 10 EVRM ongelimiteerd beperkt kan worden zolang het bij wet in formele zin plaatsvindt.

Het arrest *APV Tilburg*²³³ uit 1950 geeft de nog steeds als standaard geldende criteria op basis waarvan dit connexe verspreidingsrecht op lokaal niveau beperkt mag worden: (i) de beperkingen mogen niet zien op de inhoud van de uiting; (ii) een verspreidingsmiddel met zelfstandige betekenis mag niet in zijn algemeenheid verboden worden en (iii) de beperking moeten een gebruik van enige betekenis overlaten.

Dit eerste vereiste verzekert de scheiding tussen het verspreidings- en openbaringsrecht door beperkingen op het verspreidingsrecht los te koppelen van de openbaring. De lokale overheid kan de “tijd, plaats of wijze” van de verspreiding normeren, zo lang dit niet raakt aan of gebeurt op basis van inhoudelijke overwegingen. Het tweede criterium voorkomt dat bepaalde methodes van informatieverbreiding in de publieke ruimte volledig verboden worden. Het is nader geconcretiseerd in het arrest *Eindhoven I*,²³⁴ waar een verbod op strooibiljetten onverbindend verklaard werd omdat het een verspreidingsmiddel is dat “zelfstandige betekenis heeft en met het oog op die verspreiding in een bepaalde behoefte kan voorzien”. Andere voorbeelden zijn het aanplakken van posters, het uitdelen van bijbels en het aanbrengen van letters op een gebouw.²³⁵

Het derde criterium verzekert dat er van ieder verspreidingsmiddel ook daadwerkelijk een gebruik van enige betekenis overblijft. In het arrest *Nuth*²³⁶ werd dit additionele criterium ontwikkeld om te voorkomen dat de waarborgen omzeild werden door een zelfstandig verspreidingsmiddel niet volledig te verbieden, maar wel effectief onbruikbaar te maken. Tegenwoordig worden deze twee laatste criteria vervangen door de proportionaliteits- en subsidiariteitstoets van artikel 10 lid 2 EVRM.²³⁷

De verspreidingsleer is zonder meer van toepassing op politieke advertenties in de fysieke publieke ruimte. De verspreiding van politieke affiches, posters en flyers wordt regelmatig op gemeentelijk niveau gereguleerd. Of de verspreiding van politieke advertenties en desinformatie door internetdiensten ook beperkt kan worden door de verspreidingsleer is echter onzeker.

Het leerstuk is namelijk in het verleden alleen toegepast in de *fysieke* publieke ruimte en onduidelijk is in hoeverre het ook gelding heeft in een *online* context. Vragen zoals wat gezien moet worden als

232 Zie het standaardarrest HR 28 november 1950, NJ 1951, 137 (*APV Tilburg*); J.M. De Meij e.a., *‘Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief’*, Amsterdam: Cramwinckel 2000 p. 113; De Winter, R.E., *‘De heersende leer: honderd jaar verspreidingsjurisprudentie: 1892-1992’*, Den Haag: SDU 1993 p. 113; Asscher, L. F. *‘Communicatiegrondrechten: een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving’*, 2002, Amsterdam: Otto Cramwinckel. p.70.

233 HR 28 november 1950, NJ 1951, 137 (*APV Tilburg*).

234 HR 27 februari 1951, NJ 1951, 472 (*Eindhoven I*); Kistenkas, F. *‘Vrije straatcommunicatie. De rol van de lokale overheid bij de regulering van de uitingsvrijheid in rechtsvergelijkend perspectief’*, Deventer/Arnhem: Kluwer/Gouda Quint 1989 p. 31; De Meij, J.M. e.a., *‘Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief’*, Amsterdam: Cramwinckel 2000 p. 115.

235 Schutgens, R.J.B., *‘Jezus Redt. Beperking van de uitingsvrijheid door welstandseisen’*, *Ars Aequi*, 2011, p. 136-139.

236 HR 17 maart 1953, NJ 1953, 389 (*Nuth*).

237 Dommering, E.J., *‘De nieuwe Nederlandse Constitutie en de informatietechnologie’*, *Computerrecht*, 2000, nr. 4, blz. 182 – 183.

een “online” zelfstandig verspreidingsmiddel, hoe beperkingen naar “tijd en plaats” uitgelegd moeten worden, en of in een digitale omgeving het onderscheid tussen openbaren en verspreiden als zodanig gemaakt kan worden, zijn nog onbeantwoord. Beperkingen naar tijd zijn nog het makkelijkst voor te stellen door aan te sluiten bij het bestaan van tijdelijke maatregelen, beperkingen in de zin van verschillende dagdelen is daarentegen moeilijker voor te stellen. De afbakening van maatregelen naar plaats werpt vervolgens nog meer vragen op nu de jurisprudentie expliciet uitgaat van een fysieke locatie. Wellicht dat in plaats van het definiëren van een “plaats” op het internet, gekeken wordt naar de achterliggende rechtspersonen of de specifieke dienst die aangeboden worden ter afbakening van een maatregel.

Vervolgens werpt de toepassing van de verspreidingsleer in een online omgeving ook vragen op met betrekking tot de inzet van gemeentelijke bevoegdheden. Hoe kan, bijvoorbeeld, een gemeente op het internet binnen de territoriale grenzen van zijn bevoegdheid blijven en wanneer is er sprake van een gevaar voor de openbare orde in een digitale context, concreet genoeg om in te grijpen? Het is, los van de spanning die dit op zou leveren met artikel 10 EVRM en het Europese recht met betrekking tot internetdiensten, natuurlijk mogelijk om de regulering op lokaal niveau los te laten en op nationaal niveau bij wet in formele zin de online verspreiding van desinformatie te reguleren. Wanneer een wet in formele zin gebruikt wordt, geeft artikel 7 GW geen restricties voor de inhoud of reikwijdte van de beperking en is de verspreidingsleer formeel niet van toepassing. De normen ontwikkeld in de jurisprudentie van dit Nederlandse leerstuk kunnen natuurlijk wel dienen als leidraad voor de ontwikkeling van dergelijke wetgeving, ook in het kader van de subsidiariteits- en proportionaliteitsvereisten van artikel 10 EVRM. Hoewel de juridische doctrine met betrekking tot artikel 7 GW dus een aantal relevante inzichten kan bieden, levert het uiteindelijk weinig antwoorden op ten aanzien van de voorliggende problematiek

C. Samenvatting & conclusie

In dit hoofdstuk zijn de relevante aspecten van het recht op vrijheid van meningsuiting voor de regulering van desinformatie en politieke advertenties besproken. Een aantal belangrijke punten worden hier op een rij gezet. Het recht op vrijheid van meningsuiting is niet alleen een recht dat tegen de regering wordt uitgeoefend; het houdt ook positieve verplichtingen in voor de staat om een pluralistische omgeving te garanderen voor het publieke debat van alle lagen van de democratische samenleving. Deze verplichting houdt onder meer in dat de regering de plicht heeft om ervoor te zorgen dat het pluralistische democratische debat niet wordt verstoord en dat financieel machtige groepen geen concurrentievoordelen krijgen door middel van betaalde politieke advertenties, wat een vrij en pluralistisch politiek debat kan belemmeren.

Het hoofdstuk ging vervolgens in op verschillende aspecten van desinformatie en besprak dat een specifieke regeling van desinformatie louter op basis van het feit dat informatie onjuist of misleidend is, zonder aanvullende eisen, zoals het schaden van iemands reputatie of de rechten van een ander, moeilijk te rijmen valt met de normen voor de vrijheid van meningsuiting. Voorts zou het zeer problematisch zijn om valse informatie te verbieden louter op grond van het feit dat zij het publiek schade kan berokkenen. Een poging om onjuiste of misleidende informatie te reguleren op grond van het feit dat deze met het oog op economisch gewin wordt verspreid, zou ook problematisch zijn in het kader van artikel 10 EVRM. Een inhoudelijke regulering van desinformatie zou alleen gericht moeten zijn op informatie op basis van de bescherming van de rechten van anderen (bijv. reputatie, privacy, waardigheid) of een legitiem overheidsbelang, zoals het voorkomen van wanorde (bijv. verstoring van de openbare orde).

Cruciaal is dat een betaalde politieke advertentie wordt beschouwd als politieke meningsuiting in de zin van artikel 10 EVRM en dat het EHRM een brede visie heeft op wat politieke advertenties zijn. Het omvat niet alleen advertenties van politieke partijen die op zoek zijn naar stemmen (verkiezingsadvertenties), maar ook advertenties over zaken van algemeen belang (*issue ads*). Nu politieke advertenties een vorm van beschermde politieke uitingen zijn, kan regulering van politieke advertenties in bepaalde beperkte

situaties verenigbaar zijn met artikel 10. Wel moeten de redenen relevant en toereikend zijn met betrekking tot de specifieke inmenging in de rechten uit hoofde van artikel 10. Het EHRM zal de nationale wetgevingskaders zorgvuldig onderzoeken om ervoor te zorgen dat de wetgeving inzake politieke advertenties niet buitensporig wordt gebruikt om de journalistieke berichtgeving over een politiek debat of het recht van een campagnegroep om zich in te laten met politieke uitingen te verstikken. Verder is het ook duidelijk dat dienstverleners zelf een duidelijk recht op vrijheid van meningsuiting hebben. Dit is gebaseerd op hun cruciale rol als platform voor de vrije uitwisseling van informatie en ideeën, het verbeteren van de toegang van het publiek tot nieuws en het vergemakkelijken van de verspreiding van informatie in het algemeen. Het EHRM is zich bewust van de wijze waarop internetdiensten de amplificatie van de inhoud vergemakkelijken en door de aard van hun activiteiten kunnen hun verplichtingen verschillen.

In dit hoofdstuk wordt ook gewezen op het belang dat wordt gehecht aan het transparantiebeginsel, dat essentieel is voor de bevordering en bescherming van de vrijheid van meningsuiting. De transparantieregels voor politieke advertenties zijn in overeenstemming met artikel 10 van het EVRM wanneer zij strikt gericht, voldoende duidelijk geformuleerd en evenredig zijn. In de specifieke context van de verkiezings-tijd kan de regering namelijk de plicht hebben om tijdens de verkiezingen transparantiemaatregelen te nemen met betrekking tot betaalde politieke advertenties. Dergelijke maatregelen moeten echter strikt op maat worden gesneden om het risico van (zelf)censuur te vermijden, negatieve gevolgen voor de participatie en vertegenwoordiging van minderheidsgroepen, ongepaste beperkingen van de anonimiteit op het internet of het verdwijnen van legale politieke uitingen te voorkomen. Ten slotte werd het kader voor de vrijheid van meningsuiting onderzocht dat van toepassing is op de beperking van de buitenlandse invloed, met inbegrip van de beperkte mogelijkheden om beperkingen op te leggen aan informatie uit het buitenland en beperkingen op de uitgaven die de vrijheid van meningsuiting tijdens verkiezingen beperken.

Er kan worden aanbevolen dat om desinformatie aan te pakken op een manier die in overeenstemming is met het recht op vrijheid van meningsuiting, het noodzakelijk is om uit te gaan van de veronderstelling dat de staat de positieve verplichting heeft om pluralisme binnen het democratisch proces te garanderen. Een passend mechanisme in dit verband is wat het EHRM *algemene maatregelen* noemt, die van toepassing zijn op vooraf bepaalde situaties en als zodanig niet inhoudelijk gericht zijn, noch een voorafgaande toetsing is ten aanzien van een individuele daad van meningsuiting.

5. Europees regelgevend kader

- Het EU-kader bestaat uit de Richtlijn Elektronische Handel, de Richtlijn Audiovisuele Mediadiensten, Direct Marketing regulering, commerciële regulering, de AVG en zelfregulering;
- De daadwerkelijk toepasselijke regelgeving is afhankelijk van het type internetdienst, de inhoud van de desinformatie en de context waarbinnen deze wordt verspreid (bv. commercieel, politiek, privé);
- Het betreft een zeer dynamisch rechtsgebied. Veel elementen van het relevante Europees-rechtelijk kader zijn van recente datum (AVG & AVMD-richtlijn) of worden momenteel herzien (e-Privacy Verordening en de REH).
- Internetdiensten zelf zijn ook actief bezig met het ontwikkelen van beleid om desinformatie aan te pakken.

In dit hoofdstuk en in het volgende hoofdstuk wordt ingegaan op de relevante regelgeving voor desinformatie in Nederland. In dit hoofdstuk wordt specifiek aandacht besteed aan de relevante wet- en regelgeving van de Europese Unie, terwijl het volgende hoofdstuk, hoofdstuk 6, zich richt op de nationale wet- en regelgeving.

Het is belangrijk op te merken dat de internetdiensten in kwestie vanuit het oogpunt van het EU-recht verschillende diensten aanbieden. Zoals hieronder wordt besproken, kan bijvoorbeeld YouTube, als videoplatform, onderworpen zijn aan de EU-regels voor audiovisuele mediadiensten; WhatsApp, als elektronische communicatiedienst, kan onderworpen zijn aan de EU-telecommunicatieregels of directmarketingregels; terwijl Google Search, als zoekmachine,²³⁸ onderworpen kan zijn aan de EU-regels voor elektronische handel door diensten van de informatiemaatschappij. Als zodanig wordt in dit hoofdstuk een aantal relevante EU-instrumenten behandeld en hoe deze zich verhouden tot de verschillende aangeboden diensten.

A. Richtlijn elektronische handel

De regulering van internetdiensten met betrekking tot politieke advertenties moet in lijn zijn met de richtlijn elektronische handel ("REH"), die regels bevat voor het opleggen van toezicht verplichtingen en vrijstellingen van aansprakelijkheid voor bepaalde dienstverleners.²³⁹ In de eerste plaats bevat de richtlijn voorwaardelijke aansprakelijkheidsvrijstellingen, of *safe harbour*, voor drie soorten diensten verleend door internettussenpersonen: eenvoudige doorgifte (artikel 12), caching (artikel 13) en hosting (artikel 14). Belangrijk is dat artikel 15 van de richtlijn bepaalt dat het de lidstaten van de EU verboden is een algemene verplichting op te leggen aan de dienstverleners die onder de artikelen 12 tot en met 14 vallen, om toezicht te houden op de informatie die zij doorgeven of opslaan, of een algemene verplichting om actief te zoeken naar feiten of omstandigheden die wijzen op illegale activiteiten.

De eerste vraag die zich dus zou voordoen, is of de betrokken dienst, met inbegrip van zijn reclamefunctie, zich zou kunnen beroepen op de bescherming die een van de bepalingen die de REH biedt. De diensten

²³⁸ Zie ook de onlangs vastgestelde Verordening (EU) 2019/1150 betreffende de bevordering van eerlijkheid en transparantie voor zakelijke gebruikers van online-bemiddelingsdiensten, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R1150&from=EN#d1e563-57-1>, waarin nieuwe transparantieregels voor zoekmachines worden vastgesteld voor de belangrijkste parameters die bepalend zijn voor de rangorde.

²³⁹ Zie Joris van Hoboken et al., *Hosting Intermediary Services and Illegal Content Online: Een analyse van de reikwijdte van artikel 14 van het EG-Verdrag in het licht van de ontwikkelingen in het onlinedienstenlandschap* (Europese Unie, 2018), https://www.ivir.nl/publicaties/download/hosting_intermediary_services.pdf.

die in dit verslag aan de orde zijn, vallen onder zowel artikel 14 (onlinemediaplatformen, sociale media, sociale media en zoekmachines) als artikel 12 (communicatiediensten). Om te beginnen moet hier worden opgemerkt dat de reikwijdte van de bepalingen inzake de *safe harbour* in de lidstaten en op Europees niveau het voorwerp is geweest van rechtszaken en dat hierover hevige discussies worden gevoerd.²⁴⁰ De Europese Commissie bereidt momenteel voorstellen voor om deze bepalingen in de REH aan te passen door middel van de voorgestelde Digital Services Act. Duidelijkheid scheppen over het toepassingsbereik van de artikelen is een belangrijk onderwerp van deze herziening.²⁴¹ In Nederland zijn deze artikelen 12 tot en met 14 REH gecodificeerd, zonder belangrijke afwijkingen van de richtlijn, in artikel 6:196 van het Burgerlijk Wetboek. De regering oordeelde dat artikel 15 REH geen codificatie van het Nederlandse recht nodig heeft, omdat het bestaat uit een zorgplicht gericht op de Nederlandse staat waaraan zij reeds door middel van de richtlijn zelf gebonden is.²⁴²

De bepalingen in de REH zijn ten aanzien van desinformatie in twee aspecten relevant. Ten eerste, wat betreft de aansprakelijkheid van dienstverleners voor illegale of onwettige inhoud of activiteiten. Ten tweede, wat betreft de soorten verplichtingen die dienstverleners kunnen worden opgelegd om toezicht te houden op hun dienstenactiviteiten en die in aanmerking komen voor bescherming uit hoofde van de artikelen 14 en 15 REH. Het aanpakken van de onduidelijkheid over de reikwijdte van deze bepaling is zoals gezegd op de wetgevingsagenda van de nieuwe Europese Commissie geplaatst.

Volgens artikel 14 REH is een hosting provider een “dienst van de informatiemaatschappij” die bestaat uit de opslag van door een afnemer van de dienst verstrekte informatie. Het artikel bepaalt verder dat deze dienstverlener niet aansprakelijk is voor de informatie die op verzoek van een afnemer van de dienst is opgeslagen. Belangrijk is dat deze vrijstelling alleen van toepassing is als de dienstverlener niet daadwerkelijk op de hoogte is van illegale of onrechtmatige activiteiten of informatie, of wanneer hij/zij dergelijke kennis of bewustwording heeft verkregen en snel handelt om de informatie te verwijderen of de toegang tot de informatie te blokkeren.

In de jurisprudentie van het Hof van Justitie van de Europese Unie is voorts bepaald dat de activiteiten van een dienst “neutraal” en “passief” moeten zijn om een beroep te kunnen doen op artikel 14 van het EG-Verdrag, en dat deze dienst geen actieve rol mag hebben gespeeld “om hem kennis te geven van of controle te geven over de opgeslagen gegevens”.²⁴³ Met name met betrekking tot zoekmachines heeft het Hof van Justitie van de Europese Unie zoekmachines niet uitgesloten van het toepassingsgebied van artikel 14 van het EG-Verdrag en heeft het geconcludeerd dat reclame-elementen van een zoekmachine kunnen worden gedekt (Google Search).²⁴⁴ De conclusie is dat, afhankelijk van de specifieke kenmerken van de dienst, betaalde reclamedienstenactiviteiten van de betrokken dienstverleners onder de artikelen 14 en 15 van het EG-Verdrag kunnen vallen, gezien de mogelijkheid dat adverteerders via hun diensten illegale en schadelijke inhoud zouden kunnen verspreiden.

Dit betekent dat in dergelijke gevallen alle verplichtingen uit hoofde van het Nederlandse recht die de facto een algemene controleverplichting zouden vormen, in strijd zouden zijn met het Europese recht. Anderzijds doet artikel 14 REH geen afbreuk aan de mogelijkheid voor een rechtbank om van de dienstverlener te verlangen dat hij een onwettige communicatie beëindigt of voorkomt, noch aan de mogelijkheid voor de lidstaten om procedures vast te stellen voor het verwijderen of ontoegankelijk maken van informatie.

²⁴⁰ Voor een bespreking van het toepassingsgebied van artikel 14 van het EG-Verdrag, zie *ibid.*

²⁴¹ Bjarke Smith-Meyer, Lili Bayer en Jakob Hanke, ‘EU-ambtenaren zweven 100B euro voor Europese bedrijven’, Politico 25 augustus 2019, volledig document: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/08/clean_definite2.pdf, blz. 24.

²⁴² Tweede Kamer, vergaderjaar 2001-2002, 28 197, nee. 3, p. 27.

²⁴³ C-236/08 - Google France, par. 120.

²⁴⁴ *Idem*, p. 12.

Een nieuwe aanpak met betrekking tot de aansprakelijkheid en verantwoordelijkheid van internetdiensten, bestaat erin van dienstverleners te eisen dat zij informatie bekendmaken over hun inspanningen om illegale en schadelijke inhoud op hun diensten aan te pakken en over de risico's die hun diensten hebben met het oog op de mogelijkheid van illegale en/of schadelijke informatie en ideeën. Dergelijke bekendmakingen kunnen worden gecombineerd met toezicht, waardoor nieuwe ruimte wordt gecreëerd voor een doeltreffende regelgeving met betrekking tot internetdiensten, in de overigens sterk omstreden kwestie van de wettelijke aansprakelijkheid voor illegale online-inhoud.²⁴⁵

Een ander perspectief op het aansprakelijkheidskader betreft de veelgehoorde kritiek dat het wettelijk kader van de REH hostingproviders ertoe aanzet zich te veel te richten op het verwijderen van illegale door gebruikers gegenereerde inhoud, waarbij de bescherming van rechtmatige *content* wordt verwaarloosd. Het feit dat hostingproviders zich aan hun aansprakelijkheid kunnen onttrekken en door de *safe harbour* beschermd kunnen worden wanneer zij "prompt" inhoud verwijderen nadat zij kennis hebben gekregen van het (vermeende) onrechtmatige of illegale karakter van de inhoud, betekent dat het voor hostingproviders de moeite waard is om door gebruikers gemaakte inhoud zonder veel toezicht te verwijderen. Dit betekent dat het *safe harbour*-kader de hostingproviders ertoe aanzet om legale inhoud te verwijderen zodra er twijfel bestaat over de wettigheid of rechtmatigheid ervan. De kritiek is dat dit systeem de vrijheid van meningsuiting van de gebruikers van wie de inhoud is verwijderd onvoldoende beschermt en dat het controversieel taalgebruik bedreigt.²⁴⁶

Naast het aansprakelijkheidskader voor internettussenpersonen voorziet de REH ook in een aantal belangrijke regels die specifiek voor reclame gelden.²⁴⁷ Van bijzonder belang zijn de informatievereisten van artikel 6 van de richtlijn, die vrijwel letterlijk zijn geïmplementeerd in artikel 3:15e van het Burgerlijk Wetboek.²⁴⁸ Hoewel de REH een aantal algemene informatievereisten oplegt aan dienstverleners, heeft artikel 6 REH specifiek betrekking op "commerciële communicatie", waar ook reclame onder valt. De verplichting geldt alleen voor commerciële reclame die deel uitmaakt van een "dienst van de informatiemaatschappij", die per definitie uitsluitend langs elektronische weg, zoals internet of radio, wordt aangeboden.²⁴⁹

De bepaling schrijft voor dat handelsreclame op het internet als zodanig herkenbaar moet zijn. De adverteerder moet duidelijk te identificeren zijn en de voorwaarden voor eventuele aanbiedingen helder. Ook moet spam via "elektronische post" direct bij ontvangst, en dus voor opening van de e-mail, als zodanig te herkennen zijn.²⁵⁰ Uit Nederlandse rechtspraak blijkt dat de gegevens noodzakelijk voor identificatie niet in de advertentie zelf opgenomen te hoeven worden. Voldoende is dat "duidelijk en herkenbaar" verwezen wordt naar waar die gegevens te vinden zijn.²⁵¹

De actieve handhaving van deze, en andere in de Richtlijn voorgeschreven transparantie bepalingen wordt op basis van artikel 3:15f lid 3 BW uitgevoerd door de controleurs van het FIOD (de bij de Belastingdienst ondergebrachte Fiscale Inlichtingen- en Opsporingsdienst – Economische Controle dienst).²⁵² Deze controleurs hebben de bevoegdheid om op basis van 3:305a BW een collectieve actie op te zetten.

²⁴⁵ De Duitse NetzDG, het Britse Witboek en een recent rapport van de Franse regering bevatten elementen in deze richting.

²⁴⁶ Keller, D. (2018), "Internetplatforms: Opmerkingen over Spraak, Gevaar en Geld" (13 juni 2018). *Aegis Paper Series van Hoover Institution*, nr. 1807, 2018. Verkrijgbaar bij SSRN: <https://ssrn.com/abstract=3262936>; Angelopoulos, C., Brody, A., A., e.a. (2015) "Study of fundamental rights limitations for online enforcement through selfregulation", Institute for Information Law. beschikbaar op: <https://www.ivir.nl/publicaties/download/1796>.

²⁴⁷ Artikel 5.A, geïmplementeerd in artikel 6:196c van het Burgerlijk Wetboek.

²⁴⁸ Wanneer de tekst van de richtlijn niet woordelijk is overgenomen, staat de tekst wel in de toelichting. Het artikel zal in ieder geval moeten worden geïnterpreteerd in overeenstemming met de richtlijn. Zie Schaub, M.Y., *Groene Serie Vermogensrecht*, artikel 3:15e Burgerlijk Wetboek, noot 4.3.

²⁴⁹ Artikel 3:15 quinquies, lid 3, van het Burgerlijk Wetboek; artikel 1, onder a), van Richtlijn (EU) 2015/1535.

²⁵⁰ Kamerstukken II 2001-2002, 28 197, nr. 3, p. 19-20 en 43.

²⁵¹ Rb Rotterdam, 25 februari 2010, ECLI:NL:RBROT:2010:BL6368 onder verwijzing naar *Kamerstukken II 2001-2002*, 28 197, nr. 3, p. 42.

²⁵² Zie artikel 15f lid 3 boek 3 BW jo. artikel 1 sub 4 Wet op de economische delicten.

Dit werd nodig geacht omdat schade in een individueel geval moeilijk aantoonbaar is, en een collectief verband zich hier beter voor leent.²⁵³ Daarnaast zijn de transparantieverplichtingen ook aangemerkt als overtreding in artikel 2 lid 4 Wet op de economische delicten, en kunnen de bepalingen ook krachtens deze wet gehandhaafd worden. Het effectieve toezicht op deze bepaling is echter onderontwikkeld en in de wandelgangen wordt het als een wat vergeten bepaling beschouwd.

B. Algemene Verordening Gegevensbescherming

Het gebruik van persoonsgegevens in het communicatielandschap is aanzienlijk toegenomen. Zoals vermeld in hoofdstuk 2, kunnen politieke advertenties op internetdiensten persoonsgegevens verzamelen en gebruiken om gesponsorde berichten gericht te verspreiden. Relevante internetdiensten, zoals Facebook of Google, zorgen voor zeer granulaire en datagestuurde mogelijkheden voor gerichte communicatie met het online publiek. De Algemene Verordening Gegevensbescherming ("AVG") is in dit verband zeer relevant, aangezien het van toepassing is op de verwerking van persoonsgegevens en vereist dat een dergelijke verwerking eerlijk, rechtmatig en transparant is, de rechten van de betrokkenen beschermd worden en dat de regelgeving onder onafhankelijk toezicht wordt geplaatst. Onafhankelijke gegevensbeschermingsautoriteiten zijn begonnen kennis te nemen van de praktijken op dit gebied en hebben een leidende rol gespeeld bij het onderzoek naar problematische praktijken, zoals in het geval van Cambridge Analytica en Facebook.

The *European Data Protection Board* ("EDPB") heeft richtlijnen opgesteld voor het gebruik van persoonsgegevens in het kader van politieke campagnes, net zoals een aantal nationale gegevensbeschermingsautoriteiten (België, Frankrijk, Ierland, Polen en het Verenigd Koninkrijk).²⁵⁴ De Nederlandse Autoriteit Persoonsgegevens is in februari 2019 gestart met een onderzoek naar het gebruik van persoonsgegevens in het kader van politieke campagnes.²⁵⁵ Het onderzoek richt zich met name op de inzet van derden die de politieke partijen bijstaan bij hun verkiezingscampagnes.

De brede toepasbaarheid van de AVG, zijn brede doelstellingen om de fundamentele rechten en vrijheden van individuen in de context van de verwerking van persoonsgegevens te beschermen en zijn relatief open bepalingen die moeten worden geïnterpreteerd en toegepast op verschillende contexten, maken dat het een belangrijke rol kan spelen bij de bescherming van de rechten en vrijheden van internetgebruikers. Met betrekking tot desinformatiecampagnes kan de AVG een belangrijke algemene waarborg zijn voor de bescherming tegen onevenredige verwerking van persoonsgegevens. Terwijl het volgens de Amerikaanse wetgeving de platforms vrij staat om de informatie die zij over hun publiek hebben, in combinatie met informatie van gegevensmakelaars en andere derden, te gebruiken om mogelijkheden te creëren om mensen te beïnvloeden, vereist de Europese wetgeving dat het gebruik van persoonsgegevens voor dergelijke operaties wettig, eerlijk en transparant moet zijn. Zo is de publicatie van feitelijk onjuiste informatie op zich misschien niet onwettig, maar het onderzoek van het publiek met gerichte valse berichten zou volgens de AVG geen wettelijke basis hebben. In dit verband is het belangrijk op te merken dat veel praktijken van de betrokken diensten met betrekking tot persoonsgegevens het onderwerp zijn van rechtszaken en onderzoeken. Vragen over compliance kunnen zeker ook worden gesteld over de grote verscheidenheid aan praktijken met betrekking tot het verzamelen van publieksgegevens, inzichten en de toepassing daarvan in verschillende soorten communicatiecampagnes.

²⁵³ Tweede Kamer, vergaderjaar 2001-2002, 28 197, nr. 3, p. 8-9.

²⁵⁴ 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.

²⁵⁵ Autoriteit Persoonsgegevens "Verkennd onderzoek naar gebruik persoonsgegevens in verkiezingscampagnes", 15 februari 2019, <https://autoriteitpersoonsgegevens.nl/nl/nieuws/verkennd-onderzoek-naar-gebruik-persoonsgegevens-verkiezingscampagnes>.

De AVG bevat een speciale restrictievere regeling voor de verwerking van gevoelige categorieën persoonsgegevens die relevant is voor gerichte politieke advertenties. Volgens artikel 9 AVG vormen persoonsgegevens die de politieke opvattingen weergeven een speciale categorie gegevens. Als algemeen beginsel geldt dat de verwerking van dergelijke gegevens verboden is, en daarnaast onderworpen is aan een aantal strikt geïnterpreteerde uitzonderingen, zoals de uitdrukkelijke, specifieke, volledig geïnformeerde en vrij gegeven toestemming van de betrokkenen. De AVG bevat ook een andere uitzondering voor politieke partijen:

“[The prohibition on processing personal data revealing political opinions] shall not apply if ... processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a *political*, philosophical, religious or trade union aim and on condition that the processing relates solely to the *members or to former members of the body* or to persons *who have regular contact* with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.”

Politieke partijen kunnen dus persoonsgegevens verwerken die politieke opvattingen onthullen, maar alleen wanneer deze betrekking hebben op hun leden of voormalige leden, of personen die regelmatig contact hebben met de partij. Deze verwerking moet echter gepaard gaan met passende waarborgen, en zoals in overweging 56 van de AVG is bepaald, “[w]here in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people’s political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established”.²⁵⁶

Frankrijk heeft, zoals hieronder besproken, bepaalde dienstverleners (tijdens verkiezingen) specifieke verplichtingen opgelegd om zijn gebruikers te informeren over het gebruik van persoonsgegevens voor gesponsorde content “in verband met een debat van algemeen belang”.²⁵⁷ De gepromote en gesponsorde content die raakt aan een debat van algemeen belang moet duidelijke en transparante informatie bevatten over het gebruik van persoonsgegevens voor de gerichte verspreiding..

Kortom, omdat politieke advertenties online veelal direct gekoppeld zijn aan de verwerking van persoonsgegevens, voorziet het Europees kader voor gegevensbescherming in een aantal relevante bepalingen die internetgebruikers in staat kunnen stellen om hun rechten te waarborgen, die een bepaalde mate van transparantie kunnen bieden met betrekking tot de datagestuurde aspecten van de verspreiding van politieke advertenties, en die een mogelijkheid kunnen creëren voor de handhaving van en het toezicht op de naleving van de voorschriften door onafhankelijke regelgevende instanties in de lidstaten. Momenteel wordt het kader voor gegevensbescherming met betrekking tot de relevante internetdiensten beter gehandhaafd. Een dergelijke effectieve handhaving vormt een belangrijke waarborg om personen te beschermen tegen manipulatieve praktijken die de verwerking van persoonsgegevens met zich mee kan brengen.

Ten slotte heeft de Europese toezichthouder voor gegevensbescherming (EDPS) ook een *Opinion on online manipulation and personal data* gepubliceerd.²⁵⁸ Deze opinie is ingegeven door de invloed van de digitale informatiesystemen op de politieke economie en de wijze waarop “eliberate disinformation (“fake news”) has been propagated via this system”, onder meer door online manipulatie. In dit verband is de EDPS van mening dat onlinemanipulatie een cyclus in drie fasen omvat, van het verzamelen van gegevens

²⁵⁶ General Data Protection Regulation (EU) 2016/679 [2016] OJ L 119/1.

²⁵⁷ Wet nr. 2018-1202 van 22 december 2018 betreffende de strijd tegen de manipulatie van informatie, artikel 1, <https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte>

²⁵⁸ Europese Toezichthouder voor gegevensbescherming, “Advies van de EDPS over onlinemanipulatie en persoonsgegevens, advies 3/2018”, 19 maart 2018, blz. 7, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

via profilering tot microdoelbinding of personalisering, als een vorm van manipulatie die kan variëren van triviaal tot ernstig schadelijk.²⁵⁹ In de eerste fase, het verzamelen van gegevens, worden persoonlijke gegevens uit verschillende bronnen verzameld met behulp van verschillende technieken voor het samenvoegen van datasets, en de meeste gegevens worden automatisch geobserveerd of geregistreerd ("digitale broodkruimels") en onbewust opgeslagen als gevolg van de online- en offline-activiteiten van individuen.²⁶⁰ Ten tweede, profilering, waarbij de verzamelde gegevens worden onderzocht om mensen volgens precieze profielen te segmenteren. En ten derde, microtargeting en manipulatie. Microtargeting is waar beslissingen, gebaseerd op profilering, de informatieomgeving van een individu personaliseren met een hoge mate van personalisatie. Deze microtargeting activiteiten leiden tot een "cultuur van manipulatie" in de online omgeving, waar manipulatie de vorm aanneemt van microtargeted, managed content display die wordt gepresenteerd als het meest "relevant" voor het individu, maar die wordt bepaald om de inkomsten voor het platform te maximaliseren. De EDPS koppelt manipulatie aan de bedoeling achter het ontwerp van apparaten en software om "verslavend gedrag te veroorzaken", met kenmerken als auto-play, eindeloze nieuwsfeeds, meldingen en "streaks", die "opzettelijke pogingen zijn om de aandacht te maximaliseren" door middel van microtargeting op gebruikers (vergelijkbaar met technieken die door de gokindustrie worden gebruikt).²⁶¹

De EDPS heeft een aantal aanbevelingen over de aanpak van onlinemanipulatie, hoewel wordt erkend dat één enkele regelgevingsaanpak niet voldoende is. Deze omvatten (a) een strikte handhaving van de huidige wetgeving inzake gegevensbescherming - versterking van de bescherming van speciale gegevenscategorieën, de beginselen van transparantie, doelbinding en gegevensminimalisering, en waarborgen tegen onwettige profilering; (b) wetgevers moeten streven naar een collectieve identificatie van het probleem, zoals de mate waarin politieke bewegingen zich bezighouden met het opstellen van profielen en het richten van profielen van individuele personen, de bronnen van persoonsgegevens waarop zij vertrouwen en de instrumenten die zij gebruiken om zich te profileren en op hen af te stemmen; (c) wetgevers moeten sectorbreed samenwerken, aangezien de reacties op "fake news" moeten worden ondersteund door een grotere intersectorale samenwerking, dat wil zeggen een samenwerking tussen wetgevers op het gebied van gegevensbescherming, consumentenbescherming en verkiezingsregels; en d) zelfregulering en gedragscodes moeten worden aangemoedigd.

C. Regulering van direct marketing van elektronische communicatiediensten

Het EU-telecommunicatierecht bevat in de huidige e-Privacy Richtlijn regels voor direct marketing die relevant zijn voor de regulering van desinformatie. Deze regels zijn slechts van toepassing op direct marketing via een beperkt aantal communicatietechnologieën. De ePrivacy-Richtlijn is voornamelijk geïmplementeerd in de Nederlandse Telecommunicatiewet die van toepassing is op onder andere "openbare elektronische communicatienetwerken" zoals telefoon, televisie, internet en fax.²⁶² De grondgedachte achter deze specifieke normen is dat spam moet worden gereguleerd, aangezien communicatiediensten zoals telefoon en e-mail het direct en gericht contact vergemakkelijken. Om die reden moeten de personen een zekere mate van controle over dergelijke kanalen behouden om overlast te voorkomen.

Bij de implementatie van de e-Privacy Richtlijn in de Telecommunicatiewet heeft de Nederlandse wetgever gekozen voor een zo brede interpretatie van het verbod op spam, waar ook politieke communicatie onder valt. Met name artikel 11.7 van de Telecommunicatiewet verbiedt in de eerste plaats ongevroegde communicatie via "automatische oproep- en communicatiesystemen zonder menselijke tussenkomst,

²⁵⁹ Europese Toezichthouder voor gegevensbescherming, "Advies van de EDPS over onlinemanipulatie en persoonsgegevens, advies 3/2018", 19 maart 2018, blz. 7, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

²⁶⁰ Idem. p. 7.

²⁶¹ Idem., p. 9.

²⁶² Artikel 1.1 van de Telecommunicatiewet 'openbaar elektronisch communicatienetwerk'.

faxen en elektronische berichten” indien de ontvanger daar geen toestemming voor heeft gegeven. Hiermee is geautomatiseerde reclame per telefoon, fax of het internet verboden. Dit verbod omvat ook politieke advertenties nu er gesproken wordt over: “het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden”.²⁶³ Deze bepaling vormt de implementatie van artikel 13 e-Privacy Richtlijn,²⁶⁴ met zoals gezegd als belangrijk verschil dat waar de richtlijn in het midden laat of politieke advertenties ook onder de definitie van direct marketing vallen, de Telecommunicatiewet duidelijk aangeeft dat dat het geval is.

Nederland is niet het enige Europese land dat er voor heeft gekozen om deze regels voor direct marketing breed te interpreteren en ze van toepassing te verklaren op politieke communicatie via internetcommunicatiediensten zoals WhatsApp en Facebook Messenger. De Britse wetgever stelt zich bijvoorbeeld op het standpunt dat direct marketing “includes the promotion of the aims and ideals of any organisation including political campaigns” omvat en “appeals for funds or support for a campaign, encouraging individuals to take some form of direct action or vote for a particular political party or candidate” zou omvatten.²⁶⁵ Dit zou van toepassing zijn op alle elektronische communicatiemiddelen, met inbegrip van e-mail, maar ook op sociale media en berichtgevingstoepassingen.

Dezelfde brede reikwijdte heeft een tweede beperking in de Telecommunicatiewet, ditmaal van nationale oorsprong, gevormd door het bel-me-niet-register voor telefonische reclame. Wanneer iemand zich in dit register ingeschreven heeft mag hij niet ongevraagd telefonisch benaderd worden voor onder andere politieke advertenties.²⁶⁶ Met de invoering van de e-Privacy verordening zal dit regime naar verwachting aangepast worden van een opt-out naar een opt-in systeem. Alleen wanneer toestemming is gegeven mag reclame worden gemaakt. Dit verbod, tenzij er toestemming wordt gegeven, zal gelden voor elke vorm van ongevraagde elektronische communicatie.²⁶⁷ Het toezicht op deze regels wordt gedeeld uitgevoerd door de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt. De Autoriteit Persoonsgegevens is bevoegd waar het de verwerking van persoonsgegevens betreft, en de Autoriteit Consument en Markt op het gebied van de regulering van ongevraagde elektronische communicatie zelf.²⁶⁸

Bovendien is het belangrijk om op te merken dat beide kaders momenteel worden herzien. Ten eerste breidt het Europees wetboek voor elektronische communicatie (“**EWEC**”),²⁶⁹ die de bestaande richtlijnen inzake openbare elektronische-communicatienetwerken en -diensten vervangt, het toepassingsgebied ervan uit tot zogenaamde “over the top-diensten”, zoals internetcommunicatiediensten zoals WhatsApp en Skype. De EWEC moet uiterlijk in december 2020 in nationale wetgeving zijn omgezet en de Europese Raad heeft verklaard dat het doel van de EWEC is om ervoor te zorgen dat de consumentenvoorschriften nu ook van toepassing zijn op diensten die via het internet worden geleverd, zoals berichtenapps, en dat de lidstaten ook regels moeten vaststellen voor compensatie in het geval van wanprestatie van aanbieders van elektronische communicatienetwerken of -diensten. Ten tweede worden in de Raad van Ministers voorstellen besproken om de bestaande e-Privacy Richtlijn te vervangen door een e-Privacy Verordening.²⁷⁰

²⁶³ Artikel 11.7 lid 1 Telecommunicatiewet.

²⁶⁴ Richtlijn 2002/58/EG.

²⁶⁵ Voorlichtingsbureau van de commissaris, ‘Guidance on political campaigning’, 2018, blz. 6.

²⁶⁶ Artikel 11.7 lid 5 t/m Telecommunicatiewet.

²⁶⁷ Artikel 16(1) voorgestelde e-Privacy Verordening, COM/2017/010 final - 2017/03 (COD), zie verder hoofdstuk 5.

²⁶⁸ Artikel 17 Samenwerkingsprotocol tussen Autoriteit Consument en Markt en Autoriteit Persoonsgegevens, ACM, Stcrt. 2016 nr. 58078.

²⁶⁹ Richtlijn (EU) 2018/1972 tot vaststelling van de Europese elektronische-communicatiecode, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN>.

²⁷⁰ Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens in elektronische communicatie en tot intrekking van Richtlijn 2002/58/EG (verordening betreffende privacy en elektronische communicatie), COM(2017) 10 definitief, 10 januari 2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>

Dit voorstel voor een nieuwe ePrivacy Verordening bevat regels voor direct marketing die van toepassing kunnen zijn op het hierboven beschreven type politieke communicatie, waarbij een politieke partij een politieke boodschap rechtstreeks naar een individu stuurt via een berichtendienst zoals WhatsApp of Facebook Messenger. De voorgestelde ePrivacy Verordening kan ook een instrument zijn om het gebruik van valse accounts aan te pakken waarmee politieke boodschappen rechtstreeks via WhatsApp worden verspreid. Bij de recente Indiase verkiezingen is WhatsApp naar voren gekomen als een centrale methode om politieke boodschappen te verspreiden.²⁷¹ Als reactie op het toenemende belang van WhatsApp voor de politieke communicatie tijdens verkiezingen, heeft WhatsApp gebruikerscontroles ingevoerd om de integriteit van verkiezingen te beschermen, waaronder een doorstuurlabel, een doorstuurlimiet en een verbod op automatische berichtenuitwisseling om virale desinformatie tijdens verkiezingen te bestrijden.²⁷²

Zo wordt in de e-Privacy Verordening uitdrukkelijk vermeld dat het begrip direct marketing ook "messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties" omvat, en "messages sent by other non-profit organisations to support the purposes of the organisation." Bovendien staat in de e-Privacy Verordening dat het "[is] necessary to prohibit the masking of the identity and the use of false identities", indien ongevraagde commerciële communicatie voor direct marketingdoeleinden wordt verzonden.

De relevante regels inzake direct marketing in de voorstellen zijn opgenomen in artikel 16, wat bepaalt dat iedereen die gebruik maakt van elektronische-communicatiediensten om direct marketingcommunicatiecommunicatie door te sturen, de eindgebruikers moet informeren over "(a) the marketing nature of the communication, (b) the identity of the legal or natural person on behalf of whom the communication is transmitted; and (c) how to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications." Het voorstel voor de e-Privacy Verordening bepaalt ook dat boetes tot 10 miljoen euro kunnen worden opgelegd voor inbreuken op artikel 16. De Commissie is van oordeel dat de lidstaten de mogelijkheid hebben om de in de ePrivacy-verordening vastgestelde sancties op te leggen.

Kortom, de wettelijke kaders van de Europese Unie voor elektronische communicatiediensten voorzien reeds in regels voor direct-marketing. Wijzigingen in dit wettelijk kader zullen de relevantie van de elektronische communicatiewetgeving van de EU voor de regulering van politieke advertenties via internet-diensten verder vergroten.

D. Richtlijn Audiovisuele Mediadiensten

De richtlijn audiovisuele mediadiensten ("AVMD-richtlijn")²⁷³ beoogt een minimum aan harmonisatie in de EU van de nationale wetgeving inzake audiovisuele mediadiensten te waarborgen, teneinde belemmeringen voor het vrije verkeer van dergelijke diensten binnen de interne markt van de EU weg te nemen. Met het oog op deze doelstellingen coördineert de richtlijn een aantal gebieden: algemene beginselen; jurisdictie; aanzetten tot haat; toegankelijkheid voor personen met een handicap; grote evenementen; promotie en distributie van Europese werken; commerciële communicatie en bescherming van minderjarigen. De AVMD-richtlijn wordt voornamelijk geïmplementeerd in de Nederlandse Mediawet, die ook een groot aantal nationale bepalingen bevat over het programma-aanbod en de advertentiemogelijk-

²⁷¹ Zie Murgia, M., Findlay, S. & Schipani, A. 'India: The WhatsApp Election', Financial Times, 5 mei 2019.

²⁷² WhatsApp, 'Bijdragen aan de veiligheid van de verkiezingen in India', <https://faq.whatsapp.com/en/26000233/https://faq.whatsapp.com/en/26000233/>.

²⁷³ 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) (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0013&rom=EN>).

heden.²⁷⁴ Het toezicht op en de handhaving van de mediaregulering binnen de Nederlandse context is gedelegeerd aan het Commissariaat voor de Media.²⁷⁵

De richtlijn is voortgekomen uit de vroegere richtlijn “Televisie zonder grenzen” en heeft betrekking op zowel traditionele televisieomroep als audiovisuele mediadiensten op aanvraag. Na de herziening van de richtlijn in 2018²⁷⁶ vallen de aanbieders van videoplatformdiensten nu ook onder het toepassingsgebied van de richtlijn, voor zover zij onder de definitie van dergelijke diensten vallen. De definitie is nogal uitgebreid:

“video-sharing platform service” means a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.²⁷⁷

De gedachte achter deze verschuiving is dat particuliere tussenpersonen op het internet organisatorische controle uitoefenen over de inhoud van derden; zij bepalen de wijze waarop die inhoud beschikbaar wordt gesteld, de mate van bekendheid ervan, enzovoort. Als zij *de facto* de controle hebben over wat hun gebruikers zien en hoe zij het zien, moeten zij ook verantwoordelijk of aansprakelijk worden gesteld voor de inhoud - ook al hebben zij er geen redactionele controle over. In overweging 47 van de considerans van de richtlijn wordt deze gedachte uiteengezet met betrekking tot videoplatforms in het kader van de richtlijn:

“A significant share of the content provided on video-sharing platform services is not under the editorial responsibility of the video-sharing platform provider. However, **those** providers typically determine the organisation of the content, namely programmes, user-generated videos and audiovisual commercial communications, including by automatic means or algorithms. Therefore, those providers should be required to take appropriate measures to protect minors from content that may impair their physical, mental or moral development. They should also be required to take appropriate measures to protect the general public from content that contains incitement to violence or hatred directed against a group or a member of a group on any of the grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union (the “Charter”), or the dissemination of which constitutes a criminal offence under Union law.”

Deze redenering is onder druk komen te staan omdat het heeft geleid tot “considerable political and social pressure [being] exerted on these platforms to resolve the problems “themselves”.²⁷⁸ Dit op zijn beurt, “leads to a spiral of privatised regulation”.²⁷⁹

²⁷⁴ Zie hoofdstuk 6.

²⁷⁵ Hoofdstuk 7 van de Mediawet.

²⁷⁶ Richtlijn (EU) 2018/1808 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 de veranderende marktomstandigheden, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN>. Een gecodeerde versie is hier beschikbaar: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010L0013-20181218>.

²⁷⁷ Ibid., Article 1(1)(aa).

²⁷⁸ Ben Wagner, ‘Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech’, in Martin Moore and Damian Tambini (eds.) (2018) *Digital Dominance: the Power of Google, Amazon, Facebook, and Apple* (Oxford, Oxford University Press, 2018), pp. 219-240, at p. 223.

²⁷⁹ Ibid.

De toepasselijkheid van de richtlijn op de aanbieders van videoplatformdiensten heeft geen betrekking op alle bepalingen van de richtlijn. De nadruk ligt sterk op inhoud die schadelijk is voor minderjarigen, evenals op bepaalde soorten illegale inhoud, met name het aanzetten tot geweld of haat, en het publiekelijk uitlokken van het plegen van een terroristisch misdrijf, misdrijven op het gebied van seksueel misbruik van kinderen en misdrijven met betrekking tot racisme en vreemdelingenhaat.²⁸⁰ Onverminderd de artikelen 12 tot en met 15 van de richtlijn inzake elektronische handel zorgen de lidstaten ervoor dat de onder hun bevoegdheid vallende aanbieders van videodelingsplatforms passende maatregelen nemen om minderjarigen en het publiek in het algemeen te beschermen tegen programma's, door de gebruiker gegenereerde video's en audiovisuele commerciële communicatie die de bovengenoemde soorten inhoud inhouden.

De AVMD bevat voorschriften inzake "audiovisual commercial communications", welke gedefinieerd worden als "images with or without sound which are designed to promote, directly or indirectly, the goods, services or image of a natural or legal person pursuing an economic activity; such images accompany, or are included in, a programme or user-generated video in return for payment or for similar consideration or for self-promotional purposes".²⁸¹ "Audiovisual commercial communication" is een brede term die televisiereclame, sponsoring, telewinkelen en productplaatsing omvat. Volgens artikel 9, lid 1, onder a van de AVMD moet audiovisuele commerciële communicatie "als zodanig herkenbaar" zijn en is sluikreclame verboden. Krachtens artikel 9, lid 1, mogen ook geen subliminale technieken worden gebruikt; audiovisuele commerciële communicatie mag geen afbreuk doen aan het respect voor de menselijke waardigheid en mag geen discriminatie omvatten of bevorderen. De lidstaten moeten ervoor zorgen dat de aanbieders van videodelingsplatformaanbieders aan deze en de andere eisen van artikel 9, lid 1, voldoen "with respect to audiovisual commercial communications that are marketed, sold or arranged by those video-sharing platform providers".²⁸²

De eerste vraag is of politieke reclame onder de regels van de AVMD inzake reclame valt. Aangezien de definities in de eerste plaats betrekking hebben op de bevordering van goederen, diensten of imago bij de uitoefening van een economische activiteit, valt betaalde politieke reclame als zodanig niet onder de reclamevoorschriften van de AVMD.

De tweede vraag is of de regels die in het kader van de AVMD-richtlijn aan videoplatforms worden opgelegd, van toepassing zijn op politieke reclame die via bijvoorbeeld YouTube wordt verspreid. Artikel 28ter, dat hierboven is samengevat, bepaalt dat de beschermende maatregelen van de lidstaten niet mogen leiden tot controle vooraf of het filteren van inhoud op een wijze die niet in overeenstemming is met de richtlijn inzake elektronische handel.

Artikel 28 lid 3 bepaalt dat de maatregelen "shall consist of, as appropriate features such as: having a functionality for users who upload user-generated videos to declare whether such videos contain audiovisual commercial communications; establishing user-friendly mechanisms for users of a video-sharing platform to report or flag content; establishing easy-to-use systems allowing users of video-sharing platforms to rate the content; and providing for effective media literacy measures and tools and raising users' awareness of those measures and tools". Artikel 28 lid 6 bepaalt dat de lidstaten aan aanbieders van videoplatforms maatregelen kunnen opleggen die gedetailleerder of strenger zijn dan de genoemde maatregelen, mits deze in overeenstemming zijn met het EU-recht, met inbegrip van de richtlijn inzake elektronische handel.

280 Richtlijn (EU) 2018/1808, artikel 28 ter.

281 Ibid, article 1(1)(h).

282 Artikel 28 ter, lid 2.

De nieuwe AVMD-richtlijn verplicht de lidstaten om te verzekeren dat videoplatformdiensten bepaalde maatregelen nemen met betrekking tot de door hun gebruikers gegenereerde video's en audiovisuele commerciële communicatie. Zoals gezegd valt betaalde politieke reclame niet onder de definitie van audiovisuele commerciële communicatie. De definitie van een door de gebruiker gegenereerde video ("a set of moving images with or without sound constituting an individual item, irrespective of its length, that is created by a user and uploaded to a video-sharing platform by that user or any other user"²⁸³) kan echter van toepassing zijn op campagnevideo's en video's met politieke communicatie die door een politieke partij of groepering worden geüpload. Ook hier is het een open vraag of het concept van politieke reclame ook een politieke partij of groepering moet omvatten die een campagnevideo publiceert en deze op YouTube uploadt. Dit soort organische inhoud zou echter nog steeds onder de voorschriften van artikel 28b AVMD kunnen vallen.

Het lijkt er ook op dat een lidstaat de definitie van "audiovisuele commerciële communicatie" eventueel zou kunnen uitbreiden tot politieke reclame en vervolgens de maatregelen uit hoofde van artikel 28b lid 3 onder 1, van de AVMD zou kunnen opleggen aan videodelingsplatforms zoals YouTube. Dit zou ervoor zorgen dat de geüploade video's een mededeling bevatten dat het gesponsorde inhoud betreft en gebruikers in staat stellen om problematische inhoud te rapporteren.

Het kan ook nuttig zijn om te verwijzen naar de regels inzake de vrijheid van ontvangst, die als basis kunnen dienen voor de bespreking van de buitenlandse invloed in dit onderzoek. Krachtens artikel 3 van de AVMD-richtlijn moeten de lidstaten "freedom of reception" waarborgen en mogen zij niet "restrict retransmissions on their territory of audiovisual media services from other Member States for reasons which fall within the fields coordinated by this Directive". Daarom is het de lidstaten over het algemeen verboden om de doorgifte van audiovisuele mediadiensten uit andere lidstaten te beperken. Er zijn echter uitzonderingen op deze regel wanneer gaat om het aanzetten tot geweld of haat, het publiekelijk uitlokken van het plegen van een terroristisch misdrijf of inhoud die minderjarigen ernstig schaadt.

Tot slot zij erop gewezen dat de Europese Commissie in haar *Recommendation on disinformation and elections* suggereert dat zij zich wellicht kan "laten inspireren" door de regels van de AVMD inzake de herkenbaarheid van audiovisuele commerciële communicatie bij een mogelijke regulering van de transparantie van betaalde online politieke advertenties.²⁸⁴

E. Desinformatie & commerciële regelgeving

In de definitie van desinformatie worden sommige vormen van desinformatie expliciet gekoppeld aan economische winst, waardoor de commerciële regelgeving van de EU van toepassing is. De Europese Commissie benadrukt dat het creëren en verspreiden van desinformatie vaak economisch rendabel is, hoewel de precieze relatie niet is uitgewerkt.²⁸⁵ Het economisch gewin kan enerzijds worden bereikt via de inhoud van de desinformatie voor partijen die profiteren van de verspreiding van die specifieke valse en schadelijke informatie.²⁸⁶ Aan de andere kant zijn er ook partijen die desinformatie op grote schaal commercieel verspreiden. Deze zogenaamde "trollen" profiteren niet noodzakelijkerwijs van de inhoud van de desinformatie maar worden betaald voor het verspreiden ervan.²⁸⁷ Gezien dit winstoogmerk van

²⁸³ Article 1(1)(ba).

²⁸⁴ Europese Commissie, Aanbeveling betreffende netwerken voor samenwerking bij verkiezingen, online transparantie, bescherming tegen cyberveiligheidsincidenten en de bestrijding van desinformatiecampagnes in het kader van de verkiezingen voor het Europees Parlement, C(2018) 5949 definitief, 12 september 2018, blz. 4.

²⁸⁵ Europese Commissie, "Desinformatie online aanpakken: een Europese aanpak, COM(2018) 236 definitief", <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-236-F1-EN-MAIN-PART-1.PDF>.

²⁸⁶ Wardle, C., & Derakhshan, H. 'Information Disorder'. *Naar een interdisciplinair kader voor onderzoek en beleidsvorming*, z.p., 2017, blz. 27.

²⁸⁷ Idem, blz. 31; Bayer J. e.a., "Disinformation and propaganda - impact on the functioning of the rule of law in the EU and its Member States", Europese Unie, 2019, blz. 32, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

desinformatie kunnen twee belangrijke verbanden worden gelegd tussen commerciële regelgeving en desinformatie. In de eerste plaats zijn in de regulering van commerciële uitingen en acties het verbod op misleidende reclame, oneerlijke handelspraktijken en ongefundeerde gezondheidsclaims van belang. Ten tweede kan het grote aantal transparantieplichtingen met betrekking tot commerciële reclame worden gekoppeld aan, of dienen als voorbeeld voor de mogelijke regelgeving met betrekking tot desinformatie. Uit dit bestaande regelgevingslandschap volgt dat commercieel gedreven desinformatie die de economische verhoudingen verstoort of bijvoorbeeld schadelijke medische claims bevat die gericht zijn op consumenten, al uitgebreid gereguleerd is.

Met betrekking tot de regulering van commerciële uitingen en acties die in verband kunnen worden gebracht met desinformatie zijn twee richtlijnen van belang. Dit is allereerst de richtlijn oneerlijke handelspraktijken²⁸⁸ ("ROH"), die is geïmplementeerd in Afdeling 3A, artikelen 193a tot en met 193j van boek 6 van het Burgerlijk Wetboek ("BW").²⁸⁹ De ROH heeft belangrijke stappen gezet in de harmonisering van de commerciële regelgeving in de EU.²⁹⁰ De materiële normen van de ROH zijn in Nederland geïmplementeerd als onderdeel van het recht inzake de onrechtmatige daad, waardoor naast de handhaving door de bevoegde regelgevende instanties ook civiele handhaving mogelijk is.²⁹¹ De ROH is gericht op de bescherming van de consumentenbelangen en doet dit door middel van maximale harmonisatie.²⁹² De ROH is uitdrukkelijk gericht op de handelspraktijken van ondernemingen die gericht zijn op de consument, met uitsluiting van alle "business to business"-praktijken.²⁹³ Deze laatste betrekkingen vallen onder de hieronder besproken richtlijn inzake misleidende reclame en vallen onder de algemene categorie van een onrechtmatige daad.

Het begrip "handelspraktijken" in de context van de ROH omvat een breed scala aan activiteiten, waaronder "any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers".²⁹⁴ De inhoudelijke normen kunnen worden onderverdeeld in drie categorieën: (i) een algemeen verbod op oneerlijke handelspraktijken,²⁹⁵ (ii) specifieke normen inzake misleidende of agressieve handelspraktijken,²⁹⁶ en (iii) de handelspraktijken die onder alle omstandigheden als oneerlijk worden beschouwd.²⁹⁷ Deze normen overlappen in grote mate met desinformatie.

Het algemene verbod op oneerlijke handelspraktijken in artikel 5 van de ROH of artikel 193b, lid 2, van boek 6 BW bepaalt dat een handelspraktijk oneerlijk is indien zij "contrary to the requirements of professional diligence" en "materially distorts or is likely to materially distort the economic behaviour" van de "average consumer who is reasonably well-informed and reasonably observant and circumspect".²⁹⁸ Dit algemene verbod zou ook van toepassing zijn op elke vorm van desinformatie die indruist tegen de algemene handelsnormen (professionele toewijding) en die het economische gedrag van de consument met succes manipuleert. De specifieke reeks oneerlijke handelspraktijken die onder de categorie "mislei-

288 Richtlijn 2005/29/EG.

289 Tweede Kamer, 2006-2007, 30 928, nee. 3.

290 Stuyck, J., Terryn, E. & Van Dyck, T., 'Vertrouwen door eerlijkheid? The new directive on unfair business-to-consumer commercial practices in the internal market', *Common Market Law review* 2006, 43, blz. 107; De Very, R.W., 'Handelspraktijken en reclame', in: E.H. Hondius & G.J. Rijken, *Handboek Consumentenrecht*, 2015 Zutphen: uitgeverij Parijs, p. 381.

291 Duivenvoorde, B.B., 'Oneerlijke handelspraktijken', *TcVH* 2016-1, blz. 16-23.

292 Tweede Kamer, 2006-2007, 30 928, nee. 3 p. 1.

293 Richtlijn 2005/29/EG, artikel 3, overwegingen 6 & 8; De Vrey, R.W., "Handelspraktijken en reclame", in: Hondius, E.H. & Rijken, G.J., *Handbook Consumer Law*, 2015 Zutphen: uitgeverij Paris, p. 383; Tweede Kamer, 2006-2007, 30 928, nee. 3, blz. 1; Zie ook voor de Nederlandse context: Hof Arnhem-Leeuwarden 15 mei 2014, ECLI:NL:GHARL:2014:3884 (*Het Gilde Utrecht/Telefoonboek*).

294 Artikel 2, onder d), van Richtlijn 2005/29/EG.

295 Artikel 5 van Richtlijn 2005/29/EG; artikel 6:193a van het Burgerlijk Wetboek.

296 Misleidende handelspraktijken in de artikelen 6 en 7 van Richtlijn 2005/29/EG en de artikelen 6:193c-193f van het Burgerlijk Wetboek; agressieve handelspraktijken in de artikelen 8 & 9 van Richtlijn 2005/29/EG en artikel 6:193h van het Burgerlijk Wetboek.

297 Bijlage II Richtlijn 2005/29/EG en artikel 6:193g in samenhang met 6:193i van het Burgerlijk Wetboek.

298 CJEU, 16 juli 1998, C-210/96 (*Gut Springenheide/Steinfurt; „6-Korn - 10 frische Eier"*), par. 2.1.1, blz. 1. 37. Er bestaan nog steeds specifieke regels voor kwetsbare consumenten, zie overweging 18 en artikel 5, lid 3, van Richtlijn 2005/29/EG.

dende handelspraktijken" vallen, houden echter het nauwst verband met desinformatie. Deze categorie, die in artikel 6-7 van de richtlijn en in de artikelen 193c tot en met 193f van boek 6 BW is gecodificeerd, beschouwt een praktijk als oneerlijk wanneer deze enerzijds "contains false information and is therefore untruthful or in any way, including in overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct" en ten tweede wanneer dit er voor zorgt dat de consument "to take a transactional decision that he would not have taken otherwise".²⁹⁹ De onjuiste of misleidende informatie moet betrekking hebben op een aspect uit de uitgebreide, zij het limitatieve, lijst van aspecten zoals de belangrijkste kenmerken van het product of de identiteit van de handelaar. De bepaling heeft ook betrekking op misleidende vergelijkende reclame.³⁰⁰ Daarnaast kunnen nalatigheden ook worden beschouwd als een misleidende praktijk, bijvoorbeeld wanneer niet aan een informatievereiste wordt voldaan.³⁰¹ Met de nadruk op onjuiste of misleidende informatie valt deze categorie "misleidende handelspraktijken" zeker onder het toepassingsgebied van de desinformatie.

Daarentegen heeft de specifieke categorie van agressieve handelspraktijken minder te maken met desinformatie, aangezien het vooral gaat om intimidatie of dwang van de consument en niet zozeer om bedrog of manipulatie. Tot slot is er een lange lijst van handelspraktijken die onder alle omstandigheden als oneerlijk worden beschouwd, die is opgenomen in bijlage I van de richtlijn en die ten uitvoer wordt gelegd in artikel 193g (misleidende praktijken) en artikel 193i (agressieve praktijken), Boek 6 BW. Er zijn veel voorbeelden van valse of misleidende informatie die ook als desinformatie kunnen worden aangemerkt.

Handhaving van deze normen is zowel mogelijk via civiele procedures, aangespannen door consumenten of concurrenten,³⁰² als via de bevoegde toezichthoudende autoriteiten die boetes en bevelen kunnen opleggen.³⁰³ De Nederlandse toezichthouder, de Autoriteit Consument en Markt ("**ACM**") en, voor wat betreft financiële producten, de Autoriteit Financiële Markten ("**AFM**") zijn bevoegd voor de handhaving van deze normen in de ROH.³⁰⁴ Ook zelfregulerende instrumenten zoals de Nederlandse Reclame Code spelen een belangrijke rol in de normhandhaving die specifiek betrekking heeft op advertenties.³⁰⁵

De tweede relevante richtlijn voor de relatie tussen desinformatie en commerciële regelgeving is de richtlijn misleidende en vergelijkende reclame³⁰⁶ ("**MVR-richtlijn**") en de voorloper daarvan, de richtlijn inzake misleidende reclame.³⁰⁷ Misleidende en vergelijkende reclame binnen de Nederlandse context zijn gecodificeerd in titel 3.4, in de artikelen 194 tot 196 van boek 6 BW. In dit hoofdstuk worden de verschillende richtlijnen geïmplementeerd, hoewel sommige van deze bepalingen dateren van vóór de Europese harmonisatie-inspanningen.³⁰⁸ De MVR-richtlijn is nauw verwant aan de ROH, met enkele uitzonderingen. Een eerste opmerkelijk verschil is dat het een minimale harmonisatie biedt, waardoor er meer ruimte ontstaat voor nationale implementatie,³⁰⁹ ten tweede heeft de MVR-richtlijn een fundamenteel andere reikwijdte, omdat zij alleen betrekking heeft op de communicatie tussen bedrijven onderling.³¹⁰ Dit beperktere toepassingsgebied blijkt duidelijk uit het in artikel 1 genoemde doel: "het beschermen

299 Artikel 6 van Richtlijn 2006/114/EG zoals geïmplementeerd in artikel 6:193c van het Burgerlijk Wetboek.

300 Artikel 6, lid 2, van Richtlijn 2006/114/EG zoals geïmplementeerd in artikel 6:193c, lid 2, van het Burgerlijk Wetboek.

301 Artikel 7 van Richtlijn 2005/29/EG, geïmplementeerd in artikel 6:193d van het Burgerlijk Wetboek. Deze informatieverplichting is bijzonder belangrijk in het geval van een uitnodiging tot aankoop, zie artikel 7, lid 4, van Richtlijn 2005/29/EG. Zie ook 6:193e BW en bijlage II van Richtlijn 2005/29/EG.

302 De Vrey, R.W., '*Handelspraktijken en reclame*', in: Hondius, E.H. & Rijken, G.J., '*Handbook of Consumer Law*', 2015 Zutphen: publisher Paris, p. 405.

303 Artikel 2.9 Handhavingswet consumentenbescherming.

304 Artikel 8.8 in samenhang met 8.11 en bijlage a van de wet op de handhaving van de consumentenbescherming.

305 De Vrey, R.W., '*Commercial Practices and Advertising*', in: Hondius, E.H. & Rijken, G.J., '*Handbook on Consumer Law*', 2015 Zutphen: Uitgeverij Paris, p. 405.

306 Richtlijn 2006/114/EG.

307 Richtlijn 84/450/EEG.

308 Huis van Afgevaardigden, 1975-1976, 13 611, nr. 1-4, 13 611.

309 Artikel 8 Richtlijn 2006/114/EG.

310 De Vrey, R.W., '*Commercial Practices and Advertising*', in: Hondius, E.H. & Rijken, G.J., '*Handbook on Consumer Law*', 2015 Zutphen: uitgeverij Paris, p. 398.

van handelaren tegen misleidende reclame en de oneerlijke gevolgen daarvan en het vaststellen van de voorwaarden waaronder vergelijkende reclame is toegestaan". De focus op business-to-business communicatie maakt deze bepalingen minder relevant voor de verspreiding van desinformatie, zoals blijkt uit de focus op publieke schade en de impliciete brede maatschappelijke verspreiding van de informatie in de discussie over desinformatie. Toch verdienen de twee centrale bepalingen, artikel 194 en 194a boek 6 BW, een korte beschouwing.

Artikel 194 boek 6 BW stelt dat een op een andere onderneming gerichte reclame onrechtmatig is wanneer zij misleidend is en de misleidende informatie betrekking heeft op een beperkte lijst van aspecten die in het artikel zijn opgenomen, zoals de aard, prijs of herkomst van het product. Een reclame kan ook als misleidend worden beschouwd wanneer het gaat om informatie die nodig is om een geïnformeerde aankoop te doen.³¹¹ Reclame wordt gedefinieerd als het doen van een openbare mededeling over aangeboden goederen of diensten, ongeacht het medium, waarbij advertenties van politieke aard uitdrukkelijk worden uitgesloten.³¹² Vervolgens werd artikel 194a boek 6 BW ingevoerd vanwege de richtlijn inzake vergelijkende reclame van 2002.³¹³ De bepaling voorziet in de regel die vergelijkende reclame onder specifieke cumulatieve voorwaarden toestaat. Het HvJEU heeft in zijn jurisprudentie uitgebreid uitgewerkt hoe de verschillende voorwaarden voor rechtmatige vergelijkende reclame moeten worden geïnterpreteerd.³¹⁴ De tenuitvoerlegging via een civiele procedure wordt vergemakkelijkt door de bepalingen in artikel 195, boek 6 BW die de bewijslast verlichten. Administratief toezicht en handhaving worden, net als bij de richtlijn oneerlijke handelspraktijken, uitgevoerd door de ACM en de AFM.³¹⁵ Daarnaast speelt het zelfreguleringsinstrument van de Nederlandse Reclame Code een belangrijke rol bij de handhaving van de MVR-richtlijn en de bredere Nederlandse regels inzake misleidende en vergelijkende reclame voor business-to-business doeleinden.³¹⁶

Bovendien bestaat er een gerelateerd sectorspecifiek regelgevend kader voor gezondheidsclaims in een commerciële context. Deze bepalingen zijn met name relevant voor de discussie over desinformatie, gezien de mogelijke schade die gezondheid gerelateerde desinformatie kan toebrengen. Een voorbeeld van een dergelijk verband is de wijdverbreide schadelijke informatie over de vermeende schadelijke effecten van vaccinaties, die vermoedelijk heeft bijgedragen aan een lagere vaccinatiegraad.³¹⁷ Er bestaat een groot aantal EU-bepalingen die de inhoud van de commerciële communicatie over voedsel- en medicijnveiligheid regelen. Zo is er bijvoorbeeld de Verordening inzake voedings- en gezondheidsclaims voor levensmiddelen, waarin de voorwaarden voor dergelijke claims in de etikettering en presentatie van en reclame voor levensmiddelen zeer gedetailleerd zijn vastgelegd. Op grond van die Verordening zijn ook misleidende of valse claims verboden.³¹⁸ Wat betreft geneesmiddelen, staat de richtlijn tot vaststelling van een Communautaire wetboek betreffende geneesmiddelen voor menselijk gebruik centraal. Hierin worden bijna alle aspecten met betrekking tot de verkoop, productie, distributie en reclame voor geneesmiddelen voor menselijk gebruik geregeld.³¹⁹ Titel VIII van de richtlijn heeft met name betrekking op reclame en is geïmplementeerd in hoofdstuk 9 van de Nederlandse Geneesmiddelenwet. In het alge-

311 artikel 194 sub 2-4 boek 5 DCC.

312 Second Chamber, 1975-1976, 13 611, no. 3, p. 9; Asser/Hartkamp & Sieburgh, 6IV 2015/315 "Openbaar (doen) maken misleidende kennisgeving.

313 Richtlijn 97/55/EG.

314 CJEU 18 november 2019, C-159/09 (*Lidl SNC/Verizon Distribution SA*).

315 Bijlage een wet op de handhaving van de consumentenbescherming.

316 De Vrey, R.W., 'Commercial Practices and Advertising', in: Hondius, E.H. & Rijken, G.J., *Handbook on Consumer Law*, 2015 Zutphen: uitgeverij Paris, p. 411.

317 Voor de Nederlandse context, zie: Externe Adviescommissie Vaccinatiebereidheid tot Vaccineren, 'In gesprek over vaccineren', Rijksvaccinatieprogramma Nederland 2018' RIVM; Volkskrant, 'Vaccinatieafweerders: Why Anti-vaccineers Cause So much Resistance' 2019, <https://www.volkskrant.nl/nieuws-achtergrond/vaccinatieweigeraars-waarom-anti-vaxxers-zo-veel-weerstand-oproepen~baad1ac0/>. Voor een discussie over mogelijke verplichte vaccinatie zie: Pierik, R.H.M. (2019). Past een verplichting tot vaccineren binnen het EVRM-regime? *Tijdschrift voor Gezondheidsrecht*, 43(4), 8-25. <https://doi.org/10.5553/TvGR/016508742019043004002> en Pierik, R. (2018). Verplichte Vaccinatie: een ongekwalificeerde verdediging. *Tijdschrift voor Toegepaste Filosofie*, 35(2), 381-398. <https://doi.org/10.1111/japp.12215>.

318 Artikel 3 Verordening (EG) nr. 1924/2006.

319 Richtlijn 2001/83/EG.

meen is misleidende reclame verboden en is met name publieksreclame voor geneesmiddelen die alleen beschikbaar zijn op basis van een medisch recept of die verdovende middelen bevatten, volledig verboden.³²⁰ De richtlijn bevat verder een aantal informatie-eisen voor de toegestane medische reclame. Deze vereisten maken deel uit van bijlage II van de richtlijn oneerlijke handelspraktijken, wat betekent dat dergelijke nalatigheden ook worden beschouwd als een misleidende handelspraktijk in het kader van de richtlijn oneerlijke handelspraktijken.³²¹ In een commerciële context zijn misleidende gezondheidsclaims of het weglaten van vitale informatie over onder meer het geneesmiddel of de producent dan ook streng gereguleerd. In Nederland is de Nederlandse Voedsel- en Warenautoriteit verantwoordelijk voor het toezicht op en de handhaving van deze normen.³²²

Nauw verwant aan de bovengenoemde beperkingen op commerciële communicatie en even relevant in de discussie over desinformatie zijn de vele verschillende transparantieplichtingen met betrekking tot commerciële communicatie of meer specifiek commerciële reclame. De transparantieplichtingen die in de REH zijn opgenomen, zijn reeds besproken, maar er zijn verschillende andere normen die de openbaarmaking van relevante informatie in een groot aantal verschillende commerciële contexten regelen. Het algemene doel van deze bepalingen is ervoor te zorgen dat reclame als zodanig herkenbaar is en dat voldoende informatie wordt verstrekt om de economische actoren in staat te stellen met redenen omklede besluiten te nemen. De AVMD-richtlijn vereist bijvoorbeeld dat reclame op televisie als zodanig herkenbaar is³²³ en de e-Privacy Richtlijn vereist dat de afzender van direct-marketingberichten via elektronische post identificeerbaar is.³²⁴ Zoals eerder aangegeven, heeft de Commissie gesteld dat de lidstaten zich voor eventuele transparantiemaatregelen met betrekking tot politieke advertenties zouden kunnen laten inspireren door de informatievereisten in het REH en de AVMD-richtlijn.³²⁵

Uit dit overzicht van de commerciële regelgeving van de EU op het gebied van desinformatie volgt in de eerste plaats dat in een commerciële context onjuiste en misleidende informatie in veel gevallen al verboden is en in de tweede plaats dat er een groot aantal informatievereisten bestaat om consumenten en andere relevante economische actoren naar behoren te informeren. Een groot deel van de desinformatie voor de winst is dus al gereguleerd; zodra economische belangen in het geding zijn en het economische gedrag van mensen wordt gemanipuleerd, komt deze grote hoeveelheid regelgeving in het spel. Vanwege de vaak geringe stimulansen voor consumenten of andere personen om bij niet-naleving van deze normen gerechtelijke stappen te ondernemen, zijn toezicht en handhaving door regelgevers zoals de ACM van bijzonder belang. Van belang hierbij is dat de Europese Commissie momenteel een voorstel voor een richtlijn ter verbetering van de handhaving van de consumentenrechten bespreekt, waardoor de mogelijkheden voor representatieve verbods- en compensatiemogelijkheden zullen worden uitgebreid.³²⁶

F. Huidige stand van zaken op het gebied van zelf- en co-regulering

In 2018 heeft de Europese Commissie de oprichting van een nieuw zelfreguleringsinstrument voor desinformatie en politieke advertenties gefaciliteerd: De EU-gedragscode inzake desinformatie.³²⁷ Deze code is opgesteld in overeenstemming met de doelstellingen die zijn uiteengezet in de mededeling van de

³²⁰ Artikel 88 van Richtlijn 2001/83/EG, ten uitvoer gelegd in artikel 85 van de Geneesmiddelenwet.

³²¹ Zie bijlage II in samenhang met artikel 7, lid 4, van Richtlijn 2005/29/EG.

³²² Artikel 100 van de Geneesmiddelenwet.

³²³ Artikel 19 Richtlijn 2010/13/EU.

³²⁴ Artikel 13, lid 4, van Richtlijn 2002/58/EG.

³²⁵ Europese Commissie, *"Aanbeveling van de Commissie betreffende netwerken voor samenwerking bij verkiezingen, online transparantie, bescherming tegen cyberveiligheidsincidenten en de bestrijding van desinformatiecampagnes in het kader van de verkiezingen voor het Europees Parlement"*, C(2018)5949, blz. 4.

³²⁶ COM/2018/0184 definitief - 2018/089 (COD).

³²⁷ Europese Commissie, *'EU praktijkcode tegen desinformatie'*, preambule, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>. Zie Peter H. Chase, de EU-gedragscode inzake desinformatie: The Difficulty of Regulating a Nevelulous Problem, Transatlantic Working Group on Content Moderation Online and Freedom of Expression, 29 augustus 2019, https://www.ivir.nl/publicaties/download/EU_Code_Practice_Disinformation_Aug_2019.pdf.

Europese Commissie van 2018 over de aanpak van onlinedesinformatie³²⁸ en maakte deel uit van het actieplan tegen desinformatie.³²⁹ Onder andere Google, Facebook, Mozilla en Twitter hebben de Code ondertekend. Microsoft is in mei 2019 toegetreden.

De Code bevat een aantal maatregelen die bedrijven kunnen nemen om de uitdagingen van desinformatie aan te gaan. Deze omvatten de invoering van a) waarborgen tegen desinformatie; b) het intensiveren en aantonen van de doeltreffendheid van de inspanningen om valse accounts af te sluiten³³⁰ en duidelijke markeringssystemen en -regels voor bots, om ervoor te zorgen dat hun activiteiten niet kunnen worden verward met menselijke interacties; c) het intensiveren van, en communiceren over de doeltreffendheid van de inspanningen om de integriteit van de diensten met betrekking tot accounts die tot doel en met het oogmerk desinformatie te verspreiden te waarborgen; d) te investeren in technologische middelen om relevante, authentieke en nauwkeurige en gezaghebbende informatie te prioriteren, waar nodig in zoek-, feeds of andere automatisch gerangschikte distributiekkanalen; e) de zichtbaarheid van desinformatie af te zwakken door de vindbaarheid van betrouwbare inhoud te verbeteren; en f) te overwegen om gebruikers in staat te stellen instrumenten te gebruiken die een op maat gesneden en interactieve online-ervaring mogelijk maken, teneinde de ontdekking van content en de toegang tot verschillende nieuwsbronnen met alternatieve gezichtspunten te vergemakkelijken, en hen tevens te voorzien van gemakkelijk toegankelijke instrumenten om desinformatie te melden.

Voorts bevat de code een specifiek hoofdstuk over de integriteit van diensten en de ondernemingen die zich ertoe verbinden om (a) een duidelijk beleid in te voeren met betrekking tot de identiteit en het misbruik van geautomatiseerde bots op hun diensten en dit beleid binnen de EU te handhaven; en (b) een beleid in te voeren met betrekking tot wat ongeoorloofd gebruik van geautomatiseerde systemen is en dit beleid openbaar toegankelijk te maken voor EU-gebruikers op het platform.

Van bijzonder belang met betrekking tot de regulering van de politieke advertenties is verder de eis dat de ondertekenaars de regels moeten naleven ten aanzien van "Scrutiny of ad placements" gericht op "purveyors of disinformation" (deel II.A.) en Transparantie in politieke en *issue-based advertising* - met inbegrip van publieke bekendmakingen en gebruikersgerichte disclaimers (deel II.B.). Verder verplicht de Code de ondertekenaars tot het opstellen van jaarlijkse nalevingsverslagen. Deze bieden gedetailleerde informatie over hun politieke advertentie praktijken, zoals controle- en verificatieprocedures en verwijderingsstatistieken. (Sectie III).³³¹

De Code bevat ook een bijlage met de *best practices* van de verschillende ondertekenaars.³³² Daarnaast hebben de ondertekenaars routekaarten opgesteld voor de implementatie van de Code in hun respectieve organisaties.³³³ Facebook, Google en Twitter zijn door de Commissie gevraagd om maandelijks verslag uit te brengen over de voortgang van de implementatie van de Code. De verslagen van de maanden januari tot mei 2019 worden samen met de eigen beoordelingen van de Commissie gepubliceerd.³³⁴ De Commissie is over het algemeen tevreden over de toepassing van de code, maar heeft er bij Facebook, Google en Twitter op aangedrongen instrumenten te ontwikkelen om "de transparantie en

328 Europese Commissie, "Disinformatie online aanpakken: een Europese aanpak, COM(2018) 236 definitief", <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-236-F1-EN-MAIN-PART-1.PDF>.

329 Actieplan tegen desinformatie, GEMEENSCHAP (2018) 36 def.

330 Zie Financial Times, 'Facebook's fake numbers problem - Lex in depth', 18 november 2019 van <https://www.ft.com/content/98454222-fef1-11e9-b7bc-f3fa4e77dd47>.

331 Zie <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>

332 Europese Commissie, 'EU praktijkcode tegen desinformatie', preamble, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>

333 Zie: <https://ec.europa.eu/digital-single-market/en/news/roadmaps-implement-code-practice-disinformation>.

334 Zie: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

betrouwbaarheid van websites met advertenties ten behoeve van adverteerders te vergroten".³³⁵ Vóór eind 2019 zal de Commissie de doeltreffendheid van de code in het eerste jaar evalueren.

Concreet betekent de code dat Facebook, Twitter en Google allemaal *ad repositories*³³⁶ en *tools* voor politieke advertentietransparantie hebben gecreëerd.³³⁷ Google vereist bijvoorbeeld een identiteitscontrole voor adverteerders.³³⁸ Facebook vereist ook dat adverteerders zich moeten identificeren en stelt als extra eis dat adverteerders een inwoner moeten zijn van het land waar ze campagne willen voeren.³³⁹ De totstandkoming van dit beleid en de specifieke vereisten voor politieke advertenties door internetdiensten doet de logische vraag rijzen of deze wel effectief worden gehandhaafd. Daarnaast zijn deze en andere beleidswijzigingen door de platforms in gang gezet, specifiek ter voorbereiding op grote verkiezingen zoals de Amerikaanse presidentsverkiezingen in 2020.³⁴⁰ Verder heeft Twitter de "door de staat gecontroleerde nieuwsmedia" verboden om reclame te maken op het platform.³⁴¹ Ten slotte publiceerde Google op 20 november 2019 zijn nieuwe, meest recente beleid inzake politieke advertenties.³⁴² In het nieuwsbericht bij dit nieuwe Google-beleid wordt expliciet vermeld dat micro-targeting voor verkiezingsadvertenties niet is toegestaan. Voor verkiezingsadvertenties is targeting alleen toegestaan op basis van leeftijd, geslacht en postcode. *Contextual targeting* is wel toegestaan. In het geval van *contextuele targeting* voor verkiezingsadvertenties is het mogelijk om een advertentie te gebruiken op basis van onderwerpen en trefwoorden. Op dit moment is het nog steeds mogelijk om aan *microtargeting* te doen, aangezien het nog tot eind 2019 zal duren voordat deze verandering in heel Europa van kracht wordt. In de rest van de wereld zal dit nog langer duren. Google zal namelijk vanaf 6 januari 2020 beginnen met het doorvoeren van de wijzigingen. Het is niet bekend wanneer de implementatie zal zijn afgerond.

Naast deze georganiseerde zelfregulerende maatregelen hebben veel sociale mediaplatformen een eigen manier om desinformatie die verband houdt met politieke advertenties aan te pakken via hun platform-beleid. Facebook bijvoorbeeld, kondigde aan te stoppen met het controleren van politieke advertenties op hun inhoud, wat een debat op gang bracht over de wenselijkheid van ongecontroleerde politieke advertenties.³⁴³ Aan de andere kant kondigde Twitter aan dat het politieke advertenties op zijn platform volledig zal verbieden, wat naar verwachting opnieuw een discussie op gang zal brengen.³⁴⁴

G. Recente ontwikkelingen en voorstellen met betrekking tot desinformatie en politieke advertenties

Er zijn een aantal ontwikkelingen en voorstellen op EU-niveau inzake politieke advertenties en desinformatie, die verder gaan dan de zelfregulerende EU-gedragscodes over desinformatie. Ten eerste beveelt de Europese Commissie in haar aanbeveling van 2018 over verkiezingen en desinformatie aan dat de EU-

335 Europese Commissie, 'Code of Practice on Disinformation: Tussentijdse gerichte monitoring - Mei-rapporten'.

<https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation>.

336 Leerssen, P. e.a., 'Platform Ad Archief: Werkdocument 'Beloften en valkuilen'', 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380409.

337 Europese Commissie, 'Code of Practice on Disinformation: Tussentijdse gerichte monitoring - Mei-rapporten'.

<https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation>.

338 Google februari 2019 verslag, <https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation>.

339 Facebook april verslag p. 7 <https://ec.europa.eu/digital-single-market/en/news/fourth-intermediate-results-eu-code-practice-against-disinformation> <https://ec.europa.eu/digital-single-market/en/news/fourth-intermediate-results-eu-code-practice-against-disinformation>

340 Barrett, P.M., 'Disinformatie en de 2020-verkiezing: hoe de sociale media-industrie zich zou moeten voorbereiden', NYU Stern: september 2019, par. 3.

341 Zie Wong S., Shepherd C., & Liu, Q., 'Oude berichten, nieuwe memes: Peking's propagandaspelboek over de protesten in Hong-kong', Financial Times, 2019.

342 Google, 'Een update over ons beleid voor politieke advertenties', 20 november 2019 van <https://blog.google/technology/ads/update-our-political-ads-policy/>

343 Mike Isaac, 'Dissent Erupts at Facebook Over Hands-Off Stance on Political Ads', The New York Times, 28 oktober 2019, <https://www.nytimes.com/2019/10/28/technology/facebook-mark-zuckerberg-political-ads.html?module=inline>

344 Kate Conger, 'Twitter zal alle politieke advertenties verbieden, zegt C.E.O. Jack Dorsey', The New York Times, 30 oktober 2019, beschikbaar op: <https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html>

lidstaten a) de transparantie van betaalde online politieke advertenties en communicatie aanmoedigen en vergemakkelijken; en b) de openbaarmaking van informatie over campagne-uitgaven voor online activiteiten, waaronder betaalde online politieke advertenties en communicatie, aanmoedigen.³⁴⁵ Voorts heeft de Europese Commissie in haar mededeling over de Europese verkiezingen van 2018 verklaard dat de transparantie van politieke advertenties ook in de onlinewereld op vergelijkbare wijze moet gelden.³⁴⁶

Meer recent heeft de Europese Raad zijn conclusies over het waarborgen van vrije en eerlijke Europese verkiezingen aangenomen, waarin hij de nadruk legt op de noodzaak om "in overeenstemming met de toepasselijke regels de transparantie van betaalde politieke online-advertenties en -communicaties te bevorderen en te vergemakkelijken, met inbegrip van de reclaimedoeleinden ervan, de methoden waarmee zij op de burgers zijn gericht, en de financiering ervan".³⁴⁷

In de nieuwe politieke richtlijnen van de voorzitter van de Europese Commissie voor de volgende Commissie 2019-2024 staat dat er een Europees actieplan voor de democratie zal worden ingediend, dat "legislative proposals to ensure greater transparency on paid political advertising and clearer rules on the financing of European political parties".³⁴⁸ Daarnaast bevatten de richtsnoeren ook plannen voor "common standards to tackle issues such as disinformation and online hate messages" op digitale platforms.³⁴⁹

Een uitgelekt document van de diensten van de Commissie over de hervorming van de elektronische handel bevat specifieke regels voor "grensoverschrijdende online reclaimediensten, met inbegrip van regels over politieke advertenties, adequate mogelijkheden voor audits en verantwoordingsplicht, alsook met het oog op het verlagen van de toegangsdrempels voor concurrenten en alternatieven".³⁵⁰ Het meest recent, in oktober 2019, is de Commissie van start gegaan met haar plannen om een Europees Waarnemingscentrum voor digitale media op te richten, dat een digitaal platform zal zijn om desinformatie in Europa te helpen bestrijden.³⁵¹ Het zal dienen als een centrum voor feitencheckers, academici en onderzoekers om met elkaar samen te werken en actief samen te werken met mediaorganisaties en deskundigen op het gebied van mediageletterdheid, en om beleidsmakers te ondersteunen. Er is dus sprake van een aanzienlijke activiteit van de EU op het gebied van de regulering van desinformatie en politieke advertenties, met mogelijke EU-wetgeving over dit onderwerp die op verschillende gebieden op de wetgevende agenda van de EU komt te staan.

Naast het faciliteren van de EU Code of Practice on Disinformation, is de Europese Commissie al eerder gestart met zelfreguleringsinitiatieven die raken aan desinformatie. In 2015 werd het EU Internet Forum als onderdeel van de European Agenda on Security opgericht teneinde terroristisch en haat zaaiend materiaal tegen te gaan.³⁵² Het doel van het EU-internetforum is een gezamenlijke, vrijwillige aanpak van scha-

345 Europese Commissie, "Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and combat disinformation campaigns in the context of elections to the European Parliament", C(2018) 5949 final, blz. 8, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

346 Europese Commissie, "Mededeling over het waarborgen van vrije en eerlijke Europese verkiezingen, COM(2018) 637 definitief", <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0637:FIN>.

347 Conclusies van de Raad en de lidstaten over het waarborgen van vrije en eerlijke Europese verkiezingen, zoals aangenomen door de Raad op 19 februari 2019, 6573/1/19 REV 1, blz. 31, <https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf>.

348 Von der Leyen, U., "Een Unie die streeft naar meer - Mijn agenda voor Europa: Politieke richtsnoeren voor de volgende Europese Commissie 2019-2024", blz. 21, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

349 Ibid.

350 Zie Fanta, A. & Rudl, T., 'Leaked document: EU Commission mulls new law to regulate online platforms', [netzpolitik.org](https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/), 2019, <https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/>.

351 De Commissie doet een oproep om het Europees Waarnemingscentrum voor de digitale media op te richten, 7 oktober 2019, <https://ec.europa.eu/digital-single-market/en/news/commission-launches-call-create-european-digital-media-observatory>.

352 Europese Commissie, 'EU Internet Forum: Het samenbrengen van overheden, Europol en technologiebedrijven om terroristische inhoud en haatzaaien online te bestrijden', 3 december 2015 van https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243; zie ook: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

delijk materiaal door middel van samenwerking tussen publieke en private partijen. Ask.fm, Facebook, Google, Microsoft en Twitter nemen onder andere deel aan het EU-internetforum.³⁵³ Tijdens het vijfde EU-internetforum werd in oktober 2019 het EU-crisisprotocol gesloten. Het protocol is een reactie van de EU om de verwoesting door gebeurtenissen zoals de aanslag in Christchurch in te dammen. Het Protocol is een vorm van zelfregulering. Het protocol is ondertekend door de Europese Commissie, de lidstaten van de Europese Unie en particuliere actoren zoals Facebook, Twitter, Google, Microsoft, Dropbox, JustPaste.it en Snap.³⁵⁴ Het protocol is niet openbaar.

Het protocol bevat procedurele beschrijvingen voor de uitwisseling van kritieke informatie. Het protocol is verdeeld in vier fasen: goedkeuring, kennisgeving, uitwisseling van informatie en rapportage na de crisis. Het protocol is gebaseerd op drie beginselen: a) het publiek gerust te stellen dat de crisis wordt beheerst; b) ervoor te zorgen dat de spanningen worden verminderd; en c) de verspreiding van vals nieuws te voorkomen. Het protocol is van toepassing op uitzonderlijke situaties waarin nationale maatregelen niet volstaan. Het Protocol regelt het: a) een gecoördineerde en snelle reactie; b) een vergemakkelijking van de samenwerking tussen de openbare en de particuliere sector; en c) een vergemakkelijking van zelfregulering.³⁵⁵

H. Overzicht EU-kader

Tegen de achtergrond van het in hoofdstuk 4 ontwikkelde kader voor de grondrechten heeft dit hoofdstuk een overzicht gegeven van het relevante EU-rechtskader voor desinformatie. Het volgende hoofdstuk, waarin de Nederlandse nationale wetgeving wordt besproken, vult dit juridische kader aan.

Uit het overzicht van de relevante EU-wetgeving blijkt dat er sprake is van een grote verscheidenheid aan rechtsgebieden: aansprakelijkheid van tussenpersonen, privacyrecht, direct marketing, media- en commerciële regelgeving en zelfregulering op het gebied van desinformatie en (politieke) reclame. Belangrijk om op te merken is dat het exacte wettelijke kader dat van toepassing is op de volgende punten verschilt per: i) type dienst (hostingprovider, videoplatformdienst), ii) type communicatie (commercieel, gezondheid gerelateerd) en per iii) type medium (direct messaging, telecommunicatiedienst). De diversiteit van de relevante regelgeving betekent ook dat er verschillende toezichthouders bij betrokken zijn. Voor de Nederlandse context zijn dat de Autoriteit Persoonsgegevens, de ACM, de AFM en het Commissariaat voor de Media.

Een andere belangrijke opmerking is dat dit een zeer dynamisch rechtsgebied is. Een groot deel van de wetgeving is van recente datum (bv. de AVMD-richtlijn en de AVG), en andere wetgeving wordt momenteel herzien (bv. de e-Privacy Verordening). Naast deze wetgevende activiteiten zijn verschillende sociale-mediaplatforms actief bezig met het aanpakken van desinformatie in verband met politieke advertenties door middel van hun eigen beleid. Verder heeft de Commissie verschillende aanbevelingen gedaan en belangrijke ontwikkelingen op het gebied van zelf- en coregulering ondersteund. Deze snelle veranderingen betekenen dat het wettelijke kader voor politieke advertenties op EU-niveau zich snel ontwikkelt.

353 Europese Commissie, *'EU Internet Forum: Het samenbrengen van overheden, Europol en technologiebedrijven om terroristische inhoud en haatzaaien online te bestrijden'*, 3 december 2015 van https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243; zie ook: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

354 Europese Commissie, *'Terrorismebestrijding online: EU-Internetforum heeft zich verbonden tot een crisisprotocol voor de hele EU'*, oktober 2019 van https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6009

355 Europese Commissie, *'A Europe that protecting EU Crisis Protocol: responding to terrorist content online'*, oktober 2019 van https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf, *'A Europe that protecting EU Crisis Protocol: responding to terrorist content online'*, oktober 2019 van https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf

6. Nationaal wettelijk kader

- Het relevante nationaal wettelijk kader voor desinformatie doorsnijdt het privaatrecht, bestuursrecht en strafrecht en het omvat o.a.:
 - Privaatrecht: onrechtmatige daad (onrechtmatige perspublicatie) intellectueel eigendomsrecht.
 - Strafrecht: uitingsdelicten, verkiezingsdelicten, computercriminaliteit en verspreidingsdelicten.
 - Bestuursrecht: reclameregulering, financiering politieke partijen, nationale veiligheid, kritische infrastructuur.
- Wat betreft de zelfregulering zijn vooral de Nederlandse Reclame Code en de Raad voor de journalistiek van belang.
- Ook op nationaal niveau zijn er een groot aantal (zelf)reguleringsinitiatieven op het gebied van desinformatie.

Nu het grondrechtelijk kader van de vrijheid van meningsuiting en de van toepassing zijnde Europese regelgeving besproken zijn, kan gekeken worden naar het relevante Nationale recht. Hieronder volgt een overzicht van de verschillende nationale regelingen die van belang zijn voor de problematiek rond desinformatie. Bij de bespreking van de verschillende relevante normen wordt voor de structurering de klassieke indeling in privaatrecht, strafrecht en bestuursrecht gevolgd. Hier is voor gekozen omdat deze drie rechtsgebieden hun geheel eigen handhavingsinstrumenten en normatieve kaders kennen. Bij het bespreken van de strafrechtelijke normen ligt de focus specifiek op de reikwijdte van de delictsomschrijving “manipulatie van verkiezingen” en de vraag of deze uitgebreid kan worden om “onlinemanipulatie van verkiezingen” strafbaar te stellen. Bij deze bespreking worden ook de voor desinformatie relevante strafrechtelijke normen in het kader van computercriminaliteit besproken. Dit in het kader van de motie Asscher/Van Der Molen en de vijfde onderzoeksvraag van dit rapport.³⁵⁶ Bij de bespreking van de bestuursrechtelijke normen ligt de nadruk op regelgeving die relevant is voor de regulering van online politieke advertenties, dit vanwege deze specifieke focus uit de tussenrapportage.

Na de bespreking van de relevante wettelijke normen wordt ingegaan op de verschillende zelfreguleringsinstrumenten op nationaal niveau, voornamelijk met betrekking tot reclames en journalisten. Vervolgens wordt een overzicht gegeven van de relevante nationale regulatoire ontwikkelingen op het gebied van desinformatie.

A. Privaatrechtelijke normen

Nu het privaatrecht de algemene normen voor aansprakelijkheids-, overeenkomsten- en procesrecht omvat, raakt het onvermijdelijk op zeer veel punten aan de problematiek rond desinformatie. Aangezien het te ver reikt deze allemaal te bespreken, kan de focus gelegd worden op de nationale privaatrechtelijke normen die raken aan de vrijheid van meningsuiting en zo direct gerelateerd zijn aan desinformatie.³⁵⁷ Specifiek zijn de rechtsfiguur van de onrechtmatige daad en het intellectueel eigendomsrecht (“IE-recht”) van belang. Onrechtmatige uitingen kunnen bijvoorbeeld in veel gevallen tot desinformatie gerekend worden maar een parodie of satire nadrukkelijk niet.

³⁵⁶ Tweede Kamer, vergaderjaar 2018/2019 30 821, nr. 68.

³⁵⁷ Voor een bespreking van de Nederlandse aanpak van onrechtmatige content online zie: Brief Minister voor Rechtsbescherming, 17 juli 2019, 2644949 ‘Burgerinitiatief “Internetpesters aangepakt”’.

Binnen het civiele recht vormt de onrechtmatige daad uit artikel 6:162 BW de breedste mogelijkheid tot inperking van de vrijheid van meningsuiting. In de jurisprudentie zijn gedetailleerde normen ontwikkeld voor wanneer een uiting als onrechtmatig beschouwd kan worden en kan leiden tot onder andere schadevergoeding, een verbod of bijvoorbeeld een rectificatie.³⁵⁸ Er zijn veel raakvlakken tussen de onrechtmatige daad enerzijds en desinformatie anderzijds. Aan de ene kant kan een onrechtmatige uiting in veel gevallen onder de noemer van desinformatie geschaard worden nu het veelal onjuiste en schadelijke informatie betreft. Een belangrijk verschil is wel dat de intentie van de dader voor de onrechtmatigheid niet relevant is en voor desinformatie zoals vastgesteld wel. Aan de andere kant kan, indien er juridisch aantoonbare schade is en een duidelijke gelaedeerde, desinformatie vaak gekwalificeerd worden als een onrechtmatige uiting. In de context van de online verspreiding van desinformatie via internetdiensten zal het veelal specifiek gaan om het leerstuk van de onrechtmatige publicatie waarbij de schending van iemands eer en goede naam centraal staat. Vooral wat betreft desinformatie in connectie met nieuws gaat het juridisch gezien vaak om een onrechtmatige perspublicatie.

Dit in de jurisprudentie ontwikkelde leerstuk vereist dat de rechter een uitgebreide belangenafweging maakt waarbij de belangen van de laedens, de gelaedeerde en het bredere maatschappelijk belang tegen elkaar afgewogen worden. In de kern komt de belangenafweging neer op enerzijds de vrijheid van meningsuiting van de vermeende laedens, het recht om informatie te ontvangen van het bredere publiek en de bescherming van de persoonlijke levenssfeer van de beweerdelijk gelaedeerde.³⁵⁹ Het vormt dus een afweging waarbij twee fundamentele rechten, enerzijds artikel 10 en anderzijds artikel 8 EVRM tegen elkaar afgewogen moeten worden. Het EHRM volgt de lijn dat deze fundamentele rechten in principe van gelijkwaardig belang zijn.³⁶⁰ De Hoge Raad volgt het EHRM hierin en oordeelde in het *Hemelrijk*-arrest dat er geen aparte toetsing aan beide grondrechten plaatsvindt, maar dat er een afweging in factoren gemaakt moet worden,³⁶¹ die grotendeels ontleend worden aan het *Gemeenteraad*-arrest uit 1983.³⁶² De factoren op basis waarvan een belangenafweging gemaakt wordt, zijn onder andere of het een zaak van publiek belang betreft, of het om een publiek persoon gaat, de waarheidswaarde van de publicatie, de gebruikte toon en de werkwijze van degene die de uiting heeft gepubliceerd.³⁶³ Hieruit volgt dat het leerstuk een uitgebreide en gecompliceerde rechterlijke afweging en motivering vereist. Dit maakt dat het ook blijvend in ontwikkeling is met regelmatig nieuwe arresten.³⁶⁴

Daarnaast zijn er ook de specifiekere normen van het IE-recht, wat bijvoorbeeld het gebruik van auteurs- of merkenrechtelijk beschermd materiaal voor desinformatie verbiedt. Enerzijds reguleert het IE-recht dus specifieke typen desinformatie waarbij, bijvoorbeeld, voor commercieel gewin het publiek misleid wordt door valselijk gebruik te maken van een bepaald merk of wanneer geprobeerd wordt verkiezingen te verstoren door bepaalde teksten aan de verkeerde persoon toe te schrijven. Voor dit type desinformatie biedt het IE-recht handvatten voor regulering en handhaving. Anderzijds beschermt het IE-recht tegelijkertijd ook de vrijheid van meningsuiting door de parodie en de satire nadrukkelijk mogelijk te maken.³⁶⁵ Deze worden in de literatuur ook expliciet uitgesloten van het concept desinformatie.³⁶⁶ Het

358 Afdeling 10, titel 1, boek 6 BW.

359 Alberdingk Thijm, C., *'Kiezen uit twee hoogwaardige belangen'*, in: C. Eradus, C. Brouwer, H. & Veraart, M. (red.) *'Bodem kort geding'*, Amsterdam, 2013.

360 Couderc and Hachette Filipacchi Associés v. France (Application no. 40454/07) 10 november 2015 [GC], § 91

361 HR 18 januari 2008, NJ 2008/274 (*van Gasteren/Hemelrijk*).

362 HR 24 juni 1983, NJ 1984/801.

363 Conclusie, Hoge Raad (Advocaat-Generaal), 07-09-2007 ECLI:NL:PHR:2008:BB3210, ro. 6.

364 HR 22-03-2019, ECLI:NL:HR:2019:402 RvdW 2019/404; HR 26-10-2018, ECLI:NL:HR:2018:1987 RvdW 2018/1207; HR 25-05-2008, ECLI:NL:HR:2008:BC9107.

365 Artikel 5(3)k Richtlijn 2001/29/EG, geïmplementeerd in artikel 18b Auteurswet.

366 Zie bijvoorbeeld EAVI, juli 2017 "Beyond 'fake news' 10 types of misleading news", beschikbaar op: https://eavi.eu/wp-content/uploads/2017/07/beyond-fake-news_COLOUR_WEB.pdf;

McGonagle, T. e.a., *'Inventarisatie methodes om "nepnieuws" tegen te gaan'*, Instituut voor Informatierecht, 2018; Wardle, C., & Derakhshan, H. *'Information Disorder. Toward an interdisciplinary framework of research and policymaking'*, September 7, 2017 p. 17.

is echter niet eenvoudig vast te stellen wanneer sprake is van een parodie en er bestaat gedetailleerde jurisprudentie op zowel Nederlands als Europees niveau.³⁶⁷

Enige aansprakelijkstelling op basis van de onrechtmatige daad of auteursrechtinbreuk hangt wat betreft desinformatie verspreid via internetdiensten vervolgens ook nauw samen met het aansprakelijkheidskader voor internettussenpersonen uit de Richtlijn elektronische handel.³⁶⁸ Wanneer een internettussenpersoon buiten de zogenaamde *safe harbour* valt en niet adequaat een onrechtmatige uiting adresseert, loopt deze het risico zelf civielrechtelijk vervolgt te worden. De *safe harbour* is dus van groot belang voor de gelaedeerde nu het bepalend is voor welke actoren hij of zij aansprakelijk kan stellen. Wanneer desinformatie via een internetdienst een onrechtmatige daad vormt en deze internetdienst zich op de *safe harbour* kan beroepen, kan de gelaedeerde namelijk alleen de verspreider van de desinformatie aanspreken. Om een succesvol beroep op de hosting *safe harbour* in stand te houden, moet de internetdienst actie ondernemen zodra het kennis heeft van de onrechtmatige inhoud (*notice and action*). Aangezien de REH een horizontale beperking van de aansprakelijkheid biedt, geldt dit ook voor de hieronder te bespreken strafrechtelijke normen.

Hieraan direct gerelateerd is het feit dat het instellen van een vordering hierdoor vaak afhankelijk van door de internetdiensten aangeleverde persoonsgegevens van degene die de uiting gedaan heeft. Deze persoonsgegevens worden veelal pas op rechterlijk bevel verstrekt nu zich hier een ingewikkeld samenspel voordoet van gegevensbeschermingsnormen en verschillende aansprakelijkheidsgrondslagen uit onder andere de E-Privacy richtlijn, de Handhavingsrichtlijn en de eerder besproken REH.³⁶⁹ Wanneer een dergelijk rechterlijk bevel uitgevaardigd wordt, is in de rechtspraak ontwikkeld waarbij het *Lycos/Pessers*-arrest als de standaard geldt.³⁷⁰ De rechter toetst of (i) het voldoende aannemelijk is dat de informatie jegens de derde onrechtmatig en schadelijk is, (ii) of de derde een reëel belang heeft bij het verkrijgen van de persoonsgegevens, (iii) of er geen minder ingrijpende wijze voorhanden is om de gegevens te verkrijgen en (iv) of een afweging van de belangen van de derde, de internetdienst, en degene wiens persoonsgegevens het betreft, uitvalt in het voordeel van de derde.³⁷¹ Dit leerstuk vereist dus wederom een uitgebreide en genuanceerde rechterlijke toetsing wat maakt dat het volop in ontwikkeling is.³⁷²

Hoewel dit slechts een selectie is van de privaatrechtelijke normen die mogelijk van invloed kunnen zijn op de problematiek rond desinformatie vormt het aansprakelijkheidsrecht met specifiek de onrechtmatige daad en daarnaast het intellectueel eigendomsrecht de meest relevante privaatrechtelijke normen en kan uit deze korte uiteenzetting al een aantal heldere conclusies getrokken worden. De bovenstaande leerstukken laten namelijk duidelijk zien hoe complex en context specifiek de uitleg en concrete toepassing van deze normen zijn. De grens tussen een rechtmatige en onrechtmatige publicatie is zeer moeilijk te trekken, wat heeft geleid tot een zeer genuanceerde en afgewogen jurisprudentie. Hetzelfde geldt voor wanneer een uiting te gelden heeft als een te beschermen satire en wanneer niet. Dit compliceert de mogelijke regulering van desinformatie aanzienlijk nu het betekent dat in dit soort gevallen de juridische kwalificatie moeilijk te maken is.

367 Zie bijvoorbeeld: Hof Amsterdam 13-09-2011, ECLI:NL:GHAMS:2011:BS7825, *IER* 2012/15 met annotatie van Mr. Herman M.H. Speyart; HvJEU 03-09-2014, C-201/13 (*Deckmyn*).

368 Zie paragraaf 5.A.

369 Richtlijn 2002/58/EG; Richtlijn 2004/48/EG; Richtlijn 2000/31/EG; Zie Kingma, S.H., 'De botsing tussen IE- en privacyrechten. Het einde van het *Lycos/Pessers*-tijdperk', *P&I* 2012/4 p. 171-177.

370 HR 25-11-2005, ECLI:NL:HR:2005:AU4019.

371 Idem, r.o. 4.10.

372 Kingma, S.H. 'De botsing tussen IE- en privacyrechten. Het einde van het *Lycos/Pessers*-tijdperk', *P&I* 2012/4 p. 171-177; HvJEU nr. C-275/06 (*Productores de musica de espana (Promusicae)/Telefonica de Espana SAU*).

B. Strafrechtelijke normen

Een groot aantal van de typen uitingen die onder de noemer van desinformatie vallen, zijn (deels) op nationaal niveau strafrechtelijk genormeerd. In de eerste plaats kan gedacht worden aan de algemene strafrechtelijke normen die zuiver zien op de inhoud van een specifieke uiting en als zodanig grenzen stellen aan de vrijheid van meningsuiting. Dit zijn strafbepalingen zoals smaad (261 Sr), laster (262 Sr), haatzaaiing (137d Sr) en bijvoorbeeld groepsbelediging (137c Sr). Vervolgens zijn de strafrechtelijke normen die specifiek betrekking hebben op het democratische proces van bijzonder belang voor de problematiek rond desinformatie nu verstoring van het democratische proces één van de voornaamste gevreesde effecten van desinformatie is. Deze zullen hieronder besproken worden.

Net zoals bij de privaatrechtelijke normen hangt de handhaving van strafrechtelijk genormeerde desinformatie samen met het aansprakelijkheidskader voor internettussenpersonen uit de Richtlijn elektronische handel.³⁷³ Zolang een internettussenpersoon binnen de *safe harbour* valt kan deze niet strafrechtelijk vervolgd worden voor eventuele desinformatie. Daarnaast wordt er momenteel een verbetering in de beschikbaarheid van bewijsmateriaal via internetdiensten in strafrechtelijk onderzoek nagestreefd middels de voorstellen voor een eEvidence regulering op Europees niveau.

Drie categorieën strafrechtelijke bepalingen zijn relevant om verder uit te werken in het kader van desinformatie, specifiek in relatie tot het democratische verkiezingsproces. Dit zijn de strafrechtelijke normen die zien op het beïnvloeden van het verkiezingsproces, normen die zien op computercriminaliteit en een aantal van de zogenoemde verspreidingsdelicten.

i. Onlinemanipulatie van verkiezingen

De Motie Asscher/Van der Molen verzoekt de regering te onderzoeken “of huidige delictsomschrijvingen bij het manipuleren van verkiezingen kunnen worden uitgebreid, zodat bewuste onlinemanipulatie ook strafrechtelijk kan worden aangepakt”.³⁷⁴ Alvorens de bestaande strafrechtelijke mogelijkheden te onderzoeken is het belangrijk stil te staan bij het concept “onlinemanipulatie”. Zoals uit de analyse van het concept desinformatie in hoofdstuk 2 bleek, moet online manipulatie begrepen worden als het via technologische middelen het heimelijk beïnvloeden van iemands besluitvorming. Dit omvat een grote verscheidenheid aan praktijken en de Europese Commissie heeft aangegeven dat de problematische en onacceptabele versie van onlinemanipulatie betstaat uit beïnvloeding “[that is] subliminal, exploits existing vulnerabilities or cognitive biases, and/or encroaches on the independence and authenticity of individual decision-making”.³⁷⁵ In de context van het democratische verkiezingsproces is het van belang dat kiezers zelfstandig een mening vormen over de wijze waarop ze hun stemrecht willen uitoefenen en onlinemanipulatie technieken kunnen daar een bedreiging voor vormen.

Er zijn een aantal verschillende strafbepalingen gerelateerd aan deze conceptualisatie van “onlinemanipulatie”, en de verspreiding van desinformatie via internetdiensten in het kader van de oneigenlijke beïnvloeding van verkiezingen. Dit betreft in de eerste plaats titel IV van het wetboek van Strafrecht (“Sr”) genaamd “Misdrijven betreffende de uitoefening van staatsplichten en staatsrechten” waaronder vijf bepalingen die direct zien op het op enige wijze verhinderen van het uitoefenen van het kiesrecht. Daarnaast zijn ook enkele bepalingen uit afdeling VI van de Kieswet die bepaalde handelingen in het kader van het verkiezingsproces strafbaar stellen.

De eerste bepaling die betrekking heeft op het verkiezingsproces stelt strafbaar het verhinderen van het vrij en onbelemmerd uitoefenen van het kiesrecht door middel van geweld of de dreiging van geweld.

³⁷³ Zie paragraaf 5.A.

³⁷⁴ Tweede Kamer, vergaderjaar 2018/2019 30 821, nr. 68.

³⁷⁵ Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, Decl(13/02/2019)1, section 9.

ARTIKEL 125 SR

Hij die bij gelegenheid van een krachtens wettelijk voorschrift uitgeschreven verkiezing **door geweld of bedreiging met geweld opzettelijk iemand verhindert zijn of eens anders kiesrecht vrij en onbelemmerd uit te oefenen, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.**

Dit betreft uitoefening van het kiesrecht voor bij wet in formele zin uitgeschreven verkiezingen. Tussen het geweld of de dreiging met geweld en de verhindering van het kiesrecht moet een causaal verband vastgesteld worden. Ook moet het opzet zien op het verhinderen van de vrije uitoefening van het kiesrecht, hieronder vallen alle gradaties van opzet. Voor de invulling van “geweld” moet teruggegrepen worden op artikel 81 Sr en voor de uitleg van “dreiging met geweld” kan gekeken worden naar dezelfde bewoordingen uit artikel 95, 242 en 284 Sr. De Hoge Raad heeft verduidelijkt dat bij bedreiging met geweld noodzakelijk is “dat de bedreiging van dien aard is en onder zodanige omstandigheden is geschied, dat bij de bedreigde in redelijkheid de vrees kon ontstaan dat geweld tegen hem zou worden uitgeoefend”.³⁷⁶ Bij de invoering is discussie geweest over de vraag of er niet een bredere dreiging dan alleen de dreiging met geweld in de delictsomschrijving opgenomen moest worden. Toentertijd is er expliciet besloten alleen de dreiging met geweld strafbaar te stellen “juist omdat bij dit misdrijf de politieke inzichten en hartstogten in het spel zijn, is het wenschelijk, het strafbaar feit zoo naauwkeurig mogelijk te omschrijven”.³⁷⁷ Dit maakt dat stemmingmakerij, of bangmakerij via de media onvoldoende is. Er moet daadwerkelijk sprake zijn van een concrete bedreiging waardoor iemand redelijkerwijs kan vrezen dat er geweld tegen hem gebruikt gaat worden.

Vervolgens moet er sprake zijn van een causaal verband tussen dit geweld of deze bedreiging met geweld en de uitoefening van het kiesrecht. Dit geweld of deze dreiging moet de kiezer feitelijk belet of psychisch gedwongen hebben waardoor er geen sprake meer was van het “vrij en onbelemmerd” uitoefenen van het kiesrecht.³⁷⁸ Dit laatste bestanddeel, “vrij en onbelemmerd” uitoefenen van het kiesrecht, moet breed geïnterpreteerd worden en omvat niet slechts het inleveren van het stembiljet. Ook het stemgeheim en het zelf uitkiezen van het tijdstip van het uitbrengen van de stem valt onder.³⁷⁹ Hiermee is deze delictsomschrijving breder dan die in het hieronder te bespreken 126 Sr. Dat het geweld of de bedreiging direct in verband moet staan met het uitbrengen van de stem houdt ook in dat handelingen voorafgaande aan de verkiezingsperiode buiten beschouwing worden gelaten.³⁸⁰

ARTIKEL 126 SR

- Hij die bij gelegenheid van een krachtens wettelijk voorschrift uitgeschreven verkiezing door gift of belofte iemand omkoopt om zijn of eens anders kiesrecht hetzij niet, hetzij op bepaalde wijze uit te oefenen, wordt gestraft met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie.
- Dezelfde straf wordt toegepast op de kiezer of de gemachtigde van een kiezer die zich door gift of belofte tot een of ander laat omkopen.

Dit artikel verbiedt het een kiezer of diens gemachtigde om te kopen en heeft een iets kleinere beschermingsomvang dan artikel 125 Sr: vergelijk “vrij en onbelemmerd” met “hetzij niet, hetzij op bepaalde

³⁷⁶ HR 3 februari 2015, NJ 2015/245 zie verder HR 7 juni 2005, NJ 2005/448

³⁷⁷ Smidt (1881) p. 60-61.

³⁷⁸ T&C Strafrecht, commentaar op artikel 125 Sr.

³⁷⁹ Noyon/Langemeijer/Remmelink Strafrecht, artikel 125 Sr, aant. 7.

³⁸⁰ *Idem.*, aant. 6.

wijze". Het moet gaan om de inhoud van de stem of de wijze waarop, bijvoorbeeld via een volmacht. Omkoping tot enkel het uitbrengen van een stem ongeacht de inhoud is niet strafbaar.³⁸¹

Met "omkopen" wordt niet gerefereerd aan enig civielrechtelijke rechtsfiguur van de koop maar aan een bepaalde wederkerigheid tussen het handelen van de omkoper en de stemgerechtigde.³⁸² Het vereiste van opzet zit in dit concept besloten. Geen causaal verband is vereist tussen de omkoping en het daadwerkelijk uitoefenen van de stem, een aangenomen aanbod tot omkoping als zodanig is voldoende.³⁸³ In een recente zaak heeft de Hoge Raad geoordeeld dat wanneer een kiezer een gift en/of belofte aanneemt en daarbij, gelet op de concrete omstandigheden van het geval, de redelijke verwachting wekt dat hij zijn kiesrecht op een bepaalde wijze zal uitoefenen, het omkopen is voltooid. Dit hoeft niet uitdrukkelijk toegezegd of kenbaar gemaakt te worden.³⁸⁴

Dit artikel is zeer nauw verbonden met artikel Z4 Kieswet wat het strafbaar stelt wanneer iemand "door gift of belofte, een kiezer omkoopt om volmacht te geven tot het uitbrengen van zijn stem". Er kan dan sprake zijn van eendaadse samenloop (art. 55(2) Sr).³⁸⁵

ARTIKEL 128 SR

Hij die opzettelijk **zich voor een ander uitgevende**, aan een krachtens wettelijk voorschrift uitgeschreven **verkiezing deelneemt**, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.

Deze strafbepaling spreekt vrij voor zich. Het gaat om het uitbrengen van een stem, terwijl iemand zich voordoet als iemand anders en op die manier het stemrecht van de tweede persoon frustreert. In de officiële registratie van het stembureau staat dan immers dat deze tweede persoon al gestemd heeft, terwijl dit niet het geval is.

ARTIKEL 129 SR

Hij die bij gelegenheid van een krachtens wettelijk voorschrift uitgeschreven verkiezing, opzettelijk een laats gehad hebbende **stemming verijdt** of enige **bedrieglijke handeling pleegt waardoor aan de stemming een andere uitslag wordt gegeven dan door de wettig uitgebrachte stemmen zou zijn verkregen**, wordt gestraft met gevangenisstraf van ten hoogste een jaar en zes maanden of geldboete van de vierde categorie

In tegenstelling tot de voorgaande artikelen ziet deze bepaling op uitkomst van de verkiezingen, de andere artikelen gingen om het vrij en zuiver uitbrengen van de stem zelf.³⁸⁶ Dit is een vrij brede strafbepaling, alle handelingen die een afgelopen stemming ongeldig maken vallen hier onder. Alle handelingen vóór sluiting van de stemming vallen buiten deze strafbepaling en vallen eerder aan artikel 127 Sr. Handelingen die onder artikel 129 Sr vallen zijn bijvoorbeeld het openbreken van de stembus, of het verduisteren van de stembrieven.³⁸⁷ Bij het tweede deel van de strafbepaling kan het wel gaan om handelingen voor het sluiten van de stemming. Noodzakelijk is dat de uitslag van de verkiezingen anders

³⁸¹ *Ibidem*.

³⁸² Smidt (1881) p. 62; J.S. Nan, Commentaar op Wetboek van Strafrecht art. 126 (Strafrecht) (artikeltekst geldig vanaf 01-05-1984).

³⁸³ M.A.H. van der Woude, T&C Strafrecht, commentaar op artikel 126 Sr.

³⁸⁴ HR 7 juni 2019, ECLI:NL:HR:2019:843, NJ 2019/242, ro. 7.7.

³⁸⁵ J.S. Nan, Commentaar op Wetboek van Strafrecht art. 126 (Strafrecht) (artikeltekst geldig vanaf 01-05-1984).

³⁸⁶ Smidt II p. 65.

³⁸⁷ T&C Strafrecht, commentaar op artikel 129 Sr

geworden zijn door de handeling (als in de absolute aantallen stemmen), niet dat de winnaar of de zetelverdeling anders geweest zou zijn.³⁸⁸

ARTIKEL 127 SR

Hij die bij gelegenheid van een krachtens wettelijk voorschrift uitgeschreven verkiezing, enige bedrieglijke handeling pleegt waardoor een stem van onwaarde wordt of een ander dan de bij het uitbrengen van de stem bedoelde persoon wordt aangewezen, wordt gestraft met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie

Van al deze verschillende bepalingen lijkt artikel 127 uit deze titel IV Sr het meest geschikt om “bewuste onlinemanipulatie” onder te scharen, vandaar dat bij deze bepaling het meest uitgebreid stilgestaan wordt. Het doel van dit artikel is het beschermen van de “argeloze en onwetende kiezers” tegen misleiding.³⁸⁹ Dit artikel heeft hoofdzakelijk betrekking op fraude ten aanzien van het stembiljet zelf, bijvoorbeeld door kiezers moedwillig ongeldige stembiljetten aan te bieden. De relevante bestanddelen zijn (i) een **causaal verband**, (ii) een **bedrieglijke handeling** en (iii) het gevolg van de bedrieglijke handeling namelijk (iii-a) het van **onwaarde** worden van de stem of (iii-b) de **error in persona**.

Allereerst moet stilgestaan worden bij het **causale verband** nu dit verreweg het meest problematische bestanddeel is en bepalend is voor de omvang van zowel de mogelijke oorzaak (bedrieglijke handeling) als de mogelijke gevolgen (ongeldige stem of error in persona). Simpel gezegd moet deze concrete bedrieglijke handeling als gevolg hebben dat de stem van onwaarde is of dat de verkeerde kandidaat wordt aangewezen.³⁹⁰ Er moet dus een causaal verband vastgesteld worden tussen beide handelingen. Waar het problematisch wordt, is dat de parlementaire geschiedenis de indruk wekt dat een zogenaamde “causa proxima” vereist is waarbij de bedrieger het stembiljet rechtstreeks tot voorwerp van zijn handeling maakt. Deze indruk ontstaat omdat de voorbeelden in de parlementaire geschiedenis alle direct op het stembiljet zien.³⁹¹ Fokkens betoogt echter dat een dergelijk streng vereiste losgelaten moet worden: ook wanneer de kiezer zelf nog handelingen verricht ten aanzien van het stembiljet *na* de bedrieglijke handeling kan aan de delictsomschrijving voldaan worden.³⁹² Cruciaal aan deze interpretatie is dat het verspreiden misleidende informatie ook onder de delictsomschrijving gebracht wordt. Dit betoog wordt door Nan en van der Woude gevold.³⁹³ In dit rapport wordt de meer extensieve lezing van Fokkens aangehouden, nu het vereiste van een causa proxima de delictsomschrijving te zeer zou beperken. Het is bijvoorbeeld wenselijk om het volgende ook onder de delictsomschrijving te brengen: de situatie waarin kiezers bij het stemloket wijsgemaakt worden dat de stemprocedure gewijzigd is, waardoor hun stemmen ongeldig worden.

Het tweede te bespreken bestanddeel betreft dan ook de mogelijke gevolgen van de bedrieglijke handeling die onder de delictsomschrijving vallen: (i) de **stem wordt van onwaarde** of (ii) de **error in persona**. Met betrekking tot het eerste mogelijke gevolg, het van onwaarde worden van de stem, moet dit door het stembureau vastgesteld worden aan de hand van de objectieve criteria van het kiesreglement.³⁹⁴ Dit betekent dat het desbetreffende stembureau een uitgebrachte stem ongeldig moet verklaren. Dit is een vrij strikt en objectief vast te stellen criterium. Ook het tweede mogelijke gevolg, de error in persona, moet strikt uitgelegd worden. Of er “op een andere persoon is gestemd dan bedoeld”, moet namelijk

388 Noyon/Langemeijer/Rommelink Strafrecht, artikel 129 Sr, aant. 2.

389 Smidt II p. 62.

390 HR 10 juni 1924, W 11227.

391 Smidt II p. 62.

392 Fokkens, Noyon/Langemeijer/Rommelink Strafrecht, artikel 127 Sr, aant. 2.

393 J.S. Nan, Commentaar op Wetboek van Strafrecht art. 127 (Strafrecht) (artikeltekst geldig vanaf 01-05-1984); M.A.H. van der Woude, T&C Strafrecht, commentaar op artikel 127Sr.

394 *Ibid.*

nauw geïnterpreteerd worden: het gaat om de situatie waarbij de stemmer onder de overtuiging verkeert dat hij op de ene kandidaat X heeft gestemd terwijl hij in werkelijkheid op een andere kandidaat Y heeft gestemd.³⁹⁵ Situaties waarin een kiezer in de war is over wie een specifieke kandidaat is (was kandidaat X degene die eerder ook in de Tweede Kamer zat?) of wat de exacte politieke overtuigingen van een kandidaat zijn (Is kandidaat X wel of niet voor belastingverlaging?) vallen hier expliciet niet onder. Een recente uitspraak van het Hof Den Bosch (2008) had deze error in persona als onderwerp en verduidelijkt hoe nauw dit criterium geïnterpreteerd moet worden. Het ging over fraude met betrekking tot de stemcomputer waarbij de verdachte “als bedienaar van de stemmachine meermalen en op verschillende tijdstippen die stemcomputer niet [heeft] vrijgegeven, als een stemmer zijn of haar stem wilde/ging uitbrengen. Hij heeft vervolgens in strijd met de werkelijkheid tegen die stemmers gezegd dat zij hadden gestemd en/of die stemmers zich laten verwijderen zonder hen erop te attenderen dat zij niet een rechtsgeldige stem hadden uitgebracht en hij heeft op (een) later(e) tijdstip(pen) telkens de stemcomputer alsnog vrijgegeven en telkens een stem op zichzelf uitgebracht.”³⁹⁶

Vervolgens moet als laatste het bestanddeel “**bedrieglijke handeling**” uitgewerkt worden. Belangrijk is dat het vereiste van opzet besloten zit in dit bestanddeel en alle gradaties van opzet omvat.³⁹⁷ Dan de mogelijke handelingen die onder dit bestanddeel kunnen vallen. Dit wordt enerzijds bepaald door de omvang van het causaal verband en anderzijds door de gevolgen die onder de delictsomschrijving vallen. In algemene zin omschrijft de parlementaire geschiedenis “bedrieglijke handelingen” als “kunstgrepen” die bedoeld zijn om kiezers anders te laten stemmen dan zij van plan waren, bijvoorbeeld door middel van nepstembiljetten.³⁹⁸ De hierboven uitgewerkte meer extensieve interpretatie van het causaliteitsvereiste vult deze algemene beschrijving verder aan door ook *misleidende uitingen* onder “bedrieglijke handelingen” in de zin van de delictsomschrijving te laten vallen. Vervolgens zijn er een aantal voorbeelden uit de literatuur en jurisprudentie die het begrip verder inkleuren. Nan geeft als voorbeeld het verspreiden van misleidende informatie “zoals het doorgeven van een verkeerde kieslijst”.³⁹⁹ Fokkens geeft vervolgens als voorbeeld een partij die liegt over zijn lijstnummer, waardoor verwarring wordt gesticht. Een soortgelijke zaak uit het eind van de 19^e eeuw heeft in Utrecht tot een veroordeling geleid. Twee verkiezingen vonden tegelijkertijd plaats en ter onderscheiding hadden de stembiljetten een verschillende kleur. Eén van de partijen had kiezers aan de vooravond van de verkiezingen onjuist voorgelicht over deze kleuren waardoor mensen uiteindelijk voor een andere kandidaat gestemd bleken te hebben dan zij wilden.⁴⁰⁰ Terugkerend naar het causaliteitsvereiste geeft deze Utrechtse zaak ook steun aan de extensieve interpretatie van het vereiste causaal verband en dus de bredere interpretatie van bedrieglijke handelingen. Hoewel er brede steun is en goede argumenten te geven zijn voor deze interpretatie, is zonder een definitieve rechterlijke uitspraak niet met absolute zekerheid te zeggen of naast fysieke handelingen ook het verspreiden van misleidende of onjuiste informatie onder de delictsomschrijving gebracht moet worden.

Wat wel met volledige zekerheid gezegd kan worden is dat het te ver gaat om het verspreiden van onjuiste informatie over de *politieke overtuigingen* van een kandidaat onder “bedrieglijke handelingen” te laten vallen. Uit de parlementaire geschiedenis blijkt dat deze keuze is gemaakt met als reden “Zooveel mogelijk blijve de regter buiten de politiek; zooveel mogelijk voorkome men door eene scherpe definitie van het misdrijf, dat de politiek op het oordeel van den regter, ook zijns ondanks, invloed uitoefene”.⁴⁰¹ Dat het verspreiden van onjuiste informatie over de politieke overtuigingen niet onder de delicts-

395 *Ibid.* aantekening 4.

396 Hof Den Bosch, 18 januari 2008, ECLI:NL:GHSHE:2008:BC2171.

397 Van der Woude, T&C Strafrecht, commentaar op artikel 127 Sr.

398 Smidt II p. 63.

399 J.S. Nan, Commentaar op Wetboek van Strafrecht art. 127 (Strafrecht) (artikeltekst geldig vanaf 01-05-1984).

400 HR 10 november 1890, W 5966.

401 Smidt II p. 62; Fokkens, Noyon/Langemeijer/Rommelink Strafrecht, artikel 127 Sr, aant. 3.

omschrijving valt, volgt ook uit het feit dat dergelijke onjuiste informatie niet als causaal effect kan hebben dat dat een uitgebrachte stem van onwaarde wordt of dat er een error in persona gemaakt wordt.

Uit de analyse van de drie centrale bestanddelen volgt een vrij duidelijk beeld van welke situaties wel en niet strafbaar gesteld worden door artikel 127 Sr. Hierbij is voornamelijk het volgende van belang: misleiding over de politieke overtuigingen van een kandidaat en misleiding die erin resulteert dat iemand niet gaat stemmen vallen, zijn beide *geen* bedrieglijke handelingen en zijn dus *niet* strafbaar onder 127 Sr. Voor beide geldt namelijk dat het niet als gevolg kan hebben dat een uitgebrachte stem van onwaarde wordt of er een error in persona plaatsvindt.

Uit het voorgaande blijkt duidelijk dat artikel 127 Sr raakvlakken kent met de verspreiding van desinformatie via internetdiensten nu het beide betrekking hebben op de verspreiding van onjuiste of misleidende informatie en maatschappelijke schade, met name aan het verkiezingsproces. Omdat de huidige formulering van het artikel technologie-neutraal is, beperkt het zich al niet tot bedrieglijke handelingen in de fysieke ruimte of via een specifiek medium. De voorbeelden gegeven door Fokkens en Nan zijn geenszins medium gebonden en zouden zich ook via moderne communicatievormen kunnen voordoen. Zo is in deze lezing van artikel 127 Sr het verspreiden van opzettelijk misleidende informatie via een sociale mediadienst over, bijvoorbeeld, de vereiste stemwijze wat daadwerkelijk tot een ongeldige stem leidt, verboden. Ook het "hacken" van een stemcomputer waardoor het aanklikken van kandidaat X telkens geteld wordt als een stem voor kandidaat Y, wordt door dit artikel verboden. De onderstaande tabel geeft een beeld van het type situaties die door artikel 127 Sr al gedekt wordt in de bovenstaande interpretatie van het artikel.

Situatie	Strafbaar onder 127 Sr?		Desinformatie?
Online moedwillig mensen verkeerd informeren over de vereiste stemwijze (pen ipv rood potlood).	Ja	Als het causaal verband vastgesteld kan worden heeft deze misleidende informatie als gevolg dat een stem ongeldig is.	Ja
Een stemcomputer manipuleren waardoor als kandidaat X wordt gekozen, het geregistreerd wordt als een stem voor kandidaat Y.	Ja	Deze "bedrieglijke handeling" heeft een error in persona als gevolg.	Nee
Kiezers frauduleuze stembiljetten geven in het stemlokaal.	Ja	Deze "bedrieglijke handeling" heeft als gevolg dat een stem ongeldig wordt verklaard.	Nee
Een uitgebrachte stem verwisselen met een stembiljet waar op een andere kandidaat is gestemd.	Ja	Deze "bedrieglijke handeling" heeft een error in persona als gevolg.	Nee
Het op sociale media moedwillig verspreiden van onjuiste informatie over een verkiezingsprogramma.	Nee	Deze foutieve informatie kan niet als gevolg hebben dat een stem ongeldig wordt of een error in persona.	Ja
Online moedwillig de verkeerde datum van een stemming verspreiden.	Nee	Deze foutieve informatie kan niet als gevolg hebben dat een stem ongeldig wordt of een error in persona.	Ja

Tabel 2

Gezien al deze connecties die er te maken zijn met problematiek rond desinformatie is de vraag in hoeverre de bepaling überhaupt aangepast moet worden om ook de gewenste "onlinemanipulatie" te omvatten. Een drietal elementen zijn hierbij van belang: (i) de onduidelijkheid van het concept "online

manipulatie”, (ii) de mogelijke impact op de vrijheid van meningsuiting en (iii) het feit dat de hierboven gevolgde extensieve interpretatie van het causale verband in artikel 127 Sr niet rechterlijk bevestigd is.

Wanneer “onlinemanipulatie” vrij nauw geïnterpreteerd wordt als “opzettelijk misleidende uiting via een internetdienst die in direct causaal verband staat met of het ongeldig worden van een stem of de overtuiging bij een kiezer dat op de ene persoon gestemd is terwijl er in werkelijkheid op een ander gestemd is”, dan valt dit onder de delictsomschrijving van artikel 127 Sr. De tabel hierboven geeft een beeld van welk type handelingen dan al wel strafbaar gesteld wordt. Dit is natuurlijk wel een zeer specifieke lezing van “onlinemanipulatie” en dit begrip kan ook veel breder geïnterpreteerd worden. Maar wanneer de delictsomschrijving van artikel 127 Sr uitgebreid zou worden, ontstaan er problemen met de vrijheid van meningsuiting. De misleidende uitingen die de bepaling strafbaar stelt zijn namelijk gerelateerd aan het politieke proces waarin de vrijheid van meningsuiting van artikel 10 EVRM de meest uitgebreide bescherming kent.⁴⁰² Vervolgens geldt in algemene zin dat het verspreiden van onjuiste informatie onder de bescherming van artikel 10 EVRM valt en niet zonder verdere kwalificatie verboden kan worden.⁴⁰³ Verdere uitbreiding van de delictsomschrijving zou een verregaande inperking van de vrijheid van meningsuiting vormen.

Deze interpretatie is vervolgens ook afhankelijk van de meer extensieve lezing van het causaal verband waarbij geen “causa proxima” vereist wordt. Hoewel deze lezing door de literatuur ondersteund wordt, is het van belang een dergelijk extensieve interpretatie te toetsen aan de vrijheid van meningsuiting. De strafbepaling is immers nauw verbonden met het democratische verkiezingsproces en stelt in deze extensieve lezing uitingen gerelateerd aan dit proces strafbaar. Nu het doel is om een eerlijke en vrije verkiezingen te waarborgen moet men voorzicht te werk gaan bij het inperken van de vrijheid van meningsuiting om niet het doel voorbij te schieten. Uit het voorgaande volgt dat “bewuste onlinemanipulatie” voor een groot deel al onder artikel 127 Sr valt. Of dit daadwerkelijk het geval is hangt, samengevat, af van de volgende punten:

- **Definitie “bewuste onlinemanipulatie”:** wanneer het begrepen wordt als een opzettelijke bedrieglijke handeling via een internetdienst waardoor een stem van onwaarde wordt of een kiezer in werkelijkheid op een andere kandidaat heeft gestemd dan hij denkt, dan valt het onder artikel 127 Sr. Enig breder begrip van “onlinemanipulatie” wordt niet door artikel 127 Sr gedekt en kan vanuit een fundamenteelrechtelijk perspectief niet zonder meer onder de delictsomschrijving gebracht worden.
- **Uitleg reikwijdte artikel 127 Sr:** Naar alle waarschijnlijkheid is de uitleg van het causaal verband zonder de causa proxima onproblematisch, maar hier is door de wetgever of in de jurisprudentie geen definitief uitsluitend over gegeven.
- **Impact op de vrijheid van meningsuiting:** een extensieve uitleg van het causaal verband vereist in artikel 127 Sr is in principe verenigbaar met de vrijheid van meningsuiting, hoewel de ruimte die er is voor interpretatie ook inhoudt dat de fundamenteelrechtelijke grenzen doorlopend in gedachte gehouden moeten worden.

ii. Desinformatie & Computervredebreuk

Een ander leerstuk uit het strafrecht dat interessant is voor de problematiek rond desinformatie is computervredebreuk, of het “hackverbod”. Computervredebreuk is strafbaar gesteld in artikel 138ab Sr. Het artikel is meerdere malen gewijzigd naar aanleiding van onder andere het Cybercrimeverdrag van de

⁴⁰² EHRM Lingens vs. Oostenrijk, 8 juli 1986 (nr. 9815/82).

⁴⁰³ EHRM Salov vs Ukraine 6 september 2005. (nr. 65518/01).

Raad van Europa⁴⁰⁴ en de EU Richtlijn 2013/40/EU. In de kern bestaat computervrederebreuk uit het opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk of in een deel daarvan. Dit “binnendringen” is een open begrip dat niet-limitatief wordt ingevuld in het eerste lid van artikel 138ab Sr met (a) het doorbreken van een beveiliging, (b) een technische ingreep, (c) door middel van valse signalen of een valse sleutel of, (d) door het aannemen van een valse hoedanigheid. Er is ruimte gegeven aan de rechtspraak om dit begrip binnendringen aan te passen aan de snel veranderende realiteit.⁴⁰⁵ Zo is recentelijk door de Hoge Raad geoordeeld dat “De enkele omstandigheid dat verdachte (...) m.b.v. een scan-programma de website van aangever op kwetsbaarheden heeft onderzocht” onvoldoende is om van binnendringen te spreken.⁴⁰⁶

Het bestanddeel “geautomatiseerd werk” moet breed geïnterpreteerd worden en omvat naast computers ook netwerken, telefoon en fax en sociale media-accounts. Een systeem kwalificeert zo lang het in staat is om (i) gegevens op te slaan, (ii) te verwerken en (iii) over te dragen.⁴⁰⁷ In de rechtspraak is uitgemaakt dat ook het binnendringen van een deel van een geautomatiseerd werk computervrederebreuk vormt.⁴⁰⁸ Voorbeelden zijn een situatie waarin iemand wel geautoriseerd is voor toegang tot bepaalde gegevens maar zichzelf toegang verschaft tot andere gegevens of ook de mogelijkheid creëert deze te wijzigen,⁴⁰⁹ of het binnendringen van een router als onderdeel van een netwerk.⁴¹⁰

Het tweede lid van artikel 138ab Sr beschermt de integriteit van gegevensverwerking in een geautomatiseerd werk.⁴¹¹ Het artikel luidt als volgt: “Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervrederebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.” Noodzakelijk is dat de gegevens op duurzame wijze zijn vastgelegd.⁴¹² Waar gegevens worden vernietigd, en niet slechts overgenomen is artikel 350a Sr van toepassing.⁴¹³ Afsluitend voorziet het derde lid in strafverzwaring voor de situatie waarin via een openbaar telecommunicatienetwerk gebruik wordt gemaakt van verwerkingscapaciteit van een geautomatiseerd werk, of toegang tot een geautomatiseerd werk van een derde wordt verschaft.⁴¹⁴

Er zijn een aantal raakvlakken tussen het leerstuk computervrederebreuk en de problematiek rond desinformatie of “onlinemanipulatie”. In de eerste plaats kan gedacht worden aan het scenario dat een geautomatiseerd werk, en dan voornamelijk een elektronische communicatiedienst, binnengedrongen wordt om vervolgens via dat systeem op grote schaal desinformatie te verspreiden. Een voorbeeld is de KPN hack uit 2012 waarbij toegang verkregen werd tot klantgegevens zoals NAW-gegevens, telefoonnummers en bankrekeningnummers. Denkbaar is dat bij een dergelijke hack niet alleen toegang verkregen wordt tot klantgegevens, maar dat ook desinformatie verspreid kan worden via deze netwerken. Een gerelateerd voorbeeld is de DigiNotar hack uit 2011 waarbij meer dan 500 valse SSL-certificaten werden uitgegeven en de websites van de Nederlandse overheid tijdelijk als onveilig werden bestempeld. Deze twee voorbeelden kunnen gekwalificeerd worden als computervrederebreuk en zijn als zodanig strafbaar, inclusief

404 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23-11-2001.

405 Kamerstukken II 2004/05, 26 671, nr. 7, p. 33.

406 HR 9 april 2019, ECLI:NL:HR:2019:560.

407 Rb. Midden-Nederland 23 augustus 2016, ECLI:NL:RBMNE:2016:4673; Kamerstukken II, 2004-2005, 26 671, nr. 10, blz. 31; HR 26 maart 2013, ECLI:NL:HR:2013:BY9718.

408 HR 26 maart 2013, ECLI:NL:HR:2013:BY9718.

409 Kamerstukken II, 1990-1991, 21 551, nr. 6, p. 30-32 (MvA)

410 HR 26 maart 2013, ECLI:NL:HR:2013:BY9718.

411 Kamerstukken II, 1991-1992, 21 551, nr. 11, p. 19.

412 Kamerstukken II, 1991-1992, 21 551, nr. 12, p. 4.

413 C.M. Gerritsma-Breur & A.G. Nederlof, Commentaar op Wetboek van Strafrecht art. 138ab (strafrecht) (artikeltekst geldig vanaf 01-07-2015).

414 Idem

de strafverzwaring uit het derde lid van artikel 138ab Sr. De verspreiding van desinformatie door middel van het inbreken in een netwerk is dus al strafrechtelijk genormeerd.

Een ander mogelijk verband tussen de verspreiding van desinformatie via internetdiensten en het leerstuk van de computervredebreuk is het gebruik van “bots” of nep-accounts. Hierbij worden geautomatiseerd berichten geplaatst, gedeeld of “geliked” op sociale media via nep-accounts om bepaalde, vaak politieke, informatie te helpen verspreiden.⁴¹⁵ De vraag is in hoeverre hier sprake is van het “binnendringen” van een “geautomatiseerd werk”. Artikel 138ab(1)d Sr stelt expliciet dat “het aannemen van een valse hoedanigheid” gezien moet worden als “binnendringen”. Daarentegen is intuïtief niet onmiddellijk helder of het aanmaken van een valse account en het geautomatiseerd verspreiden van berichten gekwalificeerd moet worden als het “binnendringen” van een geautomatiseerd werk nu het eerder gezien wordt als het gebruik of zelfs misbruik maken van een dienst. Wel heeft de Hoge Raad in 2013 bevestigd dat een account op een sociale media platform gezien moet worden als een geautomatiseerd werk,⁴¹⁶ ook blijkt duidelijk uit de jurisprudentie dat het zonder toestemming gebruik maken van iemand anders account valt onder binnendringen.⁴¹⁷

In de kern ziet de problematiek van nep-accounts op het bestanddeel “opzettelijk en wederrechtelijk”. Wanneer immers slechts gebruik wordt gemaakt van een dienst wordt niet wederrechtelijk binnendringen, terwijl ongeautoriseerd gebruik van de diensten van een platform wel gezien kan worden als wederrechtelijke binnendringing. In geval van het gebruik van bots en nep-accounts staat de vraag naar de wederrechtelijkheid dus ook in direct verband tot de voorwaarden waaronder de sociale media hun dienst aanbieden. Deze gebruiksvoorwaarden zijn des te belangrijk nu er geen andere vorm van “beveiliging” is op de toegang tot de dienst, en het de enige voor de gebruiker kenbare is bron voor wat rechtmatig gebruik van de dienst inhoudt.⁴¹⁸ Deze lezing betekent dat een sociale mediadienst een “geautomatiseerd werk” is, en het gebruik maken van deze dienst in strijd met de gebruiksvoorwaarden “wederrechtelijk binnendringen” vormt.

De vraag is in hoeverre daadwerkelijk zo veel gewicht moet toekomen aan de gebruiksvoorwaarden van een internetdienst. Deze lezing van de wet zou immers verregaande gevolgen hebben en is nog niet in de jurisprudentie besproken. De lezing zou namelijk betekenen dat in veel gevallen de grens van de privaatrechtelijke binding van de eenzijdig opgelegde gebruiksvoorwaarde samenvalt met de strafrechtelijke normen voor computervredebreuk. Nu deze gebruiksvoorwaarden eenzijdig door de internetdiensten opgelegd worden en ieder moment wederom eenzijdig aangepast zouden kunnen worden, vormen deze een zeer subjectieve basis voor een strafbaarstelling. Dit, gecombineerd met het feit dat veel van de betrokken internetdiensten communicatie- en/of mediadiensten zijn waar mensen afhankelijk van zijn voor het onderhouden van hun sociale relaties en deelname aan het democratisch debat, pleit voor het hanteren van een objectievere standaard voor “binnendringen” dan alleen de gebruiksvoorwaarden. Wellicht dat het uit het consumentenrecht afkomstige begrip van “normaal gebruik” als basis kan dienen.⁴¹⁹

Mogelijk dat nog voor verder onderzoek lering getrokken kan worden bij de Amerikaanse “Computer Fraud and Abuse Act” (“CFAA”) waar zowel strafrechtelijke en privaatrechtelijke normen ontwikkeld zijn met een vergelijkbaar brede reikwijdte.⁴²⁰ Recentelijk is bijvoorbeeld door de 9th Circuit Court of Appeals

415 Zie bijvoorbeeld Howard, Philip N., Gillian Bolsover, Bence Kollanyi, Samantha Bradshaw, and Lisa-Maria Neudert (2017) ‘*Junk news and bots during the U.S. election: What were Michigan voters sharing over Twitter?*’ Computational Propaganda Data Memo, Oxford: Oxford Internet Institute.

416 HR 26 maart 2013, ECLI:NL:HR:2013:BY9718

417 Rb Midden-Nederland, 18 februari 2019, ECLI:NL:RBMNE:2019:609.

418 Eerste Kamer, vergaderjaar 2005–2006, 26 671 en 30 036 (R 1784), D.

419 Zie artikel 7:23 BW.

420 18 U.S.C.A. § 1030(a) (West 2008); Puckett, David A. (2011) “Terms of Service and the Computer Fraud and Abuse Act: A Trap for the Unwary?”, *Oklahoma Journal of Law and Technology*: Vol. 7 : No. 1 , Article 2. Available at: <http://digitalcommons.law.ou.edu>

uitgemaakt dat het in strijd met de voorwaarden gebruikmaken van informatie die openbaar toegankelijk op een internetplatform (in casu LinkedIn) geen “hacking” vormt in de zin van de CFAA, dit ondanks een uitdrukkelijk verbod van LinkedIn.⁴²¹ Een andere zaak, aangespannen door onderzoekers van algoritmische processen is nog aanhangig.⁴²²

iii. Desinformatie & verspreidingsdelicten

Een laatste categorie strafrechtelijke normen relevant voor de verspreiding van desinformatie via internetdiensten zijn de zogenaamde verspreidingsdelicten. Dit is een categorie strafbepalingen die de culpoze varianten vormen van een gronddelict, een uitingsdelict of specifiek een drukpersdelict, waar wel schuld voor vereist is.⁴²³ Dit houdt in dat dit type strafbepalingen niet gericht is op degene die moedwillig het strafbare feit pleegt (zoals bijvoorbeeld het doen van discriminerende of haat zaaiende uitingen, of het maken van afbeeldingen van seksueel misbruik van minderjarigen), maar gericht is op degene die deze informatie verder in het openbaar verspreid en “redelijkerwijs kon vermoeden” dat de informatie strafbaar is. Deze persoon heeft dus zelf geen opzet tot of schuld aan het oorspronkelijke misdrijf, maar is wel verantwoordelijk voor de verdere verspreiding. Concreet betreft het, binnen het Wetboek van Strafrecht, de strafbaarstelling van de volgende type uitingen: majesteitsschennis (artikel 113 Sr), opruiing (artikel 119 Sr), groepsbelediging, discriminatie en aanzetten tot haat (artikel 137e Sr), afbeelding van seksueel misbruik van minderjarigen (artikel 240b Sr) en smaadsmaad, laster en belediging van bijzondere organen en functionarissen (artikel 271 Sr). Artikel 134 Sr bevat ook een verspreidingsdelict, maar wijkt af van de voorgaande artikelen nu er geen specifiek gronddelict is. Strafbaar wordt namelijk gesteld de verspreiding van informatie “waarin wordt aangeboden inlichtingen, gelegenheid of middelen te verschaffen om enig strafbaar feit te plegen.” Uit de parlementaire geschiedenis blijkt dat de ratio achter deze delicten is dat, een drukpersmisdrijf voltooid is op het moment dat het gepubliceerd of geopenbaard wordt en dat verdere verspreiding daarom een *nieuw* misdrijf is.⁴²⁴

Voornamelijk relevant is artikel 137e Sr, het verspreidingsdelict dat de verspreiding van haatzaaiende, discriminerende of groepsbeledigende uitingen strafbaar stelt. In 2017 heeft de Hoge Raad in een gevolrijk arrest geoordeeld dat in die zaak de strafbepaling buiten toepassing gelaten moest worden wegens strijd met artikel 10 EVRM.⁴²⁵ Het betrof een antiquariaat dat antieke exemplaren van “Mein Kampf” van Hitler in zijn inventaris had. De Hoge Raad benadrukte dat ook dergelijke verspreidingsdelicten aan de vrijheid van meningsuiting in artikel 10 EVRM getoetst moet worden, en dat daarbij de context van de concrete verspreiding zeer van belang is: “Bij de beoordeling van deze noodzaak om in te grijpen in de vrijheid van meningsuiting zijn de bijzondere omstandigheden van het geval van belang. Bij die beoordeling kan gewicht worden toegekend aan de wisselwerking tussen de aard van de uitlating of informatie en het mogelijke effect dat die uitlating of informatie sorteert alsmede aan de context waarbinnen zo een uitlating is gedaan of informatie is verstrekt.”⁴²⁶

Deze strafbepalingen zijn zeer nauw gerelateerd aan de problematiek rond desinformatie die centraal staat in dit onderzoek nu de focus ligt op de verspreiding van strafbare uitingen. Deze strafrechtelijke normen zouden dus een aanknopingspunt kunnen vormen voor regulering van de verspreiding van illegale uitingen via internetdiensten. Het probleem is echter dat de *safe harbour* uit de Richtlijn elektronische handel een horizontale (voorwaardelijke) aansprakelijkheidsuitsluiting biedt waardoor vele internetdiensten ook gevrijwaard zijn van deze strafrechtelijke normen. Dit is natuurlijk slechts het geval voor zover deze dienst binnen de *safe harbour* valt en geen kennis hebben van het illegale karakter van de

/okjolt/vol7/iss1/2

421 United States Court of Appeals for the Ninth Circuit, 9 september 2019, no. 17-16783 (*HIQ Labs vs. LinkedIn*).

422 <https://casetext.com/case/sandvig-v-sessions>

423 Verkade, Tekst & Commentaar Intellectuele eigendom, Verspreidingsdelict, in voorraad hebben; culpoze variant bij: Auteurswet, Artikel 32.

424 Smidt II p. 46-47 & p. 401.

425 HR 14 februari 2017, ECLI:NL:HR:2017:220

426 *ibid.* Ro. 3.5 onder verwijzing naar EHRM 15 oktober 2015, ECLI:CE:ECHR:2015:1015JUD002751008 (*Perincek/Zwitserland*).

informatie, of “prompt handelt om de informatie te verwijderen”. Wel is voor de verdere reguleringsdiscussie van belang dat het Nederlandse strafrecht deze leerstukken kent waarbij een gronddelict, een uitingsdelict, verder wordt aangevuld met een verspreidingsdelict.

C. Bestuursrechtelijke normen

Een groot aantal bestuursrechtelijke normen zijn relevant voor de verspreiding van desinformatie via internetdiensten. De belangrijkste hiervan zullen hier besproken worden. In de eerste plaats reclameregulering wegens de aan desinformatie gerelateerde problematiek rond politieke advertenties en in het kader van de commerciële belangen verbonden aan desinformatie. Ook de regulering van de financiering van politieke partijen wordt besproken in het kader van aan desinformatie rakende politieke advertenties. Vervolgens wordt de verspreiding van desinformatie ook gerelateerd aan de staatsveiligheid en de bescherming van kritische infrastructuur.

i. Regulering van advertenties

De problematiek van desinformatie is op verschillende manieren gerelateerd aan de regulering van advertenties. In meer algemene zin zijn de bedrijfsmodellen van veel internetdiensten afhankelijk van de inkomsten gegenereerd uit advertenties,⁴²⁷ wat maakt dat deze diensten zo ingericht worden om de aandacht van gebruikers zo lang mogelijk vast te houden om deze reclame-inkomsten te optimaliseren. Dit kan als gevolg hebben dat de dienst sensationele, opspraak makende of “click-bait”-content prefereert en zo dezelfde logica als desinformatie hanteert.⁴²⁸ Vervolgens is desinformatie meer specifiek ook gerelateerd aan reclame via misleidende en schadelijke politieke advertenties. Zoals aangegeven staat in het debat over desinformatie de regulering van politieke advertenties als mogelijke strategie om de grotere problematiek aan te pakken momenteel hoog op de (internationale) politieke agenda.

Bij de bespreking van wetgeving met als onderwerp advertenties moet een onderscheid gemaakt worden tussen (i) de bepalingen die specifiek zien op politieke advertenties, (ii) de bepalingen die zowel op politieke als commerciële advertenties zien en (iii) bepalingen die louter van toepassing zijn op commerciële advertenties. Deze laatste categorie, hoewel niet van toepassing, wordt toch besproken omdat deze bepalingen als voorbeeld en context kunnen dienen voor de mogelijke regulering van politieke advertenties. Commerciële advertenties zijn op Europees niveau gereguleerd, zoals in hoofdstuk 5 al duidelijk naar voren komen. De REH, AVMS-richtlijn, de richtlijn oneerlijke handelspraktijken en de richtlijnen misleidende reclames bevatten allen normen over commerciële advertenties, veel hiervan transparantieverplichtingen. De regulering van politieke advertenties zijn daarentegen gezien de gevoelige en nationale aard van het politieke proces overgelaten aan de nationale wetgevers.

Politieke advertenties als zodanig worden in Nederland niet specifiek gereguleerd.⁴²⁹ Dit is historisch deels te verklaren vanuit het lang heersende idee dat de overheid zich afzijdig dient te houden van het maatschappelijke politieke proces, zo ook de structuur en de campagnes van politieke partijen.⁴³⁰ De Mediawet is de enige wettelijke bron die specifiek spreekt over politieke advertenties. Afdeling 6.1.1. van deze wet stelt vast dat gevestigde politieke partijen (die in een voorgaande verkiezing een zetel hebben verworven) kosteloos zendtijd toegekend krijgen. Deze zendtijd wordt door het Commissariaat voor de Media beschikbaar gesteld op de landelijke publieke mediadiensten voorafgaand aan een verkiezing

⁴²⁷ Zie hoofdstuk 3.

⁴²⁸ Bayer, J. e.a., *‘Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States’*, European Union, 2019, p. 31, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

⁴²⁹ Cappello, M. (ed.), *‘Media coverage of elections: the legal framework in Europe’*, IRIS Special, European Audiovisual Observatory, Strasbourg, 2017, p. 83; Vliegthart, R., & Kruikemeier, S. *‘Political Advertising in the Netherlands: (Still) Little Ado About (Almost) Nothing’* In: Holz-Bacha, C., & Just, M.R. (ed.) *‘Routledge Handbook of Political Advertising’*, New York: Routledge, 2017, p. 370.

⁴³⁰ Evaluatie- en adviescommissie Wet Financiering politieke partijen, *‘Het publieke belang van politieke partijen’*, 2018, p. 18-19.

en is voor alle gevestigde partijen gelijk.⁴³¹ Inhoudelijk moet deze zendtijd gewijd worden aan politieke programma's.⁴³² De parlementaire geschiedenis benadrukt nog dat het niet gebruikt mag worden voor handelsreclame.⁴³³ Zuiver gezien betreft deze regeling in de Mediawet geen regulering van politieke advertenties, het raakt immers niet aan de productie, inhoud of verdere verspreiding van de betreffende politieke communicatie. Daarentegen bevordert de beschikbaarstelling van de gratis zendtijd wel de zichtbaarheid van politieke partijen en draagt deze bij aan een gelijk speelveld. De invloed van deze regeling moet echter niet overschat worden nu de politieke uitzendingen doorgaans een vrij beperkt bereik hebben.⁴³⁴

Vervolgens kent de Mediawet ook een verbod op de sponsoring⁴³⁵ van media-aanbod dat bestaat uit "politieke informatie".⁴³⁶ Dit begrip wordt breed uitgelegd en omvat zowel programma's als advertenties. Wat betreft de publieke omroep was de ratio dat sponsoring in het algemeen niet passend is gezien de publieke taak van de omroep.⁴³⁷ Daarnaast is de achterliggende gedachte meer in het algemeen het voorkomen van vermenging van politieke en commerciële invloeden en het garanderen van transparantie. Oorspronkelijk vormde het verbod de implementatie van artikel 17 lid 3 van Richtlijn 89/552/EEG,⁴³⁸ hoewel de richtlijn het verbod niet motiveerde. Wat betreft het toezicht is het Commissariaat voor de Media belast met de handhaving van het sponsorverbod.⁴³⁹ Los van het verbod op sponsoring staat de Mediawet er niet aan in de weg dat politieke partijen zelf commerciële zendtijd kopen. Maar wegens de hoge kosten die hieraan verbonden zijn, de relatief kleine budgetten en de toch beperkte kijkcijfers doen partijen dit nauwelijks.⁴⁴⁰ Afsluitend moet in algemene zin opgemerkt worden dat hoewel online politieke advertenties dus niet onder een specifieke wettelijke regeling vallen, de civiele rechter als restrechter te allen tijde bevoegd is. De figuur van de onrechtmatige daad is dusdanig algemeen dat deze altijd als rechtsgrond opgeworpen kan worden en via de civiele rechter het gebruik of de inhoud van online politieke advertenties kan normeren.⁴⁴¹

Naast de besproken specifieke bepalingen van de Mediawet die politieke advertenties als onderwerp hebben, reguleert de Mediawet ook commerciële advertenties op de omroepen. Titel 2.5 en 3.2 Mediawet bevatten een uitgebreide regeling waar wordt vastgesteld hoe vaak, hoe lang en wat voor type reclame toegestaan is.⁴⁴² Net zoals de Richtlijn elektronische handel geven artikel 2.88b en 3.5b Mediawet een transparantie en informatieverplichting voor reclames verspreid via de omroepen. Het Commissariaat voor de Media is belast met het toezicht.⁴⁴³

Vervolgens kent Nederland wat betreft de algemene reclameregulering van toepassing op zowel commerciële als politieke advertenties verschillende reclameverboden, vaak opgenomen in specifieke sectorwetgeving. Deze verboden gelden ongeacht het gebruikte medium. Een goed voorbeeld is het verbod op tabaksreclame zoals opgenomen in artikel 5 lid 1 Tabakswet of het verbod op reclame voor op recept verkrijgbare geneesmiddelen uit artikel 85 Geneesmiddelenwet. Aangezien het algemene verboden zijn,

431 Artikel 6.1 Mediawet.; Tweede Kamer, vergaderjaar 2007–2008, 31 356, nr. 3, p. 73-74.

432 Artikel 6.4 Mediawet.

433 Tweede Kamer, vergaderjaar 2007–2008, 31 356, nr. 3, p. 73-74. Zie de definitie van reclame in artikel 1 lid 1 Mediawet.

434 Aalberts, J., *'Het mysterieuze voortbestaan van de zendtijd politieke partijen'*, Tijdschrift voor Mediageschiedenis, 16(2), p. 43.

435 Sponsoring wordt in artikel 1 gedefinieerd als: "het verstrekken van financiële of andere bijdragen door een onderneming of een natuurlijke persoon die zich gewoonlijk niet bezighoudt met de verzorging van mediadiensten of media-aanbod, ten behoeve van de totstandkoming of aankoop van media-aanbod, teneinde de verspreiding daarvan naar het algemene publiek of een deel daarvan te bevorderen of mogelijk te maken".

436 Artikel 2.106 lid 3 sub a jo. 3.15 lid 2 Mediawet.

437 Tweede Kamer, vergaderjaar 1993-1994, 23 752, nr. 3, p. 4.

438 Tweede Kamer, vergaderjaar 1993-1994, 23 752, nr 3, p. 6. Richtlijn 89/552/EEG is vervangen door Richtlijn 2010/13/EU die dit verbod op sponsoring van politieke programma's niet kent.

439 Artikel 7.11 Mediawet.

440 Vliegenthart, R., & Kruikemeier, S. *'Political Advertising in the Netherlands: (Still) Little Ado About (Almost) Nothing'* in: Holz-Bacha, C., & Just, M.R. (ed.) *'Routledge Handbook of Political Advertising'*, New York: Routledge, 2017, p. 371-2.

441 Zie hierover verder paragraaf 6.B.

442 Zie bijvoorbeeld 3.8 en 3.11 Mediawet voor de duur en frequentie van de reclame en 3.10 Mediawet voor de inhoud.

443 Artikel 7.11 Mediawet.

is dit type regulering van toepassing op zowel commerciële als politieke advertenties.

ii. Financiering politieke partijen

Vanuit de gedachte dat de overheid zich afzijdig moet houden van politieke partijen kent Nederland, zoals eerder aangegeven, van oudsher weinig op politieke partijen gerichte regulering.⁴⁴⁴ De enige echte uitzondering op deze regel is de Wet financiering politieke partijen. Deze wet stelt de criteria voor subsidieverstrekking en bevat financiële transparantieverplichtingen. Toezicht wordt uitgeoefend door het ministerie van Binnenlandse zaken en Koninkrijksrelaties. De Commissie toezicht financiën politieke partijen heeft een adviserende rol. Niet-naleving van de financiële transparantieverplichting kan leiden tot een bestuurlijke boete.⁴⁴⁵

Met dit relatieve gebrek aan regulering is Nederland in een internationale context vrij uitzonderlijk. Invloedrijke organisaties zoals de OSCE⁴⁴⁶ en de GRECO⁴⁴⁷ hebben meerdere malen aangegeven dat de regulering van partijfinanciering in Nederland tekortschiet vanuit het perspectief van corruptiebestrijding. Het voornaamste punt van verbetering betreft volgens deze organisaties de transparantie van partijfinanciering en uitgaven.

De implementatie van dergelijke transparantieverplichtingen kan zeer relevant zijn voor de regulering van online politieke advertenties. Financiële transparantieverplichtingen kunnen mogelijk ingezet worden om helderheid te verkrijgen over, en invloed uit te oefenen op de wijze waarop politieke partijen campagne voeren. De huidige Nederlandse regulering is alleen te algemeen van aard om dit doel te bereiken. De regeling vereist namelijk slechts transparantie van inkomsten en schulden, en niet van uitgaven.⁴⁴⁸

De bestaande financiële transparantieverplichtingen uit de Wet financiering politieke partijen betreffen hoofdzakelijk de politieke partijen zelf.⁴⁴⁹ Deze zijn verplicht al hun inkomsten en schulden te registreren, waar bij elke gift van boven de 1000 euro de gegevens van de gever vastgelegd moeten worden. Alle anoniem ontvangen giften die de 1000 euro overstijgen moeten voor die meerwaarde aan het ministerie worden overgedragen.⁴⁵⁰ De partijen zijn vervolgens verplicht jaarlijks een overzicht van hun administratie aan het ministerie te overhandigen, dat vervolgens gepubliceerd wordt in de Staatscourant.⁴⁵¹ Dit overzicht bevat slechts gegevens met betrekking tot giften van boven de 4500 en schulden boven de 25.000 euro. Ook moet een overzicht van de administratie tussen drie en twee weken voor iedere verkiezingen bij het ministerie ingeleverd worden zodat het ministerie het voor de stemming kan publiceren. Ook als een individuele kandidaat giften van in totaal groter dan 4500 euro heeft ontvangen ten bate van zijn politieke activiteiten moet dat aan de minister kenbaar gemaakt worden, zodat die het kan publiceren.⁴⁵²

Het afgelopen jaar liep er in Nederland een discussie over het verbieden van giften afkomstig uit het buitenland.⁴⁵³ In 2016 is een motie van die strekking met grote meerderheid door de Tweede Kamer

444 Evaluatie- en adviescommissie Wet financiering politieke partijen, *'Het Publieke belang van politieke partijen'* 2018, p. 18-19. Bijlage bij: Tweede Kamer, vergaderjaar 2017-2018, 32 752, nr. 50.

445 Artikel 35-37 Wet financieel toezicht politieke partijen.

446 OSCE/ODIHR Election Assessment Mission Final Report *'The Netherlands Parliamentary elections 15 March 2017'* 2017, <https://www.osce.org/odihr/elections/netherlands/321821?download=true>.

447 GRECO, *'Third Evaluation Round. Second Compliance Report on the Netherlands. Transparency of Party Funding'* 2012.

448 Artikel 20-23 Wet financiering politieke partijen.

449 De afdelingen van politieke partijen zijn uitgesloten van de transparantieverplichting (artikel 24). De verplichting is verminderd van toepassing op neveninstellingen waaronder ook jongerenorganisaties en wetenschappelijke instituten (artikel 30).

450 Artikel 20-23 Wet financiering politieke partijen.

451 Artikel 15 Wet financiering politieke partijen.

452 Artikel 28-29 Wet financiering politieke partijen.

453 Sommige landen beperken de financiering uit het buitenland voor het organiseren van verkiezingen. Zie onderstaand landenrapport over Canada, dat bepaalde buitenlandse financiering tijdens verkiezingen beperkt (Elections Modernization Act 2018, section 232.4(1) - Undue influence by foreigners).

aangenomen,⁴⁵⁴ en ook de commissie belast met de evaluatie van de Wet financiering politieke partijen adviseerde tot het verbod.⁴⁵⁵ De regering heeft inmiddels duidelijk aangegeven het verbod op buitenlandse giften te willen implementeren, en is voornemens het op te nemen in een nieuwe Wet op de Politieke Partijen en al eerder in een wijziging van de Wet financiering politieke partijen.⁴⁵⁶ Het idee is dat giften uit niet EU-landen verboden worden en giften uit andere EU-landen openbaar gemaakt moeten worden.⁴⁵⁷

Hoewel financiële transparantieplichtingen voor politieke partijen gezien kunnen worden als een mogelijkheid om grip te krijgen op het gebruik van digitale advertenties door politieke partijen, is de huidige regulering daar niet op ingesteld. Voor dit doel is transparantie over campagne-uitgaven van belang en dit aspect ontbreekt in de Nederlandse wetgeving. Mogelijk wordt een dergelijke transparantieplichting die ziet op de uitgaven samen met het verbod op buitenlandse giften wel onderdeel van de voorgenomen Wet op de Politieke Partijen.⁴⁵⁸ Daarnaast is ook relevant dat politieke partijen in Nederland over relatief zeer kleine budgetten beschikken. Dit heeft partijen bijvoorbeeld veelal belet om commerciële zendtijd op de omroepen te kopen of om op grotere schaal online campagnes op te zetten.⁴⁵⁹

iii. Nationale veiligheid

In voorkomende gevallen is desinformatie, alsmede de problematiek van oneigenlijke invloed op het Nederlandse democratisch proces middels politieke advertenties, gelinkt aan bedreigingen van de nationale veiligheid. Dit is geen nieuw fenomeen, maar altijd een factor geweest bij informatievoorziening als zodanig. Het gaat om een veelheid aan aspecten. Het kan gaan om destabilisatie van de democratie in algemene zin of om het beïnvloeden van verkiezingen en promotie van en aanzetten tot terrorisme of extremisme in het bijzonder. In de beleidsvorming staat desinformatie via buitenlandse inmenging centraal. Bij alle maatregelen op dit terrein geldt dat deze in overeenstemming moeten zijn met de vereisten van Artikel 10 EVRM.

Recentelijk, in maart 2018, is door de ministers van BZK en V&J aan de Tweede Kamer bericht over wat onder ongewenste buitenlandse inmenging wordt verstaan en op welke wijze hiermee zal worden omgegaan.⁴⁶⁰ Zo wordt, onder verwijzing naar het jaarverslag 2017 van de AIVD, als voorbeeld genoemd de heimelijke politieke beïnvloeding door Rusland, waarbij gebruik gemaakt van kwetsbaarheden van open en democratische samenlevingen. Ook in het jaarverslag van 2018 waarschuwt de AIVD opnieuw voor mogelijke ongewenste buitenlandse inmenging door middel van "heimelijke politieke beïnvloeding".⁴⁶¹ De AIVD betreft hierbij ook beïnvloeding via sociale media.⁴⁶²

Niet alle ongewenste inmenging - het bredere onderwerp van de brief - betreft desinformatie. Waar het wel gaat om desinformatie, wordt door de regering het standpunt ingenomen dat verspreiding door statelijke actoren van online desinformatie moet worden tegengegaan. Gesteld wordt: "Hierbij zijn de inspanningen van het kabinet primair gericht op drie punten: 1) vergroten van het inzicht in de omvang en aard van de dreiging, 2) verhogen van de bewustwording en 3) intensivering van de samenwerking tussen de verschillende partijen die hierin een rol kunnen spelen." Het kabinet benadrukt verder dat bij

454 Motie Amhaouch c.s., Tweede Kamer, vergaderjaar 2016-2017, 34 270, nr. 22.

455 Evaluatie- en adviescommissie Wet financiering politieke partijen, *'Het Publieke belang van politieke partijen'* 2018. Bijlage bij: Tweede Kamer, vergaderjaar 2017-2018, 32 752, nr. 50.

456 Handelingen II, vergaderjaar 2018-2019, Aanhangsel van de Handelingen, nr. 875; Tweede Kamer, vergaderjaar 2017-2018, 32 752, nr. 50; Regeerakkoord 2017-2021, *'Vertrouwen in de Toekomst'*, p. 4, Kamerstuk 34 700, nr. 34; Een wetsvoorstel ter aanpassing van de wet financiering politieke partijen ligt momenteel voor in internetconsultatie, zie: <https://www.internetconsultatie.nl/wijzigingwfpp>.

457 Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, Tweede Kamer, vergaderjaar 2018-2019, 32 752, nr. 54.

458 Zie verder paragraaf 6.C.

459 Vliegenthart, R., & Kruikemeier, S. *'Political Advertising in the Netherlands: (Still) Little Ado About (Almost) Nothing'* In: Holz-Bacha, C., & Just, M.R. (ed.) *'Routledge Handbook of Political Advertising'*, New York: Routledge, 2017, p. 371-2.

460 Kamerstukken II, 2018/19, nr. 30821, nr. 42.

461 AIVD jaarverslag 2018, p. 9 e.v.

462 Idem p. 10.

het zoeken naar oplossingen “de journalistieke onafhankelijkheid gewaarborgd en gerespecteerd blijven (...)”.⁴⁶³ Het vergroten van de weerbaarheid wordt nader in de brief uitgewerkt, terwijl tevens de EU-ontwikkelingen inzake desinformatie worden genoemd. Gesproken wordt verder over de inzet van diplomatieke instrumenten, zoals het vroegtijdig signaleren en bespreekbaar maken van ongewenste inmenging via diplomatieke kanalen, maar ook het publieke aanspreken van een land wordt genoemd. Het heeft de voorkeur van de regering om hierbij met andere landen op te trekken.

Verdere invulling en aanscherping is te vinden in een brief aan de Kamer van december 2018, waarin het kabinet onder andere aangeeft dat de dreiging van desinformatie door statelijke actoren als reëel wordt beschouwd.⁴⁶⁴ Daarnaast worden nog zes andere uitgangspunten gehanteerd waaronder het vooropstaan van rechtstatelijke waarden en grondrechten, alsook wordt er –vooral nog– vertrouwen uitgesproken ten aanzien van “de eigen verantwoordelijkheid van tech bedrijven in de vorm van zelfregulering, met in achtneming van de vrijheid van meningsuiting en persvrijheid.” In hoeverre die andere uitgangspunten zich verhouden tot desinformatie door statelijke actoren blijft in de brief onbesproken. Wel wordt de dreiging van statelijke actoren nog nader geduid door deze uit te breiden tot “actoren die aan statelijke actoren zijn te relateren”. Hier wordt waarschijnlijk bedoeld op onder meer “trol-fabrieken” waarvan wordt aangenomen dat deze in opdracht van een buitenlandse statelijke actor opereren of door een statelijke actor worden gedoogd.⁴⁶⁵

Statale dreigingen worden opnieuw besproken in een Kamerbrief van april 2019.⁴⁶⁶ Opnieuw wordt de verspreiding van desinformatie genoemd als een van de tactieken bij ongewenste buitenlandse inmenging. De aanpak van statale dreigingen wordt nader gedetailleerd en de eerdere inzet op bewustwording ten aanzien van desinformatie wordt bevestigd. In de bijlage wordt aangegeven dat een reactie van de overheid gegrond is wanneer sprake is van “een bedreiging van de economische of politieke stabiliteit of nationale veiligheid door inmenging van statale of daaraan gelieerde actoren.”

In de nationale veiligheidsstrategie 2019,⁴⁶⁷ tot stand gekomen onder de regie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)⁴⁶⁸ wordt desinformatie als een van de statale bedreigingen gezien die moet worden aangepakt. Daarbij wordt de verspreiding van onjuiste informatie rondom verkiezingen, via onder meer sociale media als voorbeeld genoemd. Onder statale dreigingen wordt in dit verband – in lijn met eerdere stukken - primair ongewenste buitenlandse inmenging verstaan. Dergelijke ongewenste inmenging zou ook van nationale aard kunnen zijn, maar lijkt niet dusdanig te zijn dat dit aanleiding was tot prioriteitstelling binnen de nationale veiligheidsstrategie.

In de informatie vanuit de overheid naar de Tweede Kamer wordt niet gesproken over het tekort schieten van instrumenten of de noodzaak tot nadere regelgeving waar het betreft desinformatie afkomstig van of afgedekt door buitenlandse statale actoren. De aanname zou derhalve kunnen zijn dat het bestaande instrumentarium afdoende is, dan wel dat een en ander mee wordt genomen bij andere nieuw te vormen beleid op nationaal en Europees niveau. Op dit laatste lijken de aangehaalde Kamerstukken te duiden, met name wanneer – zie hiervoor – wordt verwezen naar het vroegtijdig signaleren en bespreekbaar maken van ongewenste inmenging via diplomatieke kanalen, maar ook het publieke aanspreken van een land. Het beschreven beleid geeft aan dat desinformatie afkomstig van statale actoren (of daaraan gelieerde partijen) gezien de bedreiging die ervan uitgaat voor de rechtstaat een hoger belang vertegen-

⁴⁶³ Kamerstukken II, 2018/19, nr. 30821, nr. 42.

⁴⁶⁴ Kamerstukken II, 2018/19, nr. 30821, nr. 51.

⁴⁶⁵ Details over het opereren van het zogenoemde Internet Research Agency in Rusland, zijn bekend geworden via het onderzoek van Mieller in de Verenigde Staten. Zie bijvoorbeeld <https://www.justice.gov/file/1035477/download>.

⁴⁶⁶ Kamerstukken II, 2108/19, nr. 30821, nr. 72.

⁴⁶⁷ Kamerstukken II, 2018/19, nr. 30821, nr. 81 (bijlage).

⁴⁶⁸ De NCTV vervult een centrale rol bij de analyse en bestrijding van statale dreigingen. Tot het takenpakket behoren onder meer het analyseren van informatie, beleidsvorming en het realiseren van samenwerking tussen betrokken partijen, zie: <https://www.nctv.nl/organisatie/wieisnctv/index.aspx>.

woordigt dan andere vormen van desinformatie. Dit wordt bevestigd door de moties die in de Tweede Kamer zijn aangenomen over manipulatie/buitenlandse inmenging.⁴⁶⁹

Het aspect van competenties op nationaal niveau, in verhouding tot het Europeesrechtelijk kader, speelt een belangrijke rol voor het zekerstellen van aan nationale veiligheid rakende aspecten. De Europese Unie heeft geen directe bevoegdheden ten aanzien van nationale veiligheid en het is de vraag in hoeverre andere Europese competenties voldoende zijn om bedreigingen van statelijke actoren via desinformatie aan te pakken zonder te raken aan de nationale soevereiniteit. Tenslotte is het van belang dat voldoende transparantie bestaat over de aanpak van desinformatie via internetdiensten door betreffende diensten, gezien de mogelijke beperkingen die hieruit kunnen voortvloeien voor de vrijheid van meningsuiting en het vereiste dat beperkingen bij wet voorzien en noodzakelijk zijn in een democratische samenleving. Relevante bevoegdheden van de diensten in dit kader zijn de bevoegdheden met betrekking tot onder meer sigint (signal intelligence, af luisteren, aftappen, analyse van meta data) en osint (Open-source intelligence, informatievergaring uit openbare media, via onder/bevraging, internet, sociale media), en de uitwisseling van inlichtingen in internationaal verband. Deze bevoegdheden zijn met name terug te vinden in hst 3 en 4 Wet op de Inlichtingen en Veiligheidsdiensten 2017.

iv. Vitale/kritische infrastructuur

In toenemende mate is er aandacht voor vitale/kritische infrastructuur en de zeggenschap daarover. Delen van de informatie-infrastructuur vallen onder de werking van Wet beveiliging netwerk- en informatiesystemen.⁴⁷⁰ Telecommunicatienetwerken en elementen van de digitale infrastructuur vallen onder werking van de wet. Ofschoon de focus in deze wet ligt op het in standhouden van elementaire voorzieningen en het voorkomen van kwetsbaarheden, is er een relatie met desinformatie. Falende communicatie-infrastructuur kan grote consequenties hebben, zoals diverse incidenten hebben uitgewezen. Overigens waren deze incidenten niet gelinkt aan het vraagstuk van desinformatie.

Momenteel ligt bij het parlement het wetsvoorstel “Wet ongewenste zeggenschap telecommunicatie” ter behandeling voor.⁴⁷¹ Het biedt de mogelijkheid om de zeggenschap over telecommunicatiepartijen te beperken waar het betreft de controle over betrokken ondernemingen. Directe aanleiding vormde de mogelijke overname van KPN door een Mexicaanse partij. Openbare orde en nationale veiligheid kan bij dergelijke overnames in het geding komen, zo volgt uit de memorie van toelichting.⁴⁷² Er wordt niet expliciet verwezen naar risico's op het gebied van desinformatie, maar wel wordt aangegeven dat continuïteit en vertrouwelijkheid van communicatie geschaad kunnen worden.

Evenmin direct gerelateerd aan desinformatie kan nog worden gewezen op de discussie over de eigendom van Nederlandse kranten die in belangrijke mate ligt bij Belgische partijen.⁴⁷³ Nederland kent geen bijzondere regels die de eigendom van mediabedrijven beperken of verbieden. Daarbij wordt geen onderscheid gemaakt of controlerende invloed ligt bij ondernemingen uit EU-landen of daarbuiten.

D. Zelfregulering

Aangezien desinformatie als beleidsonderwerp nog vrij nieuw is, kent Nederland geen zelfreguleringsinstrumenten op nationaal niveau die specifiek toegesneden zijn op de problematiek. De zelfreguleringsinitiatieven die zich hebben ontwikkeld bevinden zich voornamelijk op Europees niveau. Daarentegen is er in Nederland wel sterk ontwikkelde zelfregulering met betrekking tot reclame via de Nederlandse

⁴⁶⁹ Kamerstukken II, 30821, nrs. 61, 63 en 68.

⁴⁷⁰ Stb 2018, 387/389.

⁴⁷¹ Kamerstukken II, 35153.

⁴⁷² Kamerstukken II, 35153, nr. 3, p.1/2.

⁴⁷³ Zie o.a.: Aanhangsel handelingen II, 2016/17, nr. 1250.

Reclame Code. Bovendien kent de media een eigen zelfreguleringsorgaan: de Raad voor de Journalistiek, die een rol speelt ten aanzien van desinformatie in de media.

De afwezigheid van wettelijke regulering leidt er toe dat in de Nederlandse context zelfregulering de belangrijkste bron voor specifieke normen voor politieke advertenties vormt.⁴⁷⁴ Ook wat betreft handelsreclame zijn de verschillende zelfreguleringscodes van groot belang. Deze codes bevatten namelijk doorgaans zwaardere normen, en in aanvulling op de wet ook normen die zien op de zedelijkheid of maatschappelijke aanvaardbaarheid van advertenties.⁴⁷⁵

Centraal staat de Stichting Reclame Code die als onafhankelijke organisatie verantwoordelijk is voor de Nederlandse Reclame Code ("NRC").⁴⁷⁶ Deze NRC bestaat uit een algemeen deel, van toepassing op alle vormen van reclame, en in aanvulling daarop 23 verschillende bijzondere reclamecodes die zien op reclame binnen een bepaalde sector.⁴⁷⁷ De code gaat uit van een zeer brede definitie van reclame, waar politieke advertenties ook onder vallen: "iedere openbare en/of systematische directe dan wel indirecte aanprijzing van goederen, diensten en/of denkbeelden door een adverteerder of geheel of deels ten behoeve van deze, al dan niet met behulp van derden."⁴⁷⁸ De NRC kent geen specifieke definitie van "een adverteerder" en uit de tekst van de code zelf kan niet veel meer dan een circulaire definitie worden afgeleid. Zie bijvoorbeeld artikel 19 NRC die een adverteerder duidt als "een organisatie of instelling die reclame maakt".⁴⁷⁹

Een groot aantal belangenorganisaties en beroepsgroepen zijn aangesloten⁴⁸⁰ en nemen zitting in het zogenaamde Platform van Deelnemers dat invloed uitoefent op de vaststelling van de codes.⁴⁸¹ Naast de vrijwillige aansluiting van organisaties zoals de Bond van Adverteerders en de Nederlandse Cosmetica Vereniging, zijn op grond van de Mediawet alle media-instellingen die reclame verzorgen verplicht aangesloten bij de code.⁴⁸² Geen van de organisaties die onder de definitie van internetdiensten zoals besproken in hoofdstuk 2 vallen is aangesloten bij de NRC. De dominante internetdiensten zijn daarentegen wel aangesloten bij de eerder besproken *EU Code of Practice against disinformation*⁴⁸³ die voornamelijk voorziet in transparantieverplichtingen. Gezien het internationale karakter van de diensten die de meeste internetbedrijven aanbieden, de mogelijkheid tot Europese coördinatie en het feit dat de internetbedrijven zelf niet aangemerkt kunnen worden als adverteerder is het onwaarschijnlijk dat deze internetbedrijven zich bij de NRC aan zullen sluiten in het kader van Nederlandse zelfregulering.

Wat betreft de handhaving is de NRC niet bindend en er staan geen formele juridische consequenties op niet-naleving.⁴⁸⁴ Wel voorziet de code in de Nederlandse Reclame Commissie die op basis van klachten uitspraak ("aanbevelingen") kan doen over specifieke gevallen. Hoewel daartoe dus niet de verplichting bestaat, geeft de Stichting Reclame Code aan dat 96% van de aanbevelingen van de Reclame Code Commissie worden opgevolgd.⁴⁸⁵ Specifiek relevant voor deze studie is dat de Reclame Code Commissie niet alleen bevoegd is in geschillen waarin een bij de code aangesloten partij betrokken is. Ook ingeval van

474 Cappello, M. (ed.), *'Media coverage of elections: the legal framework in Europe'*, IRIS Special, European Audiovisual Observatory, Strasbourg, 2017 p. 83, 87.

475 Zie bijvoorbeeld artikel 3 Nederlandse Reclame Code: "Reclame mag niet strijdig zijn met het algemeen belang, de openbare orde of de goede zeden."

476 Artikel 2 Statuten Stichting Reclame Code NL01-000131.00001/JS.

477 Zie <https://www.reclamecode.nl/nrc/>.

478 Artikel 1 Nederlandse Reclame Code.

479 Zie bijvoorbeeld ook artikel 2b Reclamecode Social Media & Influencer Marketing: Adverteerder is degene die de Verspreider stimuleert tot het maken en/of openbaar maken van Reclame via Social Media en/of degene die reclame maakt door deze op social media te plaatsen en/of door uitingen op social media te (laten) bewerken.

480 Zie: <https://www.reclamecode.nl/over-src/organisatie/>

481 Artikel 6 jo. artikel 10 statuten Stichting Reclame Code, NL01-000131.00001/JS.

482 Artikel 2.92 jo. 3.6 Mediawet.

483 Zie paragraaf 5.F.

484 Tweede Kamer, vergaderjaar 2000-2001, 27 619, nr. 3, p. 9-10.

485 Jaarverslag Stichting Reclame Code 2017 p. 32.

betrokkenheid van een niet bij de code aangesloten internetdienst is de Commissie bevoegd aanbevelingen te doen.⁴⁸⁶ Wel zijn de normen van de verschillende reclamecodes in principe slechts van toepassing op adverteerders, en niet op de voor ons relevante aanbieders van internetdiensten. Internetbedrijven kunnen hiermee dus slechts door de Reclame Code Commissie aangesproken worden wanneer zij handelen in de hoedanigheid van adverteerder. Dit neemt niet weg dat “adverteerdersmacht” ook op sociale netwerken van betekenis kan zijn. Wanneer belangrijke adverteerders zich terugtrekken of daarmee dreigen kan dat grote impact hebben.

Inhoudelijk vormen verschillende transparantieplichtingen en een verbod op misleiding de kern van de reclamecodes.⁴⁸⁷ Daarnaast bestaan er een groot aantal vrij algemeen geformuleerde normen die zien op de maatschappelijke aanvaardbaarheid van de reclame. Zo moet de reclame in overeenstemming zijn met “de goede smaak en het fatsoen”,⁴⁸⁸ mag het niet “nodeloos kwetsend zijn”⁴⁸⁹ of in strijd met “de goede zeden”.⁴⁹⁰ Met betrekking tot politieke advertenties heeft de Reclame Code Commissie aangegeven dat, gezien het grote belang van de vrijheid van meningsuiting bij politieke uitingen, er terughoudend getoetst moet worden.⁴⁹¹

In aanvulling op deze algemene code is ook relevant de bijzondere reclamecode die ziet op “Social Media & Influencer Marketing” uit 2019. Deze code richt zich zowel op de adverteerders als de “verspreiders”, degene die tegen betaling of een andere tegenprestatie reclame maakt voor de adverteerder via sociale media.⁴⁹² De verspreiders zijn dus de influencers, bloggers en vloggers die de reclame via sociale media verspreiden. Inhoudelijk bestaat de code uit een drietal aspecten die alle heel relevant zijn voor de problematiek rond desinformatie: (i) transparantieplichtingen, (ii) verbod op nepaccounts en (iii) een zorgplicht van de adverteerder. De eerste inhoudelijke verplichting, in artikel 3 van de code, bevat de bekende informatie- en transparantieplichtingen waarbij de reclame als zodanig herkenbaar moet zijn. Bijzonder aan deze verplichting is dat specifiek de “relevante relatie” tussen de verspreider en de adverteerder duidelijk gemaakt moet worden. Dit is “de relatie tussen de Adverteerder en de Verspreider gericht op het (doen) verspreiden van Reclame via Social Media, tegen betaling of enig voordeel, dat de geloofwaardigheid van de Reclame via Social Media kan beïnvloeden.”⁴⁹³ Er moet dus zowel sprake zijn van enig voordeel, als van de mogelijkheid dat de geloofwaardigheid aangetast wordt. De code geeft gedetailleerde voorbeelden van hoe deze relevante relatie duidelijk gemaakt kan worden, bijvoorbeeld door middel van hashtags (“#adv” of “#spon”) of aangeven wat de verspreider als vergoeding heeft ontvangen. Recentelijk is op basis van deze verplichting een interessante aanbeveling gegeven door de Reclame Code Commissie. Het betrof een Facebookfilmpje van Jan Roos waarin hij zich keert tegen de invoering van neutrale sigarettenpakjes. Hij vermeldde er echter niet bij dat het filmpje gesponsord was door de tabaksindustrie, wat volgens de Commissie een schending van de informatieplichting inhield.⁴⁹⁴

Vervolgens bevat de code een manipulatieverbod, die net zoals de transparantieplichting nauw aansluit bij de Europese consumentenregelgeving voor commerciële reclame.⁴⁹⁵ Interessant is dat in artikel 4 sub d de code expliciet verbiedt om “systematisch en in bulk valse/ niet-bestaande identiteiten aan te maken en/ of te gebruiken om via social media te berichten over een product en/of dienst”. Dit houdt

486 Tweede Kamer, vergaderjaar 2000-2001, 27 619, nr. 3, p. 9-10.

487 Cappello, M. (ed.), *Media coverage of elections: the legal framework in Europe*, IRIS Special, European Audiovisual Observatory, Strasbourg, 2017 p. 83.

488 Artikel 2 Nederlandse Reclame Code.

489 Artikel 4 Nederlandse Reclame Code.

490 Artikel 3 Nederlandse Reclame Code.

491 Stichting Reclame Code, 30 oktober 2012, 2012/00789B. Zie bijvoorbeeld ook een bespreking van verschillende zaken met betrekking tot politieke advertenties in IRIS Special: *Political Debate and the Role of the Media - The Fragility of Free Speech*, Nikoltchev, S. red., Strasbourg: European Audiovisual Observatory 2004 p. 12-13.

492 Artikel 2 Reclamecode Social Media & Influencer Marketing 2019.

493 artikel 2 d Reclamecode Social Media & Influencer Marketing 2019.

494 Reclame Code Commissie, 16 oktober 2019, nr. 2019/00571, <https://www.reclamecode.nl/uitspraken/influencer/tabak-2019-00571/255894/>.

495 zie hoofdstuk 5.E ‘Desinformatie en commerciële regulering’.

een verbod op het gebruik van nepaccounts, trollen en bots in en heeft dus hele duidelijke raakvlakken met de verspreiding van desinformatie wat veelal via deze technieken gebeurt. Dit verbod wordt in de toelichting gekoppeld aan de algemene en ook uit het Europees recht afkomstige verplichting om de identiteit van de adverteerder duidelijk te vermelden. Bij het gebruik van bots worden mensen immers misleid over de identiteit van de adverteerder. Dan biedt de code in de derde plaats een zorgplicht voor de adverteerder om te verzekeren dat de verspreider zich aan de reclamecode houdt.⁴⁹⁶ Vooral het begrip “relevante relatie” en de zorgplicht zijn interessante toevoegingen aan het bestaande Europeesrechtelijke kader voor commerciële communicatie gezien vanuit de desinformatie problematiek.

In het afgelopen jaar heeft de Commissie meerdere malen uitspraak gedaan naar aanleiding van klachten over politieke advertenties. Er werd geklaagd dat advertenties van onder andere Forum voor Democratie, de Partij voor de Arbeid en de Partij voor de Dieren onjuiste of misleidende informatie bevatten.⁴⁹⁷ In alle gevallen zijn de klachten afgewezen en heeft de Commissie terughoudend getoetst. Bij een tweetal uitspraken werd expliciet aangegeven dat “Het is niet aan de Reclame Code Commissie om een politieke partij te verbieden in ideële reclame te refereren aan punten uit haar verkiezingsprogramma en de argumenten die zij daarbij aanvoert, ook al worden die door velen onjuist bevonden, zolang de wijze waarop dat gebeurt binnen de grenzen van het toelaatbare blijft.”⁴⁹⁸

Hoewel de Nederlandse Reclame Code de voornaamste bron van inhoudelijke normering vormt, blijkt dat ook deze vorm van zelfregulering niet veel aanknopingspunten biedt voor dit onderzoek. De terughoudende toetsing van de Reclame Code Commissie en het feit dat de code zich in principe niet richt tot internetbedrijven maken dat code in de praktijk veel impact mist met betrekking tot politieke advertenties.

Naast de NRC is er op zelfreguleringsgebied de Raad voor de Journalistiek. De Raad voor de Journalistiek is een zelfreguleringsorgaan voor de media. De kerntaak van de Raad voor de Journalistiek is het vormgeven van zelfregulering. Bij de Raad voor de Journalistiek kunnen benadeelden terecht wanneer het medium zelf geen gehoor geeft aan de verzoeken van de benadeelde.⁴⁹⁹ De Raad voor de Journalistiek publiceert niet bindende conclusies.

De Raad voor de Journalistiek oordeelt op basis van de Leidraad van de Raad voor Journalistiek 2018 (“**Leidraad**”).⁵⁰⁰ De Leidraad is gepresenteerd in 2007, en inmiddels vier keer herzien. In de Leidraad staat goede journalistiek centraal. Goede journalistiek heeft een aantal kenmerken, het is namelijk: waarheidsgetrouw, nauwgezet, onpartijdig, fair, controleerbaar en integer.⁵⁰¹ De verantwoordelijkheid van de journalist staat in de Leidraad centraal. Hoewel de Leidraad primair is gericht op journalisten en journalistieke organisaties, moedigt de Raad voor de Journalistiek ook andere partijen die zich met journalistiek bezig houden aan om de Leidraad te volgen. De Leidraad bevat een aantal voor desinformatie relevante bepalingen, bijvoorbeeld de verplichting tot bronvermelding en tot het maken van een duidelijk onderscheid tussen feiten, beweringen en meningen.⁵⁰² Voor columnisten, cartoonisten en recensenten geldt een uitzondering: zij zijn vrij om te overdrijven en om bewust eenzijdig te berichten. Een andere relevante bepaling in het kader van desinformatie is de bepaling dat beeldmateriaal niet mag worden gebruikt als illustratie bij een ander onderwerp of met een andere context dan waarvoor de beelden zijn gemaakt. Bovendien mogen beeldmanipulaties niet misleiden en dienen ingrepen die een duidelijke verandering in

496 Artikel 6 Reclamecode Social Media & Influencer Marketing 2019.

497 Reclame Code Commissie 5 juni 2019, 2019/00333; Reclame Code Commissie 27 maart 2019, 2019/00204; Reclame Code Commissie 27 maart 2019, 2019/00201/A; Reclame Code Commissie 13 maart 2019, 2019/00157.

498 Reclame Code Commissie 27 maart 2019, 2019/00204; Reclame Code Commissie 27 maart 2019, 2019/00201/A.

499 <https://www.rvdj.nl/over-de-raad>

500 Leidraad van de Raad voor Journalistiek, 2018 via <https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae>

501 Leidraad van de Raad voor Journalistiek, 2018 via <https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae>, p. 2.

502 Leidraad van de Raad voor Journalistiek, 2018 via <https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae>, p. 4.

het beeld tweewegbrengen worden gemeld aan de lezer en kijker.⁵⁰³ In het geval van ingezonden reacties die ernstige beschuldigingen bevatten, dient de redactie van een nieuwsmedium te onderzoeken of er voor de beschuldiging een feitelijke grond bestaat.⁵⁰⁴

Op 18 maart 2019 heeft de Raad voor de Journalistiek een conclusie gepubliceerd inzake de klachten jegens de Gelderlander en het AD.⁵⁰⁵ De klager voert aan dat in een artikel desinformatie wordt verhuuld als nieuwsfeiten. Het artikel zou namelijk tal van feitelijke onjuistheden bevatten. De Raad voor de Journalistiek concludeert dat door het publiceren van de zin “FIOD doet onderzoek” journalistiek onzorgvuldig is gehandeld, aangezien in het artikel geen inzicht wordt gegeven in het verrichte onderzoek en het beschikbare bronnenmateriaal. De journalist had namelijk van de curator vernomen dat er een FIOD-onderzoek plaatsvond, maar in het artikel werd het bestaan van het onderzoek als een vaststaand feit gepresenteerd. De Raad voor de Journalistiek komt tot de slotsom dat het voor de lezers onvolgende inzichtelijk en controleerbaar is waar de informatie op is gebaseerd, waardoor de berichtgeving kan worden gekwalificeerd als onevenwichtig en tendentius. De Gelderlander heeft op 19 maart 2019 gehoor gegeven aan het advies van de Raad voor de Journalistiek en de conclusie gepubliceerd.⁵⁰⁶

Op 24 oktober 2019 heeft de Raad voor de Journalistiek een conclusie gepubliceerd over misleidende koppen.⁵⁰⁷ JOOP, de online opinie pagina van BNNVARA, had een artikel getiteld “Nederlandse psycholoog trekt opnieuw nazi-wetenschap uit de kast” gepubliceerd.⁵⁰⁸ In de intro van het artikel wordt vermeld dat de psycholoog de intelligentie van nazi kopstukken roemt. De kop en de intro wekken de onjuiste suggestie dat de psycholoog nazi-wetenschap bedrijft, aldus de Raad voor Journalistiek. Een kop mag wel “een vergroving van de inhoud van het bijbehorende artikel bevatten. Daarmee worden de grenzen van journalistieke zorgvuldigheid alleen overschreden als de kop geen grond vindt in het artikel.” De Raad voor de Journalistiek komt tot de slotsom dat de journalist en JOOP onzorgvuldig hebben gehandeld.⁵⁰⁹

Naast de Leidraad heeft de Raad voor de Journalistiek ook een beroepsethische code, de Code van de Raad voor de Journalistiek (“Code”). De meest recente versie van de Code werd is van kracht sinds september 2019. De Code is geactualiseerd naar aanleiding van digitalisering en de maatschappelijke aandacht voor “nepnieuws”.⁵¹⁰ De Code bevat aparte artikelen over waarheidsgetrouw berichten en onafhankelijk informeren. Deze artikelen bevatten onder andere een verbod op het schrappen of verdraaien van essentiële informatie.⁵¹¹ Het publiek mag op geen enkele wijze misleid worden door beeldbewerkingen of archiefmateriaal wat niet als zodanig herkenbaar is.⁵¹² Bovendien dient een journalist voor het publiek een duidelijk onderscheid te maken tussen feitelijke berichtgeving en commentaar.⁵¹³

Op 7 juni 2018 heeft de voorzitter van de Raad voor de Journalistiek de wens tot het doen van een verbeteringsonderzoek aangekondigd. De aanleiding voor dit onderzoek is volgens de voorzitter de verspreiding van desinformatie: *“Zelfregulering kan duidelijk maken wat het verschil is tussen goede en slechte journalistiek, tussen journalisten, die zichzelf en hun publiek serieus nemen en die dat niet doen”*, aldus de voorzitter van de Raad voor de Journalistiek.⁵¹⁴

503 Leidraad van de Raad voor Journalistiek, 2018 via <https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae>, p. 5.

504 Leidraad van de Raad voor de Journalistiek, 2018 via <https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae>, p. 6.

505 Raad van de Journalistiek, conclusie nummer 2019/16 via <https://www.rvdj.nl/2019/16>.

506 <https://www.gelderlander.nl/nijmegen-e-o/uitspraak-raad-voor-journalistiek-over-klacht-nijmegenaar-jankie-ac33758d/>

507 Raad van de Journalistiek, conclusie nummer 2019/46 via <https://www.rvdj.nl/2019/46>.

508 <https://joop.bnnvara.nl/nieuws/nederlandse-psycholoog-trekt-opnieuw-nazi-wetenschap-uit-de-kast>; <https://joop.bnnvara.nl/over-joop>

509 Raad van de Journalistiek, conclusie nummer 2019/46 via <https://www.rvdj.nl/2019/46>.

510 <https://www.rvdj.be/nieuws/herwerkte-code-met-oog-voor-fake-news-en-digitalisering>

511 Artikel 3 Code van de Raad voor de Journalistiek, p. 9 via <https://www.rvdj.be/sites/default/files/pdf/code-rvdj.pdf>

512 Richtlijn bij artikel 3, Code van de Raad voor de Journalistiek, p. 14 via <https://www.rvdj.be/sites/default/files/pdf/code-rvdj.pdf>

513 Artikel 4 Code van de Raad voor de Journalistiek, p. 9 via <https://www.rvdj.be/sites/default/files/pdf/code-rvdj.pdf>

514 <https://www.rvdj.nl/over-de-raad/berichten/sterkere-raad-voor-de-journalistiek-is-nu-meer-dan-ooit-nodig>

Tot slot, ten aanzien van journalistieke ontwikkelingen op het gebied van desinformatie, heeft het Stimuleringsfonds voor de Journalistiek subsidie verleend aan DROG, een organisatie die zich tot doel stelt om burgers te informeren over misleiding en polarisatie door desinformatie.⁵¹⁵ DROG richt zich voornamelijk op jongvolwassenen.⁵¹⁶ DROG heeft onder andere het *Slecht Nieuws spel* ontwikkeld, waarmee gratis via slechtnieuws.nl een spel over desinformatie kan worden gespeeld.⁵¹⁷

E. Nationale politieke ontwikkelingen

De mogelijke regulering van desinformatie is al enige tijd onderwerp van maatschappelijk debat en de afgelopen maanden is in aanvulling hierop specifiek de regulering van politieke advertenties in toeneemende mate op de agenda gekomen. Hieronder volgt een overzicht van de belangrijkste recente politieke ontwikkelingen op dit gebied, die mede de aanleiding vormen voor dit rapport.

i. Rapport Staatscommissie Parlementair Stelsel

Van belang is de Staatscommissie Parlementair Stelsel die in december 2018 haar rapport “Lage drempels, hoge dijken” heeft afgerond.⁵¹⁸ Vier aanbevelingen van de commissie zijn specifiek relevant voor deze studie.⁵¹⁹ Ten eerste stelt de commissie voor om politieke partijen te verplichten te rapporteren over de digitale campagne instrumenten die zij inzetten. De tweede en derde aanbeveling zien op de invoering van een transparantieplichting voor digitale politieke advertenties onder toezicht van een onafhankelijke toezichthouder. Ten vierde beveelt de commissie aan om een onafhankelijke organisatie aan te wijzen die rapporteert over de invloed van algoritmische rangschikking van politieke informatie op online platforms.

Meer specifiek beveelt de commissie aan dat de transparantieplichting omvat hoeveel geld uitgegeven wordt aan digitale advertenties, op welke groepen deze advertenties gericht zijn en op basis van welke gegevens deze groepen uitgekozen zijn. Ook beveelt de commissie aan om een limiet te zetten op het percentage van advertenties die slechts aan een specifieke groep gericht worden, en dat de overige advertenties ongericht getoond moeten worden.⁵²⁰ Daarnaast moeten gebruikers van sociale media snel en gemakkelijk kunnen zien of het een betaalde advertentie betreft, en wie de achterliggende partij is. Ook pleit de commissie voor duidelijkheid voor de gebruikers over of, en zo ja op basis waarvan, advertenties op hen gericht zijn.⁵²¹ Dit alles zou onder toezicht staan van een nieuw te creëren onafhankelijke toezichthouder. De commissie baseert deze aanbeveling deels op de in hoofdstuk 5 besproken Commissie aanbeveling van september 2018.⁵²²

Met betrekking tot de rol van algoritmische ordening van door gebruikers gegenereerde informatie op internet platforms, signaleert de commissie dat de algoritmisch gestuurde aanbevelingen bepaalde

⁵¹⁵ <https://wijzijndrog.nl/>

⁵¹⁶ <https://www.svdj.nl/nieuws/drog-wil-jonge-mensen-immuun-maken-voor-desinformatie/>

⁵¹⁷ <https://wijzijndrog.nl/serious-game-over-propaganda>

⁵¹⁸ Staatscommissie parlementair stelsel, *‘Lage Drempels, Hoge Dijken. Democratie en rechtstaat in balans’* Den Haag 2018, bijlage bij Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 9. Zie ook: Voerman, G., *‘De positie van de politieke partij in het eindrapport van de staatscommissie Parlementair stelsel’*, 2018 https://www.denederlandsegrondwet.nl/9353000/1/j4nvih7l3kb91rw_j9vvkl1ouc6v2/vkurgjfw8x4/f=/bijdrage_gerrit_voerman.pdf

⁵¹⁹ Staatscommissie parlementair stelsel, *‘Lage Drempels, Hoge Dijken. Democratie en rechtstaat in balans’* Den Haag 2018, par. 6.4.2 - 6.4.5.

⁵²⁰ Idem, par. 6.4.2.

⁵²¹ Idem, par. 6.4.3.

⁵²² Europese Commissie, *‘Commission Recommendation of 12 September 2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament’*, C (2018) 5949.

politieke denkbeelden bevoordeelt.⁵²³ De aanbeveling dat een onafhankelijke organisatie dit monitort en hierover rapporteert, dient voornamelijk tot het verkrijgen van meer inzicht in en grip op deze praktijk. De commissie biedt dit aan als mogelijke oplossing voor de huidige verregaande informatie asymmetrie tussen de internetbedrijven enerzijds en de overheid en de maatschappij anderzijds. Ook in wetenschappelijk verband staat de vraag naar de kenbaarheid en meetbaarheid van de dynamiek op internet platformen, vanuit de vraag naar de maatschappelijke impact, in de aandacht.⁵²⁴

Naar aanleiding van het rapport “Lage drempels, hoge dijken” heeft het kabinet in juni 2019 een kabinetsstandpunt gepubliceerd.⁵²⁵ Het kabinet erkent dat in het rapport terecht wordt gewezen op digitale risico’s voor het democratisch proces, zoals de aantasting van de autonomie van de kiezer door micro-targeting.⁵²⁶ Het kabinet onderschrijft het advies om wettelijke voorwaarden aan micro-targeting te stellen.⁵²⁷ Het kabinet streeft ernaar om dergelijke wettelijke voorwaarden op te nemen in de Wet op de Politieke Partijen.⁵²⁸ Het in het leven roepen van een aparte, onafhankelijke toezichthouder acht het kabinet een reële optie in het geval van een forse uitbreiding van het takenpakket.⁵²⁹

ii. Wet op de politieke partijen

Naar aanleiding van het bovengenoemde rapport van de Staatscommissie Parlementair Stelsel⁵³⁰ en het in paragraaf 6.B besproken advies uit februari 2018 van de Evaluatie- en Adviescommissie Wet financiering politieke partijen⁵³¹ heeft de regering aangegeven voornemens te zijn een nieuwe Wet op de Politieke Partijen in te stellen.⁵³² De regering schrijft dat zij tot doel heeft om de onafhankelijke positie van politieke partijen verder te versterken, onder andere door de wettelijke positie van politieke partijen duidelijker te regelen. De Wet op de politieke partijen zal transparantieplichtingen voor politieke partijen bevatten.⁵³³ Het streven is om in deze wet de aanbevolen transparantieplichtingen voor politieke partijen met betrekking tot digitale politieke campagnes en micro-targeting op te nemen.⁵³⁴ Met de Wet op de Politieke Partijen zal worden voorzien in een samenhangende regeling die nu ontbreekt, met uitzondering van de Wet financiering politieke partijen en de Kieswet.⁵³⁵ De Wet op de Politieke Partijen zal de Wet financiering politieke partijen omvatten en delen van de Kieswet aanpassen. De wet zal ook een verbod op giften van buiten de EU aan Nederlandse politieke partijen bevatten.

De Evaluatie- en Adviescommissie Wet financiering politieke partijen (de commissie-Veling) heeft in februari 2018 een rapport getiteld “Het publieke belang van politieke partijen” gepubliceerd. Uit dit rapport blijkt onder andere de terughoudendheid van de overheid in subsidiering in verband met de opvatting van de gepaste afstand die de overheid dient te bewaren.⁵³⁶ Bij de voorbereiding van de Wet

523 Idem, par. 6.4.5 op basis van Hazenberg, H. e.a., ‘Micro-targeting and ICT media in the Dutch Parliamentary System’, p. 49-51. Nieder, B, ‘From ranking algorithms to ‘ranking cultures’. Investigating the modulation of visibility in YouTube search results’ The International Journal of Research into New Media Technologies, 2018, 24/1, p. 50-68. Er loopt internationaal een discussie over de toegang voor wetenschappers tot relevante data van sociale mediabedrijven voor onderzoek naar de impact op democratische processen. Zie bijvoorbeeld dit recente bericht van de Social Science Research Council in the VS over de moeilijkheden die in dit kader worden ondervonden om de data beschikbaar te kunnen maken aan onderzoekers. SSRC, Statement from Social Science Research Council President Alondra Nelson on the Social Media and Democracy Research Grants Program, 27 Augustus 2019, <https://www.ssrc.org/programs/view/social-data-initiative/sdi-statement-august-2019/>.

524 Zie bijvoorbeeld N.Diakopoulos & M. Koliska, Algorithmic Transparency in the News Media, Digital Journalism, 2017, 5:7, 809-828, DOI: 10.1080/21670811.2016.1208053 en K. Yeung, Why Worry about Decision-Making by Machine? In: K. Yeung & M. Lodge (ed.) Algorithmic Regulation, Oxford University Press, 2019.

525 Kamerstuk 34 430, nr. 10 F.

526 Kamerstuk 34 430, nr. 10 F, p. 3.

527 Kamerstuk 34 430, nr. 10 F, p. 12.

528 Kamerstuk 34 430, nr. 10 F, p. 11.

529 Kamerstuk 34 430, nr. 10 F, p. 12.

530 Staatscommissie parlementair stelsel, ‘Lage Drempels, Hoge Dijken. Democratie en rechtstaat in balans’ Den Haag 2018, p. 18.

531 Tweede Kamer, vergaderjaar 2017-2018, 32 752, nr. 50; Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 10, p. 12.

532 Tweede Kamer, vergaderjaar 2018-2019, 32 752, nr. 54; Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 10, p. 10-12.

533 Tweede Kamer, vergaderjaar 2019-2020, 30821, nr. 91, p. 6.

534 Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 10, p. 12.

535 Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 10, p. 11.

536 Evaluatie- en Adviescommissie Wet financiering politieke partijen, ‘Het publieke belang van politieke partijen’, 2018, p. 18.

op de Politieke Partijen worden aanbevelingen van de commissie-Veling onderzocht.⁵³⁷ Het betreffen de aanbevelingen die de commissie-Veling heeft gedaan die nog niet meegenomen worden bij de herziening van de Wet financiering politieke partijen.⁵³⁸

iii. Moties

Asscher en Buitenweg

In het kader van de Provinciale Statenverkiezingen is op 7 februari 2019 door de Tweede Kamer leden Asscher en Buitenweg een motie ingediend over digitale politieke advertenties. De indieners willen de garantie van Facebook dat er volledige transparantie gegeven wordt over de afzenders van politieke advertenties op het platform.⁵³⁹ De motie is met een meerderheid van 22 stemmen aangenomen.

De regering heeft op 19 februari per brief gereageerd⁵⁴⁰ en wijst in zijn reactie voornamelijk op de Europese zelfreguleringscode. De motie is ten dele uitgevoerd door middel van de doorgaande implementatie van de *Code of Practice on Disinformation*. De aangesloten platforms, waaronder Facebook, zouden nu bij iedere politieke advertentie in de EU aangeven wie de afzender is, hoeveel ervoor betaald is en door hoeveel mensen de advertentie gezien is. Zoals aangegeven in paragraaf 5.D worden in de Code politieke advertenties vrij nauw gedefinieerd als direct betrekking hebbend op een specifieke verkiezing of verkiezingskandidaat.⁵⁴¹ Vervolgens worden deze advertenties in een openbare database geplaatst.⁵⁴² Uit een onderzoek van burgerrechten organisatie Bits of Freedom van afgelopen mei blijkt echter dat Facebook nog niet goed in staat is een politieke advertentie als zodanig te herkennen en om vervolgens de juiste maatregelen toe te passen.⁵⁴³

Naast deze zelfreguleringsmaatregelen wijst de minister in zijn reactie op de motie ook op de aanstaande Wet politieke partijen en de mogelijke daarin vervatte regelgeving met betrekking tot politieke advertenties.⁵⁴⁴

Motie Asscher en van der Molen

De Kamerleden Asscher en van der Molen hebben op 13 maart 2019 een motie ingediend over het strafrechtelijk aanpakken van bewuste online manipulatie.⁵⁴⁵ De motie is op 19 maart 2019 gewijzigd.⁵⁴⁶ De enige wijziging van de motie betrof de toevoeging van "onder andere" in de constatering dat "onder andere" sociale mediabedrijven te vaak regels ten aanzien van online manipulatie hebben overschreden. De motie verzoekt de regering om te onderzoeken of huidige strafrechtelijke delictomschrijvingen kunnen worden uitgebreid en daarmee ook toepassing kunnen vinden op bewuste online manipulatie. De motie ziet op situaties waarin bijvoorbeeld digitaal de boodschap wordt verspreid dat de verkiezing niet plaatsvindt of op een andere datum plaatsvindt.⁵⁴⁷

Het huidige artikel 127 Wetboek van Strafrecht heeft voornamelijk betrekking op frauduleuze handelingen met betrekking tot het stembiljet.⁵⁴⁸ Het huidige artikel 129 Wetboek van Strafrecht regelt onder andere het verhinderen van de stemming, zoals het verduisteren van stembriefjes, het openbreken van

⁵³⁷ Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 10, p. 11-12.

⁵³⁸ Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 10, p. 11-12.

⁵³⁹ Motie Asscher en Buitenweg, Tweede Kamer, vergaderjaar 2018-2019, 35 078, nr. 21.

⁵⁴⁰ Tweede Kamer, vergaderjaar 2018-2019, 35 078, nr. 26.

⁵⁴¹ Artikel 3-4 EU Code of Practice on Disinformation.

⁵⁴² Tweede Kamer, vergaderjaar 2018-2019, 30 821, nr. 74, p. 3; EU Commission, *Code of Practice on Disinformation. Intermediate Targeted Monitoring - March reports*, 23 April 2019, <https://ec.europa.eu/digital-single-market/en/news/third-monthly-intermediate-results-eu-code-practice-against-disinformation>. Zie verder paragraaf 5.F.

⁵⁴³ NOS, 'Bits of Freedom: 'Facebook gaat de fout in met politieke advertenties'', 20 mei 2019 <https://nos.nl/nieuwsuur/artikel/2285561-bits-of-freedom-facebook-gaat-de-fout-in-met-politieke-advertenties.html>.

⁵⁴⁴ Tweede Kamer, vergaderjaar 2018-2019, 35 078, nr. 26, p. 2.

⁵⁴⁵ Motie Asscher- Van der Molen, Tweede Kamer, vergaderjaar 2018/19, 30821, nr. 60.

⁵⁴⁶ Gewijzigde Motie van leden Asscher en Van der Molen, Tweede Kamer, vergaderjaar 2018/19, 30821, nr. 68.

⁵⁴⁷ <https://zoek.officielebekendmakingen.nl/h-tk-20182019-62-5.pdf>

⁵⁴⁸ Noyon/Langemeijer/Remmelink Strafrecht, artikel 127 Sr, aant. 2; HR 10 november 1890, W 5966.

een stembus of het manipuleren van een stemmachine.⁵⁴⁹ Met artikel 129 Wetboek van Strafrecht wordt de zuiverheid van verkiezingen en de uitkomst daarvan beschermd.⁵⁵⁰

Motie Kuiken en Verhoeven

In een motie van 25 juni 2019, unaniem aangenomen door de Tweede Kamer, verzoeken de leden Kuiken en Verhoeven de regering om de mogelijkheid tot de invoering van “een wettelijke transparantieplicht voor politieke advertenties op onlineplatforms te onderzoeken”.⁵⁵¹ De motie van de leden Kuiken en Verhoeven bouwt voort op de transparantie-aanbeveling van de Staatscommissie Parlementair Stelsel in het reeds eerder genoemde rapport “Lage drempels, Hoge dijken”.

iv. Bewustwordingscampagnenationale

Op 16 november 2017 verzochten de leden Verhoeven, Van der Molen, Middendorp, Kuiken en Van der Graaf om een voorlichtingscampagne te starten “om het bewustzijn te vergoten over beïnvloeding door statelijke actoren van de interne aangelegenheden en democratische processen in Nederland”.⁵⁵² Daarnaast zijn naar aanleiding van een motie van de leden Westerveld en Van den Hul gesprekken gevoerd over mediawijsheid met onder andere Mediawijzer.net, de Koninklijke Bibliotheek en de Vereniging van Nederlandse Gemeenten. Uit deze gesprekken is gebleken dat een samenhangende aanpak voor mediawijsheid gewenst is.⁵⁵³ Tussen 11 maart en 23 mei 2019 werd, vannuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de bewustwordingscampagne “Blijf nieuwsgierig. Blijf kritisch” gevoerd.⁵⁵⁴ Op de website blijfkritisch.nl kunnen burgers praktische tips vinden. De campagne, die bestaat uit radiospotjes, en online video's, is onderdeel van een bredere verbetering van de mediawijsheid. Op de website blijfkritisch.nl staat onder andere een checklist “Is die informatie echt?”.⁵⁵⁵ Met deze checklist kunnen burgers zelf, bijvoorbeeld door bronnenonderzoek, verifiëren of informatie echt is. De website vermeldt uitdrukkelijk dat het niet een taak van de overheid is om te oordelen over de (on)juistheid van informatie. Tot slot uitten de Autoriteit Consument en Markt en het Commissariaat voor de Media dat zij de mogelijkheden voor nieuwe initiatieven om de mediawijsheid te vergroten gaan inventariseren.⁵⁵⁶ De toezichthouders hebben de volgende risico's gesignaleerd: verdringing van kwaliteitsnieuws, verschrapping van het nieuwsaanbod en verdunning van de mediasector.⁵⁵⁷ Minister Ollongren schrijft dat in het regeerakkoord extra middelen zijn vrijgemaakt voor de versterking van onderzoeksjournalistiek.⁵⁵⁸

v. Mediawijzer

De Mediawijzer is onderdeel van het Netwerk Mediawijsheid waar ook Mediawijsheid.nl en HoeZoMediawijs.nl onderdeel van uitmaken.⁵⁵⁹ De missie van het Netwerk Mediawijsheid is om Nederland mediawijs te maken.⁵⁶⁰ Mediawijsheid is volgens Mediawijzer een verzameling competenties die nodig zijn om actief en bewust deel te kunnen nemen aan de mediasamenleving.⁵⁶¹ De website van Mediawijsheid heeft een apart dossier getiteld “Nepnieuws”.⁵⁶² Het Netwerk Mediawijsheid wordt aangestuurd door: het Nederlands Instituut voor Beeld en Geluid, het ECP, Human, Kennisnet en de Koninklijke Bibliotheek.⁵⁶³ In 2017

549 Smidt II, p. 64; Noyon/Langemeijer/Rommelink Strafrecht, artikel 129 Sr, aant. 1a.

550 Van der Woude, *T&C Strafrecht, commentaar op artikel 129 Sr*, 2019, Wolters Kluwer.

551 Motie Kuiken en Verhoeven, Tweede Kamer, vergaderjaar 2018-2019, 32 761, nr. 145.

552 Tweede Kamer, vergaderjaar 2017-2018, 34 775 VII, nr. 21

553 Tweede Kamer, vergaderjaar 2018-2019, 35000-VIII, nr. 91, p. 26.

554 <https://www.rijksoverheid.nl/actueel/nieuws/2019/03/11/campagne-nepnieuws-vandaag-van-start>; zie ook: Tweede Kamer, vergaderjaar 2018-2019, 30 821, nr. 51, p. 5.

555 <https://www.rijksoverheid.nl/onderwerpen/desinformatie-nepnieuws/checklist-tips-tegen-nepnieuws-desinformatie>

556 ACM & CvdM, *Digitalisering en nepnieuws: een gezamenlijke verkenning van de Autoriteit Consument & Markt en het Commissariaat voor de Media*, 2018, p. 13; zie ook Commissariaat voor de Media: wettelijke ZBO-evaluatie p. 28 via <https://zoek.officielebekendmakingen.nl/blg-877381>.

557 Tweede Kamer, vergaderjaar 2018-2019, 30 821, nr. 51, p. 2.

558 Tweede Kamer, vergaderjaar 2018-2019, 30 821, nr. 51, p. 2.

559 <https://www.mediawijzer.net/over-ons/>.

560 <https://www.mediawijzer.net/onzemissie/>.

561 <https://www.mediawijzer.net/van-mediawijzer-net/competentiemodel/>.

562 <https://www.mediawijsheid.nl/nepnieuws/>.

563 Idem.

werd desinformatie besproken als onderdeel van de Week van de Mediawijsheid, georganiseerd door Mediawijzer.⁵⁶⁴

vi. NL DIGIbeter 2019

De “NL DIGIbeter 2019: Agenda Digitale Overheid” valt onder de Nederlandse digitaliseringsstrategie en is een jaarlijks geactualiseerd document.⁵⁶⁵ In de NL DIGIbeter 2019 wordt onder andere aandacht geschonken aan publieke waarden. In opdracht van het Ministerie van Justitie en Veiligheid loopt een onderzoek naar algoritmische besluitvorming.⁵⁶⁶ Dit onderzoek wordt uitgevoerd door de Universiteit Utrecht.⁵⁶⁷

Het Strategisch Actieplan voor Artificiële Intelligentie sluit aan bij de Nederlandse digitaliseringsstrategie 2018.⁵⁶⁸ Het Strategisch Actieplan voor Artificiële Intelligentie bevat als onderdeel van Spoor 3 het blijven beschermen van publieke waarden en mensenrechten.⁵⁶⁹ In het actieplan wordt niet besproken hoe eventuele automatische besluitvorming invloed kan hebben op nieuws in het algemeen of desinformatie in het bijzonder. Wel wordt in het rapport gesignaleerd dat de vrijheid van meningsuiting kan worden beperkt bij bijvoorbeeld ordening van zoekresultaten en algoritmes die zonder menselijke tussenkomst content verwijderen.⁵⁷⁰

vii. Toezegging minister Dekker

In een debat van 19 februari 2019 in de Eerste Kamer heeft de Minister voor Rechtsbescherming naar aanleiding van een vraag van het lid Duthler een aantal toezeggingen gedaan met betrekking tot de regulering van politieke advertenties. Minister Dekker heeft toegezegd “in kaart te brengen wat de effecten zijn van mirco-targeting en daarbij te kijken naar de kansen, maar vooral ook naar de risico’s die dat oplevert voor specifieke waarden en individuele vrijheden”. Hierbij zullen de internationale componenten ook betrokken worden.⁵⁷¹

viii. Brief minister Ollongren

Op 18 oktober 2019 heeft minister Ollongren per brief de Tweede Kamer geïnformeerd over het beleid ten aanzien van desinformatie.⁵⁷² De brief kaart aan dat de democratische rechtstaat betere bescherming behoeft op het gebied van digitale risico’s.⁵⁷³ Dit schrijft de minister naar aanleiding van de motie van de leden Middendorp en Verhoeven.⁵⁷⁴ De brief bespreekt de drie actielijnen van de desinformatie-strategie: preventie, verstevigen van de informatiepositie en reactie.⁵⁷⁵ De nadruk ligt op de preventieve actielijn, die weer uit vier pijlers bestaat: de weerbaarheid van burgers versterken, de weerbaarheid van politieke ambtsdragers vergroten, de transparantie vergroten en een pluriform medialandschap behouden.⁵⁷⁶

F. Overzicht nationale wetgeving

Het brede scala aan wet- en regelgeving dat in dit hoofdstuk, als ook in hoofdstuk 5, de revue gepasseerd heeft, laat de diversiteit en breedte van het relevante reguleringslandschap zien. De verschillende

⁵⁶⁴ McGonagle, T. e.a., *‘Inventarisatie methodes om “nepnieuws” tegen te gaan’*, Instituut voor Informatierecht, 2018, p. 65.

⁵⁶⁵ NL DIGIbeter 2019: Agenda Digitale Overheid, p. 5.

⁵⁶⁶ NL DIGIbeter 2019: Agenda Digitale Overheid, p. 30.

⁵⁶⁷ <https://www.uu.nl/nieuws/wodc-onderzoek-naar-juridische-aspecten-van-algoritmen-die-besluiten-nemen> ; <https://www.wodc.nl/onderzoeksdatabase/2947-regulering-van-algoritmen-die-zelfstandig-besluiten-nemen.aspx>.

⁵⁶⁸ ‘Strategisch Actieplan voor Artificiële Intelligentie’, p. 10.

⁵⁶⁹ ‘Strategisch Actieplan voor Artificiële Intelligentie’, p. 6.

⁵⁷⁰ ‘Strategisch Actieplan voor Artificiële Intelligentie’, p. 41.

⁵⁷¹ Eerste Kamer, vergaderjaar 2018-2019, nr. 19, item 9, p. 19-20; Eerste Kamer, vergaderjaar 2018-2019, nr. 19, item 11, p. 25.

⁵⁷² Tweede Kamer, vergaderjaar 2019-2020, 30821, nr. 91.

⁵⁷³ Tweede Kamer, vergaderjaar 2019-2020, 30821, nr. 91, p. 3.

⁵⁷⁴ Tweede Kamer, vergaderjaar 2019-2020, 30821, nr. 63.

⁵⁷⁵ Tweede Kamer, vergaderjaar 2019-2020, 30821, nr. 91, p. 2; zie ook <https://www.rijksoverheid.nl/actueel/nieuws/2019/10/18/kabinet-zet-in-op-transparantie-in-strategie-tegen-desinformatie>.

⁵⁷⁶ Tweede Kamer, vergaderjaar 2019-2020, 30821, nr. 91, p. 6.

wettelijke bepalingen relevant voor de problematiek rond desinformatie snijden dwars door de klassieke rechtsgebieden heen. Dit vergroot de complexiteit van de problematiek nu de drie algemene rechtsgebieden, het privaatrecht, strafrecht en het bestuursrecht, alle drie een eigen normatief en procedureel kader kennen. De verschillende privaatrechtelijke, strafrechtelijke en bestuursrechtelijke normen in dit hoofdstuk besproken zijn als volgt:

Privaatrecht	Strafrecht	Bestuursrecht
Onrechtmatige daad (onrechtmatige pers-publicatie)	Uitingsdelicten (o.a. smaad, laster, haatzaaiing, belediging)	Reclameregulering (mediawet)
	Verkiezingsdelicten (o.a. artikel 127 Sr)	Wet financiering politieke partijen
Intellectueel eigendomsrecht	Computercriminaliteit (artikel 138ab Sr)	Nationale veiligheid
	Verspreidingsdelicten (o.a. artikel 137e Sr)	Kritische infrastructuur

Tabel 3.

Een eerste observatie naar aanleiding van dit overzicht is dat op nationaal niveau de voor desinformatie relevante wetgeving voornamelijk betrekking heeft op de inhoud van een uiting. Daarnaast blijkt ook duidelijk dat een groot aantal vormen van desinformatie al gereguleerd is. Vervolgens hebben de privaatrechtelijke en strafrechtelijke normen met elkaar gemeen dat deze veelal zeer context-specifiek zijn. Voornamelijk wat betreft de onrechtmatige daad is de concrete toepassing van deze normen zeer complex en context specifiek, wat heeft geleid tot een zeer genuanceerde en afgewogen jurisprudentie. Hetzelfde geldt voor wanneer een uiting te gelden heeft als een te beschermen satire en wanneer niet. Ook strafrechtelijke normen die aan desinformatie raken zijn divers en zeer contextgevoelig, zeker wat betreft de uitingsdelicten en de bijbehorende verspreidingsdelicten is de juridische kwalificatie zeer afhankelijk van de specifieke context. Dit compliceert de mogelijke regulering van desinformatie aanzienlijk nu het betekent dat in dit soort gevallen de juridische kwalificatie moeilijk te maken is.

Vervolgens is ook nog stilgestaan bij de verschillende relevante zelfregulering, voornamelijk de Nederlandse Reclame Code en de Raad voor de Journalistiek. Beiden bieden een uitgebreid normenkader waarbij onder andere ook mogelijke desinformatie verspreid in het kader van commerciële reclame of nieuws wordt geadresseerd. Afsluitend is een overzicht geboden van de verschillende nationale politieke ontwikkelingen die relevant zijn voor de regulering van desinformatie. Hieruit blijkt duidelijk dat het veld in beweging is en dat nieuwe wetgeving op het gebied van de financiering van politieke partijen te verwachten is.

7. Synthese

- De onderzochte landen hebben een breed scala aan verschillende reacties op desinformatie geïmplementeerd. Dit omvat programma's voor mediageletterdheid, mediafinanciering, nationale veiligheidsstrategieën, wetgeving die desinformatie verbiedt, wetgeving die zorgplichten oplegt aan onlineplatforms, wetgeving die gericht is op buitenlandse invloeden en wetgeving met betrekking tot bots en geautomatiseerde software.
- Regulering van politieke reclame zal naar verwachting geen oplossing bieden voor veel van de uitdagingen in verband met desinformatie.
- Het huidige juridische kader voor de regulering van desinformatie en politieke advertenties heeft betrekking op wetgeving en beleid op drie onderling samenhangende niveaus: de EU, de nationale wetgeving en het nationale beleid, en het niveau van het beleid voor de particuliere sector

A. Desinformatie

i. Landenstudies en beleidsvoorbeelden

In de bijgevoegde landenstudies (zie appendix) is onderzocht hoe een aantal landen (het Verenigd Koninkrijk, Frankrijk, Duitsland, Zweden, VS en Canada) de problemen rondom desinformatie die verspreid wordt via internetdiensten hebben aangepakt. Hier kwamen een aantal verschillende benaderingen uit naar voren.

Ten eerste hebben een aantal regeringen nieuwe programma's voor **mediageletterdheid** opgezet en meer financiële middelen voor bestaande programma's vrijgemaakt. Het doel is om ervoor te zorgen dat de gebruikers van internetdiensten beter bestand zijn tegen desinformatie (zie bijvoorbeeld Canada, Frankrijk, het Verenigd Koninkrijk, Zweden). Deze programma's worden ook specifiek gericht op de belangrijke internetdiensten. Zo heeft in Frankrijk de media toezichthouder (Conseil Supérieur de l'Audiovisuel) een nieuwe wettelijke verplichting voor internetdiensten ingevoerd om toe te zien op de uitvoering van maatregelen ter bevordering van de media- en informatievaardigheden. Het Verenigd Koninkrijk heeft ook een voorstel gedaan voor een nieuwe toezichthoudende instantie die verantwoordelijk is voor online mediageletterdheid. Deze instantie houdt ook toezicht op de uitgaven van internetdiensten voor mediageletterdheid programma's. De Zweedse regering heeft bijvoorbeeld de Zweedse Raad voor de Media de verantwoordelijkheid gegeven voor een nieuw programma met betrekking tot mediageletterdheid om desinformatie tegen te gaan. Andere voorbeelden zijn de financiering van de Canadese regering voor haar nieuwe Digital Citizen Initiative, een meervoudige strategie die tot doel heeft de democratie te ondersteunen door het opbouwen van de weerbaarheid van burgers tegen online desinformatie. Deze maatregelen sluiten aan bij de aanbevelingen van de vier speciale internationale mandaten inzake vrijheid van meningsuiting, de Europese Commissie en de Raad van Europa dat het versterken van de mediageletterdheid één van de beste manieren is om desinformatie tegen te gaan.⁵⁷⁷

⁵⁷⁷ United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint declaration on freedom of expression and "fake news", disinformation and propaganda, FOM.GAL/3/17, 3 March 2017, para. 3(e); European Commission, Tackling online disinformation: a European Approach, COM(2018) 236 final, sec. 3; and Council of Europe, Committee of Ministers' Recommendation CM/Rec(2018)1 to Member States on media pluralism and transparency of media ownership (7 March 2018), Appendix, sec. 5.

In de tweede plaats hebben regeringen **media financieringsprogramma's** opgezet. De Britse regering heeft bijvoorbeeld overheidsmiddelen (18 miljoen pond) ingezet om de onafhankelijke media te versterken, en om desinformatie en vals nieuws in Oost-Europa en de westelijke Balkan tegen te gaan. De Zweedse regering heeft daarnaast via de Zweedse Innovatieautoriteit ook geld (13,5 miljoen kronen) geïnvesteerd in een nieuw digitaal platform om de verspreiding van valse nieuwsverhalen online te voorkomen.

Ten derde is desinformatie ook door overheden opgepakt in het kader van de **nationale veiligheid**.⁵⁷⁸ Zo behandelt de Zweedse regering desinformatie als een nationale veiligheidskwestie, en maakt de bestrijding van desinformatie tijdens verkiezingen deel uit van de nationale veiligheidsstrategie van de Zweedse regering. Daarnaast heeft het Zweedse Bureau voor civiele rampenbestrijding een handboek van 50 pagina's gepubliceerd genaamd *Countering information influence activities*. Ook de Verenigde Staten behandelt desinformatie als een nationale veiligheidskwestie. Het wees \$120 miljoen in financiering toe aan het Ministerie van Buitenlandse Zaken van de V.S. om een agentschap op te richten. Dit agentschap moet overheidsinitiatieven ontwikkelen en synchroniseren die buitenlandse informatieverrichtingen tegen de nationale veiligheidsbelangen van de V.S. bloot kunnen leggen en tegen kunnen gaan en die daarnaast op feiten gebaseerde narratieven te bevorderen die de bondgenoten en de belangen van de V.S. steunen.

Ten vierde hebben bepaalde landen specifieke wetten die **desinformatie** of valse informatie **verbieden**. Het beste voorbeeld is Frankrijk, dat een specifieke wet heeft die de publicatie van vals nieuws verbiedt. Dit is al vele jaren strafbaar op basis van de Persvrijheidwet van 1881. Daarnaast is de meest relevante nieuwe Franse wetgeving voor internetdiensten de Wet op de manipulatie van informatiewet van 2018. Hierbij kan een rechtbank een online platform gelasten om "onjuiste misleidende beschuldigingen of beschuldigingen van feiten" te verwijderen, die "de oprechtheid van een komende stemming kunnen veranderen", en "opzettelijk, kunstmatig of geautomatiseerd worden verspreid" op grote schaal. Het eerste arrest van het Hof van Justitie op basis van deze bepaling verduidelijkte dat de inhoud gesponsord moet zijn, d.w.z. derden moet betalen om de verspreiding van informatie kunstmatig te vergroten, of dat het inhoud is die wordt gepromoot met behulp van geautomatiseerde instrumenten, zoals bots.⁵⁷⁹ Verder verbiedt Canada de publicatie van bepaalde valse verklaringen over politieke figuren met de bedoeling de verkiezingsuitslag te beïnvloeden.

Ten vijfde hebben verschillende regeringen nieuwe wettelijke **zorgplichten** opgelegd, of zijn ze voornemens om dergelijke wettelijke **verplichtingen op te leggen** aan internetdiensten om desinformatie tegen te gaan. Frankrijk heeft in dit verband een nieuwe verplichting tot samenwerking opgelegd aan grote internetdiensten, en in het Verenigd Koninkrijk en Canada zijn er voorstellen om wetgeving te creëren voor het opleggen van soortgelijke zorgplichten. Zo hebben in Frankrijk bepaalde online platforms op basis van Titel III van de Wet op de manipulatie van informatie van 2018 de verplichting om de verspreiding van valse informatie die de openbare orde kan verstoren of de oprechtheid van bepaalde verkiezingen kan wijzigen, tegen te gaan. De wetgeving *verplicht* platforms bepaalde mechanismen in te voeren om gebruikers in staat te stellen valse informatie te rapporteren, en omvat ook maatregelen die platforms kunnen invoeren, zoals het promoten van inhoud van bepaalde mediabedrijven. De Franse toezichthouder voor de media (*Conseil Supérieur de l'Audiovisuel*) geeft aanvullende richtlijnen voor de implementatie van deze maatregelen en de platforms zijn verplicht verslag uit te brengen aan deze toezichthouder. Naast het Franse voorbeeld zijn er twee soortgelijke voorstellen in het Verenigd Koninkrijk en Canada om een nieuw regelgevend kader te creëren met als doel illegale en schadelijke online-in-

578 Zie, Rosenberger, L. & Hanlon, B. "Countering Information Operations Demands A Common Democratic Strategy" (Alliantie voor het waarborgen van de democratie, 2019), <https://securingdemocracy.gmfus.org/countering-information-operations-demands-a-common-democratic-strategy/>.

579 Tribunal de grande instance de Paris, (ord. réf.), 17 mei 2019, Mme V. et M. O. (zie Blocman, A., 'First urgent application to block dissemination of a tweet under the Act on combating the manipulation of information', 2019, IRIS 2019-7, 14, <http://merlin.obs.coe.int/iris/2019/7/article14.en.html>).

houd, waaronder desinformatie, aan te pakken. Het centrale element van de voorstellen zou erin bestaan bepaalde internetdiensten een nieuwe wettelijke zorgplicht op te leggen om “redelijke maatregelen” te nemen om de veiligheid van de gebruikers te waarborgen en illegale en schadelijke activiteiten aan te pakken. Wat desinformatie betreft, zouden internetdiensten “evenredige en proactieve maatregelen” moeten nemen om de verspreiding van misleidende en schadelijke desinformatie tot een minimum te beperken en, wat van cruciaal belang is, “de toegankelijkheid van betrouwbare en gevarieerde nieuw-sinhoud te vergroten”. Belangrijk is dat de wettelijke zorgplicht door een onafhankelijke toezichthouder wordt gehandhaafd en dat de toezichthouder door middel van nieuwe gedragscodes uiteenzet hoe internetdiensten hun wettelijke taken moeten vervullen. Deze toezichthouder zou aanzienlijke handhavingsbevoegdheden hebben, waaronder boetes, en mogelijk de bevoegdheid om platforms te blokkeren als laatste redmiddel voor de handhaving.

Ten zesde, een andere specifieke beleidsoptie die uit de landenstudies naar voren komt, is nieuwe wetgeving die een onlineplatform verplicht om **duidelijk illegale inhoud** binnen 24 uur na ontvangst van een klacht te verwijderen. Illegale inhoud waar de wet op van toepassing is omvat een aantal strafbare feiten die momenteel van toepassing zijn op valse informatie: zoals laster, opzettelijke laster, belediging, smaad, belediging van godsdiensten en de verspreiding van propagandamateriaal. Dit systeem is in Duitsland ingevoerd via de veelbesproken NetzDG-wetgeving en bepaalt ook dat platforms “alle illegale inhoud” binnen zeven dagen moeten verwijderen of de toegang daartoe moeten blokkeren. De Duitse wetgeving maakt het overtreden van de wet strafbaar en er kunnen aan de platforms bestuurlijke boetes tot 5 miljoen euro worden opgelegd.

Ten zevende, sommige landen hebben wetgeving die gericht is op oneigenlijke **buitenlandse beïnvloeding**. Deze wetgeving wordt gebruikt om buitenlandse groepen die zich schuldig maken aan desinformatie te vervolgen.⁵⁸⁰ In de Verenigde Staten, bijvoorbeeld, verbiedt de Campagnefinancieringswet dat buitenlanders bijdragen of uitgaven doen voor bepaalde verkiezingen en verbiedt het individuen, groepen en partijen om een (onafhankelijke) uitgaven te doen of vergoedingen te geven voor bepaalde communicatie over verkiezingen. Ook in Canada is onlangs wetgeving aangenomen met betrekking tot de buitenlandse invloed op verkiezingen. De Wet Modernisering Verkiezingen verbiedt daar buitenlandse personen, bedrijven, groepen, partijen of overheden om de kiezers op ongepaste wijze te beïnvloeden door uitgaven te doen om een kandidaat of partij bij een verkiezing rechtstreeks te promoten of zich daartegen te verzetten.

Ten achtste zijn er ook nieuwe wetgeving en voorstellen met betrekking tot **bot- en geautomatiseerde softwareregulering**. In Californië is het nu bijvoorbeeld onwettig een bot te gebruiken om online met een andere persoon in Californië te communiceren met de bedoeling deze andere persoon te misleiden over zijn kunstmatige identiteit, specifiek met de intentie deze persoon te misleiden over de inhoud van de communicatie om op deze manier een verkiezing te beïnvloeden. Er rust echter geen verplichting op online platformen om ervoor te zorgen dat de gebruiker de inzet van bots bekendmaakt. In dit verband is er een voorstel op federaal niveau in de Verenigde Staten (*Bot Disclosure and Accountability Act*) om het gebruik van bots op sociale media te reguleren. Dit voorstel vereist dat de aanbieders van sociale media procedures in voeren die hun gebruikers te verplichten het gebruik van geautomatiseerde softwareprogramma's die bedoeld zijn om zich voor te doen als een imitatie of reproductie van menselijke activiteiten online openbaar te maken. De Amerikaanse toezichthouder voor consumentenbescherming - de Federal Trade Commission - zou worden belast met het definiëren van botsoftware en het toezicht op de naleving van de wet.

⁵⁸⁰ <https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html>.

Deze beleidsvoorbeelden kunnen als volgt worden samengevat:

1. *Mediageletterdheid*: mediageletterdheidsprogramma's om desinformatie tegen te gaan. Mogelijke verplichting voor een toezichthouder om een programma voor online mediageletterdheid op te zetten en een mogelijke verplichting voor internetdiensten om online mediageletterdheid te bevorderen.
2. *Financiering van de media (faciliterende omgeving voor de media)*: financieringsprogramma's ter ondersteuning van onafhankelijke media en van goed toegeruste publieke media. Zoals de Raad van Europa aanbeveelt, moeten de media te allen tijde over de middelen beschikken om hun taak te vervullen, zijnde het verschaffen van nauwkeurige en betrouwbare verslaggeving over zaken van algemeen belang, aangezien kwaliteitsjournalistiek en verslaggeving belangrijke instrumenten zijn om propaganda en desinformatie tegen te gaan.⁵⁸¹
3. *Gedragscodes*: zelfreguleringscode (of co-reguleringscode van de minister of toezichthouder) voor de aanpak van schadelijke inhoud op internetdiensten, met inbegrip van desinformatie. De code zou procedures bevatten voor het melden en verwijderen van schadelijke inhoud en desinformatie. De code zou in overleg met de belanghebbenden en het maatschappelijk middenveld worden goedgekeurd (bv. het Verenigd Koninkrijk).
4. *Wettelijke verplichting tot samenwerking*: een wettelijke verplichting tot samenwerking, waarbij de nadruk ligt op het verplicht stellen van bepaalde processen en structurele elementen. Deze verplichting wordt opgelegd aan de platforms om maatregelen te nemen tegen de verspreiding van valse informatie die de openbare orde kan verstoren of de integriteit van bepaalde verkiezingen kan aantasten. Specifieke maatregelen die zijn vastgelegd in een gedragscode die door de regelgevende instantie is uitgevaardigd (bv. Frankrijk).
5. *Wettelijke zorgplicht*: een wettelijke zorgplicht die aan platforms wordt opgelegd om redelijke maatregelen te nemen om ervoor te zorgen dat gebruikers veilig zijn en illegale en schadelijke activiteiten, waaronder desinformatie, worden aangepakt. Specifieke maatregelen worden in gedragscodes uiteengezet door de toezichthouder die de bevoegdheid heeft om boetes op te leggen en te streven naar een door de rechtbank voorgeschreven opheffing van de dienst (bv. in het Verenigd Koninkrijk).
6. *Platformverplichting om illegale inhoud te verwijderen*: leg platforms een verplichting op om illegale inhoud te verwijderen die op grond van bepalingen in het Wetboek van Strafrecht van toepassing is op valse informatie, zoals belediging, smaad, en het aanzetten tot haat (bijv. Duitsland).
7. *Door de rechtbank bevolen verwijdering van desinformatie*: gerechtelijke procedure om platforms te gelasten valse of misleidende informatie te verwijderen tijdens de verkiezingstijd, met termijnen voor procedures, bijvoorbeeld 48 uur (bijv. Frankrijk).

⁵⁸¹ Aanbeveling CM/Rec(2018)1 van het Comité van Ministers aan de lidstaten over mediapluralisme en transparantie van media-eigendom, paragraaf 1.4, bijlage.

8. *Bot software regelgeving*: regelgeving gericht op internetdiensten om procedures in te voeren om gebruikers te verplichten het gebruik van geautomatiseerde softwareprogramma's bekend te maken; of het criminaliseren van het gebruik van een bot op een sociaal netwerk met de bedoeling mensen te misleiden over de kunstmatige identiteit ervan met als uiteindelijk doel mensen bewust te misleiden over de inhoud van de communicatie om een verkiezing te beïnvloeden (bijv. Californië).
9. *Verbod op de publicatie van valse informatie*: nieuw strafbaar feit voor de publicatie van valse of misleidende informatie (bv. Frankrijk).
10. *Verbod onder buitenlandse invloed*: verbiedt buitenlandse individuen, groepen, partijen en regeringen om geld uit te geven aan verkiezingscampagnes (bijv. in de Verenigde Staten en Canada).
11. *Nationale veiligheid*: desinformatie behandelen als een nationale veiligheidskwestie en als onderdeel van een nationale veiligheidsstrategie (bv. Zweden, Verenigde Staten).

ii. Verkiezingstoezicht en desinformatie

De Europese Commissie heeft benadrukt dat desinformatie tijdens verkiezingen "bijzondere aandacht" vereist.⁵⁸² In dit verband is het van belang te verwijzen naar de rol van de OSCE, die toezicht houdt op verkiezingen in heel Europa, met inbegrip van verkiezingen in Nederland. Het OSCE-rapport over de Tweede Kamerverkiezingen van 2017 doet een aantal aanbevelingen met betrekking tot het toezicht op de verkiezingen, buitenlandse en anonieme donaties, het recht om in beroep te gaan tegen de verkiezingsuitslag en normen in het kader van internationale *best practices* voor vrije en eerlijke verkiezingen.⁵⁸³

Ten eerste merkte de OSCE op dat de Nederlandse wet niet voorziet in een mechanisme om een beroep te doen op een gerechtelijke instantie tegen het definitieve besluit van de Tweede Kamer over de verkiezingsuitslag, hetgeen "inconsistent" is met "OSCE commitments and international good practice".⁵⁸⁴ Ten tweede merkte de OSCE op dat buitenlandse donaties in Nederland zijn toegestaan en dat "contrary to good practice" anonieme donaties tot 1.000 euro zijn toegestaan. De Raad van Europa heeft ook aanbevolen dat staten specifiek de donaties van buitenlandse donoren moeten beperken, verbieden of anderszins reguleren.⁵⁸⁵

Voorts heeft het EHRM met betrekking tot het toezicht op de verkiezingen geoordeeld dat het bevoegd is om te beoordelen of de verkiezingen vrij en eerlijk zijn verlopen. Dit vloeit voort uit artikel 3 van Protocol nr. 1 bij het EVRM, dat de lidstaten van de RvE, waaronder Nederland, verplicht tot het houden van vrije verkiezingen "onder voorwaarden die de vrijheid van meningsuiting van de bevolking bij de keuze van de wetgever waarborgen".⁵⁸⁶ Het EHRM heeft namelijk geoordeeld dat het "principeel" bevoegd is om na te gaan of de media-aandacht voor de verkiezingen, en met name eventuele manipulatie van de media, ertoe heeft geleid dat de verkiezingen niet vrij en eerlijk zijn verlopen.⁵⁸⁷ Het Hof benadrukte ook dat de lidstaten een positieve verplichting van "procedurele aard" hebben om te zorgen voor een nationaal systeem met een doeltreffende behandeling van individuele klachten en beroepen in verband met het kiesrecht.⁵⁸⁸ In dezelfde zaak oordeelde het Hof dat de specifieke klacht over de ongelijke berichtgeving in de media over de verkiezingen door een onafhankelijke instantie was onderzocht en dat er een met

⁵⁸² Europese Commissie, 'Aanpak van online desinformatie: een Europese aanpak', blz. 11.

⁵⁸³ OSCE Office for Democratic Institutions and Human Rights, The Netherlands: Parliamentary Elections 15 March 2017, OSCE/ODIHR Election Assessment Mission Final Report, <https://www.osce.org/odihr/elections/netherlands/321821?download=true>.

⁵⁸⁴ *ibid.*, p. 16.

⁵⁸⁵ <https://rm.coe.int/16806cc1f1>.

⁵⁸⁶ Artikel 3 van Protocol nr. 1 bij het Europees Verdrag tot bescherming van de rechten van de mens.

⁵⁸⁷ *Communist Party of Russia and Others v. Russia* (Application no. 29400/05) 19 June 2012, r.o. 79.

⁵⁸⁸ *Ibid.*, para. 124.

redenen omkleed vonnis was gewezen, waarmee het systeem van beroepen over de verkiezingen dat was ingevoerd toereikend was om aan de positieve verplichting van de staat te voldoen.⁵⁸⁹

Hoewel het EHRM (nog) geen klachten over de online-verslaggeving van verkiezingen in overweging heeft genomen, suggereren de bovenstaande normen wel dat een belangrijk element is in het veiligstellen dat verkiezingen worden beschermd tegen online desinformatie, dat er een passend mechanisme is om ervoor te zorgen dat een onafhankelijke beroepsinstantie of rechtbank kan beoordelen of een verkiezing vrij en eerlijk is verlopen. De gedragscode van de Commissie van Venetië inzake verkiezingen bepaalt dat dit onafhankelijke orgaan bevoegd moet zijn de correcte naleving van de regels voor de verkiezingscampagne en de verkiezingsuitslag te controleren en dat het bevoegd moet zijn om verkiezingen nietig te verklaren wanneer onregelmatigheden de uitslag kunnen hebben beïnvloed.⁵⁹⁰ Dit mechanisme zou een belangrijke toetssteen zijn om na te gaan of de online desinformatie zo wijdverbreid is dat deze de verkiezingsuitslag heeft beïnvloed. Natuurlijk zou dit een ex post mechanisme zijn, en het proactief beschermen van verkiezingen tegen desinformatie is ook een belangrijke benadering. Een doeltreffend mechanisme voor de evaluatie van verkiezingen en de rol van online desinformatie in die verkiezingen, is echter even belangrijk.

iii. Politieke advertenties en desinformatie

Hoewel de kwesties van desinformatie en de regulering van de politieke advertenties aan elkaar gerelateerd zijn, moeten zij vanuit juridisch perspectief onderscheiden worden. Met name op EU-niveau worden de twee begrippen in de verschillende beleidsdocumenten onder één gebracht, in die zin dat geïmpliceerd wordt dat het aanpassen van de regelgeving voor politieke advertenties via internetdiensten ook de problemen rondom desinformatie zou adresseren. Daarentegen wordt nauwelijks melding gemaakt van politieke advertenties in de twee belangrijkste onafhankelijke rapporten van de EU en de Raad van Europa over desinformatie. In het rapport van de Raad van Europa worden politieke advertenties slechts één keer genoemd,⁵⁹¹ terwijl in het rapport van de HLEG van de EU slechts vermeld wordt dat één van de mogelijke kwetsbaarheden voor verkiezingen de ondoorzichtige verspreiding van politieke advertenties is.⁵⁹² Los daarvan moet verder worden erkend dat er nog steeds een gebrek is aan empirisch bewijs voor een koppeling van de problematiek rondom desinformatie aan politieke advertenties, en aan empirisch bewijs of het reguleren van politieke advertenties daadwerkelijk effect zal hebben op de omvang van de desinformatie. In dit verband schrijft de Europese Commissie dat “in most known cases” de desinformatie is vervat in “written articles, sometimes complemented by authentic pictures or audiovisual content taken out of context”.⁵⁹³

Een van de redenen voor een verschuiving van aandacht van het reguleren van desinformatie als zodanig naar het reguleren van politieke advertenties kan zijn dat dit laatste als praktisch haalbaarder en maatschappelijk beter te accepteren wordt beschouwd. Aanvankelijk werd het probleem van desinformatie besproken als een probleem van “nepnieuws”. Onafhankelijke rapporten van de EU en de Raad van Europa hebben echter gewezen op de misleidende werking en ontoereikende strekking van dit concept, dat wordt beschouwd als een “mechanism by which the powerful can clamp down upon, restrict, undermine and circumvent the free press”.⁵⁹⁴ Er volgden vele waarschuwingen van internationale speciale rapporteurs over de gevaren die verbonden zijn aan pogingen om “nepnieuws” te reguleren.⁵⁹⁵ Aangezien

589 Ibid., para. 124.

590 European Commission for Democracy Through Law, ‘Code of Good Practice in Electoral Matters’, par. 3.3, [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2002\)023rev2-cor-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev2-cor-e)

591 Wardle, C., & Derakhshan, H. ‘Information Disorder. Toward an interdisciplinary framework of research and policymaking’, z.p., 2017 p. 74.

592 HLEG, ‘A multi-dimensional approach to disinformation’, p. 13.

593 European Commission, Tackling online disinformation: a European Approach, COM(2018) 236 final, para. 2.2

594 See Report of the independent High level Group on fake news and online disinformation, A multi-dimensional approach to disinformation (European Commission, 2018), p. 10; and Claire Wardle and Hossein Derakhshan, Information Disorder: Toward an interdisciplinary framework for research and policymaking (Council of Europe, 2017), p. 5.

595 The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-opera-

veel van de risico's die aan dergelijke regelgeving verbonden zijn nog steeds bestaan met betrekking tot de verschillende vormen van desinformatie, is te verklaren dat de aandacht verschoven is naar een meer afgebakend onderwerp als politieke reclame als specifiekere reguleringsonderwerp.

Deze trend wordt bevestigd in de landenstudies, opgenomen als bijlage. Frankrijk is het enige land dat specifieke wetgeving over desinformatie heeft aangenomen (Frankrijk heeft ook jarenlang de publicatie van valse berichten strafbaar gesteld). Andere landen bespreken nieuwe mogelijke wettelijke kaders met betrekking tot desinformatie, bijvoorbeeld de "whitepaper" van de Britse regering over "online-harms".⁵⁹⁶ Het voorstel van het Verenigd Koninkrijk omvat een nieuwe wettelijke zorgplicht voor internetdiensten om schade als gevolg van inhoud of activiteiten op hun diensten aan te pakken, dit onder het toezicht van een (nieuwe) onafhankelijke regelgevende instantie. Het voorstel omvat de meer recente kwestie van desinformatie, maar is daarnaast gericht op de volledige breedte van illegale en schadelijke informatie op het internet. Commentatoren hebben gewaarschuwd voor de mogelijke negatieve gevolgen voor de vrijheid van meningsuiting: "[i]f platforms are required to prevent potentially harmful content from being posted, this incentivises widespread prior restraint".⁵⁹⁷

In contrast met het gebrek aan wetgeving met betrekking tot desinformatie zijn daarentegen in Canada, Frankrijk, Schotland, de Verenigde Staten (Californië, Maryland, New Jersey, New York, Nevada en Washington) wel voorbeelden te geven van wetgeving die specifiek gericht is op politieke advertenties. Deze maatregelen zijn vooral gericht op het waarborgen van (verschillende vormen van) transparantie (zie ook paragraaf 7.C hieronder). Dit hoewel de regulering van de politieke advertenties, met name de transparantievereisten, slechts betrekking heeft op een zeer specifiek deel van de problemen gerelateerd aan desinformatie.

Gezien de moeilijkheden gerelateerd aan de regulering van de problematiek van desinformatie en de reguleringskaders voor politieke advertenties, is het nuttig om een overzicht te geven van de problemen gerelateerd aan desinformatie zoals in kaart gebracht door de Europese Commissie, alsmede van de mogelijke gevolgen van transparantie met betrekking tot politieke advertenties voor deze problemen:

1. "Disinformation erodes trust in institutions and media, and harms democracies by hampering the ability of citizens to take informed decisions;
2. Disinformation often supports radical and extremist ideas and activities;
3. Disinformation campaigns are being widely used by a range of domestic and foreign actors to sow distrust and create societal tensions;
4. Disinformation campaigns by third countries can be part of hybrid threats to internal security, including election processes, in particular in combination with cyberattacks; and
5. Domestic and foreign actors can use disinformation to manipulate policy, societal debates and behaviour in areas such as climate change, migration, public security, health."⁵⁹⁸

In combinatie met deze problemen vergemakkelijken internetdiensten volgens de Europese Commissie de snelle en wijdverbreide verspreiding van desinformatie via verschillende mechanismen:

tion in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and "Fake News"', FOM.GAL/3/17, 3 March 2017.

596 Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department, 'Online Harms White Paper' 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf. See Peter Pomerantsev, The UK White Paper on Online Harms and the Dangers of Regulating Disinformation, Transatlantic Working Group on Content Moderation Online and Freedom of Expression, 1 October 2019, https://www.ivir.nl/publicaties/download/Cycle_Censorship_Pomerantsev_Oct_2019.pdf.

597 Jim Killock and Amy Shepherd, "UK: Online Harms Strategy must "design in" fundamental rights", EDRI, 10 April 2019, <https://edri.org/uk-online-harms-strategy-must-design-in-fundamental-rights/>.

598 European Commission, Tackling online disinformation: a European Approach, COM(2018) 236 final, para. 1.

- a. *“Algorithm-based*: algorithmic systems prioritise personalised and sensational content; facilitate the sharing of personalised content among like-minded users; and indirectly heighten polarisation and strengthen the effects of disinformation;
- b. *Advertising-driven*: digital advertising models reward sensational and viral content; and facilitate placement of advertisements on websites that publish sensationalist content appealing to user emotions, including disinformation; and
- c. *Technology-enabled*: online technologies such as automated services (bots) artificially amplify the spread of disinformation. These mechanics can be facilitated by simulated profiles (fake accounts) which have no authentic user behind them, sometimes orchestrated on a massive scale (troll factories).”⁵⁹⁹

Uit het bovenstaande blijkt duidelijk dat de potentiële schade die desinformatie kan aanrichten zeer ernstig is voor een democratische samenleving en dat internetdiensten de potentiële gevaren van desinformatie kunnen vergroten. Het reguleren van politieke advertenties zal echter, vooral wanneer deze regulering beperkt blijft tot politieke advertenties voor politieke kandidaten in enge zin, geen oplossing bieden voor de problemen gerelateerd aan (a) algoritmen of aan (b) digitale reclamemodellen. Het effect van het reguleren van politieke advertenties op (c) technologische amplificatie, door bots, nepaccounts of astroturfing, is afhankelijk van hoe breed de definitie van politieke advertenties is die wordt gehanteerd. Het beperken van bepaalde vormen van politieke advertenties kan ook tot meer problemen op andere gebieden leiden.

De grootste uitdaging met betrekking tot het reguleren van politieke advertenties is namelijk dat de advertenties weliswaar kunnen worden misbruikt voor het verspreiden van desinformatie, maar dat het over het algemeen een legitieme methode van politieke communicatie kan zijn die al vele jaren wordt gebruikt om het publiek te informeren. Bovendien wordt bij moderne politieke campagnes (en *grass-root* campagnes) gebruik gemaakt van de door internetdiensten aangeboden technologische amplificatiemethoden voor in een democratische samenleving volstrekt legitieme campagnes. En ten slotte kan een striktere regulering van betaalde politieke advertenties gemakkelijk leiden tot een verschuiving van gesponsorde communicatie naar organische contentstrategieën, wat betekent dat betaalde politieke advertenties niet simpelweg geïsoleerd kunnen worden bekeken. Deze punten moeten in aanmerking worden genomen bij de regulering van politieke advertenties. Een andere reden om voorzichtig te werk te gaan is het gebrek aan sterk empirisch bewijs waaruit blijkt dat er in Nederland op grote schaal gebruik wordt gemaakt van politieke advertenties om desinformatie te verspreiden.

Met het oog hierop is in dit rapport gedetailleerd ingegaan op de legitieme redenen die ten grondslag kunnen liggen aan, en de juiste beleidsopties die beschikbaar zijn voor een effectievere regulering van politieke advertenties op internetdiensten. Hierbij wordt deze kwestie geplaatst in de bredere discussie over de aanpak van desinformatie online. Het is echter belangrijk om in gedachten te houden dat de regulering van politieke advertenties niet kan worden verwacht veel van de uitdagingen in verband met desinformatie op te lossen. Bovendien moeten beperkingen op politieke advertenties zorgvuldig worden beoordeeld op hun doeltreffendheid, aangezien er andere manieren zijn waarop geld kan worden gebruikt om de effectieve verspreiding van politieke communicatie via internetdiensten te financieren, naast de specifieke kanalen voor gesponsorde communicatie.

⁵⁹⁹ Ibid., para. 2.2.

B. Beleidsniveaus voor het reguleren van desinformatie en politieke advertenties

Het huidige juridische en beleidsmatige kader voor de regulering van politieke advertenties en desinformatie in Nederland en de aanpak van desinformatievraagstukken in dit verband betreft wetgeving en beleid op drie samenhangende niveaus:

- Het Europese wettelijke kader voor relevante internetdiensten en handelspraktijken met betrekking tot (politieke) advertenties en onlinecommunicatie in het algemeen. Dit kader bestaat uit relevante EU-wetgeving (met inbegrip van beperkingen van de aansprakelijkheid voor tussenpersonen, transparantievereisten voor commerciële communicatie, regelgeving inzake direct-marketing in elektronische communicatie, een afzonderlijk pakket verplichtingen voor audiovisuele mediadiensten en wetgeving inzake gegevensbescherming). Bovendien gaat het om de bescherming van de grondrechten in de context van de EU en de Raad van Europa, met name het recht op vrijheid van meningsuiting. Opmerkelijk in dit verband is dat de EU ook een toonaangevend forum is voor zelfregulering en co-regulering van internetdiensten op het gebied van desinformatie, waarbij ook de transparantie van politieke advertenties een rol speelt.
- Het nationale juridische en beleidsniveau in Nederland betreft ten eerste de implementatie en handhaving van relevante Europese regelgeving, waarbij een aantal onafhankelijke toezichthouders, waaronder de ACM, het Commissariaat van de Media en de Autoriteit Persoonsgegevens, mede zijn betrokken. Van bijzonder belang voor de Nederlandse wetgevingsagenda gerelateerd aan desinformatie en politieke advertenties die tot de kern- of uitsluitende bevoegdheid van Nederland blijven behoren, bijvoorbeeld het functioneren van verkiezingen en de nationale veiligheid.
- Het beleidsniveau van de private sector, dat bestaat uit het ontwerpen en aanbieden van methoden om (des)informatie snel te verspreiden en het aanbieden van (politieke) advertentiemogelijkheden in het kader van internetdiensten. Dit beleidsniveau omvat de bijbehorende definities en het beleid van de betrokken ondernemingen, onder meer door middel van contractuele bepalingen, zelfregulering in de sector, informatieverstrekking en handhaving.

Zoals duidelijk blijkt uit hoofdstuk 5 en 6, zijn er, ondanks het feit dat er een breed scala aan verschillende wetten van toepassing is, in Nederland geen specifieke regels met betrekking tot online desinformatie en politieke advertenties. Met betrekking tot online politieke advertenties, illustreren de landenstudies ook dat Nederland zich, samen met Zweden, onderscheidt in het relatieve gebrek aan regelgeving op het gebied van politieke advertenties in het algemeen. Wij zien dit niet als het resultaat van een trage reactie op de nieuwe dynamiek van media- en technologische ontwikkelingen. Nederland is een land dat van oudsher weinig regelgeving heeft op het gebied van politieke advertenties, in tegenstelling tot Zweden dat nog maar tien jaar geleden de politieke advertenties via de omroep heeft gedereguleerd (zie de studie over Zweden in de bijlage).⁶⁰⁰ Dit gebrek aan regelgeving kan, althans gedeeltelijk, worden verklaard door de in het Nederlandse politieke systeem dominante opvatting dat de regering zich moet onthouden van inmenging in politieke partijen en het politieke debat in de samenleving.⁶⁰¹ Daarnaast kunnen bepaalde vormen van regulering en co-regulering het gevaar met zich meebrengen dat internetdiensten worden gestimuleerd om politieke communicatie te beperken op een manier die de politieke expressie onnodig beperkt en pluralisme schaadt. Dit gevaar bestaat ook in verband met de huidige ontwikkelingen op EU-niveau en deze moeten vanuit dit oogpunt kritisch worden gevolgd, alsmede vanuit het vereiste dat inmenging met de vrijheid van meningsuiting bij wet moet worden voorgeschreven.

⁶⁰⁰ Johansson, B., 'Sweden: Ten Years with Television Advertising' in: Holtz-Bacha, C. & Just, M.R. (eds), 'Routledge Handbook of Political Advertising', Routledge, 2017, p. 271.

⁶⁰¹ Evaluatie- en adviescommissie Wet Financiering politieke partijen, 'Het publieke belang van politieke partijen', 2018, p. 18-19.

Het onderzoek heeft echter ook duidelijk aangetoond dat er een breed scala aan regels bestaat die op verschillende manieren van toepassing zijn op desinformatie en online politieke advertenties. Dit rechtskader wordt vooral gekenmerkt door zijn diversiteit en het feit dat het veel verschillende rechtsgebieden en -instrumenten omvat. Dit relevante wettelijke kader voor de juridische status en het beheer van online desinformatie en politieke advertenties dat uit hoofdstuk 5 en 6 naar voren komt, kan ook worden bekeken door de lens van de volgende inhoudelijke juridische gebieden:

1. Het grondrechtelijk kader, in het bijzonder de vrijheid van meningsuiting;
2. De algemeen geldende inhoudelijke beperkingen op de uitingsvrijheid en verspreiding van online inhoud in het privaats- en strafrecht;
3. Strafrechtelijke bepalingen met betrekking tot de veiligheid en integriteit van informatiesystemen (cybercriminaliteit);
4. Zelfregulering die relevant is voor desinformatie en (politieke) reclame, waaronder de "Nederlandse Reclame Code" en zelfregulering met betrekking tot journalistiek;
5. Beperking van de aansprakelijkheid voor de activiteiten van tussenpersonen;
6. Zelf- en co-reguleringsinstrumenten op Europees niveau met verantwoordelijkheden op het gebied van internetdiensten, waaronder de EU-gedragscode inzake desinformatie;
7. Beperkingen op direct marketing via elektronische communicatiediensten;
8. De regulering van de verzameling en het gebruik van persoonsgegevens in online manipulatie, *microtargeting* en (politieke) advertenties;
9. Audiovisueel media(diensten)recht;
10. Regelgeving met betrekking tot (commerciële) advertenties, inclusief transparantie-vereisten, waarvan er momenteel slechts enkele van toepassing zijn op politieke advertenties;
11. Nationale veiligheidswetgeving;
12. Transparantie en toezicht in de wetgeving inzake de financiering van politieke partijen;

Het op deze manier indelen van het relevante juridische kader dat in dit rapport wordt geanalyseerd, maakt inzichtelijk welke gebieden op nationaal niveau kunnen worden aangepakt. Er zijn verschillende gebieden waarop Nederland de mogelijkheid heeft om wetgeving te creëren die (delen van) de problemen met betrekking tot online politieke advertenties aanpakt. Het tweede gebied, dat betrekking heeft op de algemeen geldende inhoudelijke beperkingen van de meningsuiting in het privaats- en strafrecht, bestaat bijvoorbeeld uit het nationale recht, ook al worden de buitengrenzen gevormd door het kader van de grondrechten. Aanvullingen op, of wijzigingen van, dit algemene kader op nationaal niveau kunnen mogelijk grote gevolgen hebben voor de verspreiding van desinformatie en online politieke advertenties. Dergelijke veranderingen in dit meer algemene kader moeten echter worden overwogen vanuit het perspectief van desinformatie en illegale en schadelijke online-inhoud meer in het algemeen, en niet op basis van de daarmee samenhangende, maar wel specifieke kwestie van politieke advertenties.

De Europese Commissie bereid momenteel een grondige herziening voor van het algemene kader voor de aansprakelijkheid van tussenpersonen op het internet (gebied 5 en aanverwant gebied 6). De reikwijdte van de "safe harbour" voor hosting, de status van (politieke) advertenties in het kader van dergelijke regels, internetmarktmechanismen zoals het land-van-oorsprongbeginsel en inhoudsmatiging en kennisgevings- en actienormen zullen hier naar verwachting deel van uitmaken. De herziening van de richtlijn kan ook een herziening van de transparantievereisten voor commerciële communicatie inhouden, zodat de verplichting voor internetdiensten om een duidelijk onderscheid te maken tussen organische en gesponsorde communicatie mogelijk verder wordt verduidelijkt. De aansprakelijkheid en verantwoordelijkheid van internetdiensten voor communicatie en activiteiten van derden, met inbegrip van desinformatie, moeten tegen de achtergrond van deze regels en ontwikkelingen worden geplaatst.

De zelfreguleringsinstrumenten op nationaal niveau (gebied vier) vallen volledig binnen het nationale beleidsniveau. Dat is vooral relevant gezien het feit dat zelfregulering een dominante vorm is waarmee desinformatie en politieke advertenties in Nederland wordt genormeerd. Met betrekking tot internet-diensten is het echter van belang op te merken dat de zich ontwikkelende zelfregulering niet specifiek geïnformeerd is door of afgestemd is op de specifieke situatie in Nederland. Dit kan worden beschouwd als een specifieke uitdaging voor effectieve regelgeving, die een voorbeeld is van de veel bredere uitdaging om ervoor te zorgen dat internationaal opererende internetdiensten aan te spreken zijn op de specifieke lokale effecten van het gebruik van hun diensten.

Een ander gebied dat op nationaal niveau wordt genormeerd, is de nationale veiligheidswetgeving (gebied 11), aangezien de EU op dit gebied geen wetgevende bevoegdheid heeft. Hetzelfde geldt voor de Wet op de Financiering van Politieke Partijen. Deze heeft betrekking op de nationale politieke partijen en moet daarom op nationaal niveau worden gereguleerd (gebied 12).

Ten slotte wordt een groot deel van de EU-wetgeving tot stand gebracht in de vorm van richtlijnen die nationale implementatie behoeven of verordeningen die ook toezicht en handhaving op nationaal niveau vereisen. Dit geeft de rijksoverheid en relevante toezichthouders in Nederland ruimte voor een specifieke invulling die aansluit bij de nationale context. Sommige Nederlandse toezichthouders, zoals de AP, zijn begonnen met het verkennen van het terrein van politieke advertenties vanuit hun perspectief, maar deze acties staan nog in de kinderschoenen en zouden gebaat zijn bij een betere coördinatie en het bundelen van relevante expertise en middelen.

C. Landenstudies en beleidsvoorbeelden

In de uitgevoerde landenstudies wordt gedetailleerd beschreven hoe er nieuwe wetgeving is ontwikkeld voor politieke advertenties verspreid via internetdiensten. Hier zijn een aantal punten van belang. Ten eerste betreft het voornamelijk wijzigingen in de kieswetgeving (bijvoorbeeld de Franse Kieswet of de Political Reform Act uit Californië), en veel van de nieuwe regels zijn *beperkt tot de verkiezingsstijd*. Er is geen wetgeving tot stand gekomen die politieke advertenties buiten de verkiezingsperiode in het algemeen regelt. Zelfs de Franse wetgeving, die het meest verstrekkend is, is alleen van toepassing in de maanden voorafgaand aan een verkiezing.

Verder heeft de wetgeving vooral betrekking op de bescherming van verkiezingen en niet zozeer op de bescherming tegen desinformatie in het algemeen. Anders zou de regelgeving immers niet beperkt blijven tot verkiezingsperioden. Dit verklaart ook waarom een deel van de wetgeving alleen betrekking heeft op politieke advertenties die gericht zijn op een politieke kandidaat of partij, en niet op politieke advertenties over een kwestie van openbaar belang (ook wel issue-advertising genoemd). Ten derde is er een breed scala aan vormen van regelgeving: van geen regels, regels voor openbaarmaking, tot een verbod op betaalde politieke advertenties. De meest voorkomende vorm van regelgeving bestaat uit transparantieplichtingen.

Uit een analyse van de bestaande wet- en regelgeving met betrekking tot betaalde politieke advertenties, onder meer via de landenstudies, volgen een aantal beschikbare beleidsopties, variërend van disclaimer-regels tot een totaal verbod op betaalde politieke advertenties:

1. Transparantieregels die zich richten op wie voor een advertentie heeft betaald (zie Frankrijk, Schotland, Californië en Maryland). Deze regels kunnen worden opgelegd aan de persoon die het bericht plaatst, zoals in Californië, waar politieke advertenties een disclaimer vereisen over wie ervoor betaald heeft. Of regels die kunnen worden opgelegd aan de internetdiensten zelf, zoals in Canada.

2. Transparantieregels die gericht zijn op persoonsgegevens die worden gebruikt bij het richten van een advertentie (zie Frankrijk). Deze regels kunnen worden opgelegd aan internetdiensten, zoals de Franse wet op de manipulatie van informatie van 2018, die voor gebruikers transparante informatie vereist over het gebruik van persoonsgegevens in het kader van gesponsorde politieke inhoud.
3. Transparantieregels gericht op het archiveren van politieke advertenties (zie Canada, Californie en Maryland). Op grond van Canada's Elections Modernization Act zijn internetdiensten verplicht om een register te publiceren van alle partijdige reclameboodschappen en verkiezingsreclame. Men kan zich ook een niet-openbare bewaarplicht voor relevante diensten voorstellen.
4. Regels voor de financiering van campagnes die gericht zijn op de verplichting om verslag uit te brengen over de uitgaven voor onlinecampagnes (zie het Verenigd Koninkrijk en Canada). Deze optie kan gericht zijn op politieke partijen en campagnegroepen, in plaats van op internetdiensten. Het kan transparantie brengen in de uitgaven van groepen die zich bedienen van astroturen en het betalen van natuurlijke personen voor het verspreiden van informatie.⁶⁰²
5. Campagnefinancieringsregels die buitenlandse uitgaven voor verkiezingsreclame verbieden (zie Canada). Deze optie kan gericht zijn op buitenlandse individuen en groepen en kan ook worden toegepast op internetdiensten. Canada's Elections Modernization Act verbiedt de verkoop van advertentieruimte (inclusief online platforms) voor verkiezingsreclame aan buitenlandse partijen, groepen of overheden.
6. Verbod op betaalde politieke advertenties tijdens de verkiezingen (zie Frankrijk). Het verbod van de Franse kieswet op betaalde politieke advertenties tijdens de verkiezingen strekt zich uit tot online communicatie.
7. Het verbieden van betaalde politieke advertenties tijdens en buiten de verkiezingstijd. Deze optie bestaat alleen in de nationale voorschriften voor de omroepsector.

Om te bepalen of deze verschillende beleidsopties eventueel in Nederland kunnen worden uitgevoerd, moet rekening worden gehouden met de volgende perspectieven.

Voordat de verschillende beleidsinstrumenten op hun merites kunnen worden beoordeeld, moet eerst worden vastgesteld welke problemen deze maatregelen precies zullen worden aangepakt. Er bestaat een relatief brede consensus, ook in Nederland, dat een gebrek aan transparantie in politieke reclames een kwestie is die moet worden bekeken en aangepakt. Tegelijkertijd is vooralsnog niet goed empirisch vastgesteld in hoeverre er in Nederland sprake is van een problematische situatie ten aanzien van politieke advertenties en of het huidige (gebrek aan) een wettelijk kader met betrekking tot online politieke reclame, waaronder het ontbreken van specifieke regels over transparantie, een prangend probleem vormt. Toch suggereren de internationale normen voor de vrijheid van meningsuiting, specifiek voor politieke reclame tijdens verkiezingen, dat regeringen (op maat gesneden) transparantiemaatregelen voor betaalde politieke reclame invoeren.⁶⁰³

En daarnaast kunnen de enkele mogelijkheid dat politieke reclame wordt gebruikt voor de verspreiding van desinformatie, alsmede de mogelijkheid dat betaalde politieke reclame wordt gemaakt zonder dat duidelijk is wie betaalt om kiezers te beïnvloeden bij Nederlandse verkiezingen, als een probleem worden beschouwd. In de bredere context van het debat over de afhankelijkheid van digitale infrastructuur⁶⁰⁴ kunnen beleidsmaatregelen gerechtvaardigd zijn die erop gericht zijn de gereedheid te waarborgen om bedreigingen van de democratie op het gebied van politieke reclame (en desinformatie in het algemeen)

⁶⁰² See also, Yochai Benkler, *Election Advertising Disclosure: Part 1*, Harvard Law Review Blog, 31 October 2017, <https://blog.harvardlawreview.org/election-advertising-disclosure-part-1/>.

⁶⁰³ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Human Rights Council, A/HRC/26/30, 2 July 2014, para. 82, <https://undocs.org/A/HRC/26/30>.

⁶⁰⁴ See in het bijzonder het recente WRR rapport 'Voorbereiden op Digitale Ontwrichting', September 2019.

aan te pakken. Dergelijke maatregelen moeten ook worden overwogen gezien de bredere noodzaak om de bestaande informatie asymmetrie van overheden en regelgevers met betrekking tot relevante internetdiensten aan te pakken. Op dit moment lijkt de informatiepositie van de Nederlandse overheid ten aanzien van de nieuwe dynamiek die wordt gefaciliteerd door een handvol dominante internetdiensten en de maatschappelijke effecten daarvan, gehinderd te worden door fragmentatie (naast de complexiteit van het onderliggende fenomeen). Academisch en journalistiek onderzoek naar de democratische impact van internetdiensten stuit tevens op aanzienlijke beperkingen in de juridische (beschikbaar gestelde) informatie. Dit zijn echter bredere problemen die een bredere discussie en oplossingen vereisen.

Gezien het belang van een vrij politiek debat en de uitgebreide bescherming van de politieke meningsuiting, moet de impact van een eventuele beleidsoptie op het recht op vrijheid van meningsuiting grondig worden onderzocht. Vanuit het oogpunt van subsidiariteit en proportionaliteit in verband met artikel 10 EVRM betekent dit ook dat de voorkeur moet worden gegeven aan maatregelen die niet aan de inhoud van politieke advertenties raken of het pluralisme in de Nederlandse mediaomgeving dreigen te schaden. Transparantieregels zijn zo'n inhoudsneutrale maatregel. Maar zelfs deze transparantieregels moeten zeer doelgericht, voldoende duidelijk en proportioneel zijn. De overkoepelende overweging vanuit het perspectief van de vrijheid van meningsuiting moet hierbij zijn dat dergelijke maatregelen, indien nodig geacht, zodanig worden ontworpen dat het risico van (zelf)censuur, hetgeen het democratisch debat kan beïnvloeden, te beperken.

Het is dus van cruciaal belang om te benadrukken dat politieke reclame en betaalde politieke communicatie in het algemeen, een vorm van politieke expressie is. Politieke reclame kan niet op dezelfde manier worden gereguleerd als commerciële reclame. Terwijl de mogelijkheden om de commerciële communicatie te beperken talrijker zijn, is de regulering van de politieke reclame aan een strengere regeling door de vrijheid van meningsuiting worden onderworpen. Politieke reclame is grotendeels overgelaten aan de markt en zelfregulering. De media- en reclamediens ten omgeving bevatten de facto veel meer vrijwillige beperkingen voor politieke reclame dan voor commerciële communicatie, waarvan de regulering beter is verankerd in de relevante wetgeving inzake consumentenbescherming en mediawetgeving.

Het onderscheid tussen de regulering van politieke en commerciële reclame is ook relevant in de samenwerking tussen het nationale en Europese beleidsniveau. Politieke reclamemogelijkheden via internetdiensten worden in feite beheerst door een reeks van bestaande wettelijke kaders die verschillende aspecten adresseren. Een aanzienlijk deel van de lacunes in de regelgeving en van de bestaande problemen wordt momenteel op EU-niveau actief bestudeerd.

Terwijl de harmonisatie van de wetgeving inzake commerciële communicatie logischerwijs voortvloeit uit het project van de Europese interne markt, bestaat er geen sterke traditie voor de regulering van de politieke reclame op Europees niveau. Het verband tussen politieke reclame in enge zin en (nationale) verkiezingen is een deel van de verklaring hiervoor. Voor politieke reclame in brede zin impliceert de diversiteit van de politieke en democratische culturen in Europa ook dat de EU idealiter een ondersteunende en faciliterende rol blijft spelen. Een dergelijke rol is met name nodig gezien de verspreiding van online politieke reclame via onlinediensten die de nationale of Europese grenzen overstijgen.

Tot slot heeft Nederland geen relevante geschiedenis van het reguleren van politieke advertenties en met deze lange traditie van ongehinderde campagnes voor politieke partijen, maatschappelijke organisaties en individuen moet rekening worden gehouden bij het overwegen van regulering voor online politieke advertenties. De invoering van relatief restrictieve regelgeving, zoals die al bestaat in landen met een langere geschiedenis van regulering van politieke reclame (bv. Frankrijk), lijkt een ongerechtvaardigde afwijking van deze traditie.

Met dit in het achterhoofd komt het volgende beeld naar voren: optie 4 en 5 zouden geschikt kunnen zijn

voor implementatie in Nederland, optie 1 en 3 kunnen beter op EU-niveau worden opgepakt en optie 6 en 7 zijn te restrictief voor Nederland. Optie 2 is niet urgent gezien de toepasbaarheid van de AVG en het onafhankelijke toezicht door de Autoriteit Persoonsgegevens. De belangrijkste uitdaging op dit gebied is om ervoor te zorgen dat de betrokken autoriteiten over de capaciteit en deskundigheid beschikken om een dergelijk toezicht doeltreffend uit te oefenen en op de hoogte blijven van nieuwe ontwikkelingen.

Beleids optie 4 bestaat uit het opstellen van regels voor campagnefinanciering die gericht zijn op de verplichting om verslag uit te brengen over de uitgaven voor online campagnes. Het is gericht op de nationale politieke partijen en kan als zodanig het beste op Nederlands nationaal niveau worden geïmplementeerd. Transparantie in de uitgaven van politieke partijen voor onlineadvertenties biedt de mogelijkheid om meer inzicht te krijgen in de omvang van de praktijk en ook de mogelijkheid van democratische controle op het gebruik ervan. De maatregel wijkt minimaal af van de huidige regelgeving, aangezien politieke partijen al verplicht zijn om een gedetailleerde administratie te voeren en regelmatig verslag uit te brengen aan de overheid.⁶⁰⁵ Het vormt ook een minimale beperking van de vrijheid van meningsuiting. Al deze factoren wijzen erop dat het creëren van transparantie-eisen voor politieke partijen in Nederland met betrekking tot hun uitgaven voor online politieke reclame goed zou passen in het huidige regelgevingslandschap en waardevol inzicht zou kunnen bieden in het daadwerkelijke gebruik van online politieke advertenties. Samengevat biedt dit rapport ondersteuning voor het advies van de commissie over het Nederlandse parlementaire systeem en het voornemen van de regering om deze transparantie-eis in de “Wet op de Politieke Partijen” te implementeren.⁶⁰⁶

Op basis van dezelfde redenering kunnen delen van beleids optie 5 in de nieuwe wet worden geïmplementeerd. Zoals besproken in hoofdstuk 6 is de regering al van plan om in het kader van de herziening van de “Wet financiering politieke partijen” een verbod op buitenlandse giften aan politieke partijen in te voeren. De uitbreiding van het verbod tot buitenlandse uitgaven voor verkiezingsreclame in het algemeen kan als een te grote stap voor de Nederlandse situatie worden beschouwd, nu momenteel regelgeving op dit punt geheel ontbreekt. Daarbij weerspiegelt de activiteit van buitenlandse actoren bij nationale verkiezingen deels een wereld waarin veel politieke kwesties van transnationale aard zijn. Ook staat niet vast dat de buitenlandse uitgaven bij de Nederlandse verkiezingen een substantieel probleem vormen dat een verbod rechtvaardigt. Ook beleids opties 6 en 7 vormen voor Nederland een te grote stap, gezien de strenge en uitgebreide regelgeving die deze beleids opties met zich meebrengen. Ook hier is het niet duidelijk dat een dergelijke vergaande beperking van de vrijheid van meningsuiting in de Nederlandse context evenredig is.

⁶⁰⁵ Zie artikel 21 Wet financiering politieke partijen.

⁶⁰⁶ Tweede Kamer, vergaderjaar 2018-2019, 32 752, nr. 54; Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 10, p. 10-12. Staatscommissie parlementair stelsel, *'Lage Drempels, Hoge Dijken. Democratie en rechtstaat in balans'* Den Haag 2018, bijlage bij Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 9.

8. Samenvatting en conclusies

A. Context & onderzoekopdracht

De verspreiding van desinformatie is de laatste jaren een steeds duidelijkere zorg geworden, ook in Nederland. Het is van belang deze zorg kort te contextualiseren. Een aantal structurele oorzaken dragen namelijk bij aan dit fenomeen. Zo heeft het maatschappelijk debat en de daarmee samenhangende informatie en communicatie zich steeds meer verplaatst naar kanalen waar geen sprake is van (of zelfs geen mogelijkheid bestaat tot) actieve controle door relevante diensten op de inhoud en integriteit van communicatie, of op de daarbij betrokken processen en actoren. Los van de vragen die spelen ten aanzien van het functioneren van redactionele media en de journalistiek, roept het functioneren van internetdiensten vragen op. Bedrijfsmodellen kunnen ertoe leiden dat het vasthouden van de aandacht van gebruikers zwaarder weegt dan journalistieke, wetenschappelijke of vergelijkbare op het publiek debat gerichte kwaliteits- en integriteitscriteria voor informatie en communicatie. Internetdiensten zullen er verder doorgaans op gericht zijn om op zo groot mogelijke schaal hun diensten aan te bieden, en met een zo klein mogelijke investering eventuele maatschappelijke schade te adresseren.

Een deel van de problematiek is gelegen in de vergaande nieuwe mogelijkheden tot beïnvloeding van het publiek die door internetdiensten geboden worden. Daaronder vallen nieuwe kanalen voor communicatie en data-gestuurde mogelijkheden tot beïnvloeding. Het is duidelijk dat dit relatief open media- en communicatielandschap ook nieuwe mogelijkheden biedt voor oneigenlijke beïnvloeding door binnenlandse alsmede door buitenlandse, waaronder statelijke, actoren. De oorzaak van desinformatie kan ten slotte niet slechts gezocht worden in economische of technische factoren. Deze oorzaak is deels gelegen in hierdoor gefaciliteerde sociale processen, waaronder een sterke polarisatie van het politieke speelveld, en als ondemocratisch te kwalificeren communicatiegedrag.

Het een en ander heeft geleid tot een roep vanuit de politiek om meer helderheid over het reguleringskader voor de verspreiding van desinformatie. Dit onderzoek is voortgekomen uit deze oproep. Aan het onderzoek liggen een zevental door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties voorgelegde onderzoeksvragen ten grondslag. De vragen variëren van heel algemeen naar zeer specifiek, en zien alle in essentie op de vraag naar het bestaande juridische kader. De opdracht voor dit onderzoek is gegeven in het kader van het bredere beleid van de regering ter bescherming van de democratie tegen desinformatie. Uitgangspunt van dit beleid zijn de rechtsstatelijke waarden en grondrechten waaronder de vrijheid van meningsuiting en vrijheid van de pers. De doelstelling is “de stabiliteit en kwaliteit van onze democratische rechtsorde en onze open samenleving te beschermen, met inbegrip van de vrijheid van meningsuiting en pers.”⁶⁰⁷ De voorgelegde onderzoeksvragen luiden als volgt:

1. Welke huidige wet- en regelgeving bestaat er gericht op/gerelateerd aan het tegengaan van verspreiding van (des)informatie, en specifiek voor/door tech bedrijven?
2. Welke eisen stelt de wet- en regelgeving aan de verspreiding van informatie? Zijn deze techniekonafhankelijk beschreven?
3. Hoe houdt de huidige wet- en regelgeving rekening met de transparantie van de herkomst van informatie op sociale mediaplatforms? Worden hier grenzen gesteld aan eventuele buitenlandse invloeden, bijv. t.a.v. het plaatsen van politieke advertenties (motie Asscher/Vd Molen)?
4. Welke toezichtmogelijkheden en sanctionering biedt de wet- en regelgeving ten aanzien van online manipulatie (motie Asscher/Vd Molen, 62)?

⁶⁰⁷ Tweede Kamer, 2019-202, 30 821, nr. 91 Kamerbrief ‘beleidsinzet bescherming democratie tegen desinformatie’.

5. Zou bewuste online manipulatie onder de delictsomschrijvingen in het strafrecht inzake het manipuleren van verkiezingen kunnen worden gebracht? (motie Asscher- Van der Molen, Kamerstukken II, 2018/19, 30821, nr. 68).
6. Welke betekenis heeft de rechtsvorm voor de maatregelen die techbedrijven kunnen of moeten nemen t.a.v. content-moderatie, bevorderen van transparantie en bescherming rechten van burgers? Wat is de verantwoordelijkheid van techbedrijven voor de verspreiding via hun zoekmachines, sociale platforms e.d.?
7. Hoe zijn de rechten van burgers beschermd tegen bewuste misleidende informatie? Ook in het kader van gebruik van persoonsgegevens (privacy) en vrijheid van meningsuiting (ook t.a.v. verwijderen van content).

Deze vragen en de manier waarop dit rapport de vragen heeft geadresseerd vergen toelichting. Zo hanteert dit rapport de definitie van desinformatie zoals geformuleerd door de Europese Commissie, als "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". Er is voor gekozen deze brede Europese definitie te volgen, en niet de nauwere definitie van de Nederlandse overheid, aangezien deze bredere definitie zich beter leent voor het maken van een omvattende analyse van het zich ontwikkelende juridisch kader voor desinformatie. Vervolgens wordt, in plaats van de term "techbedrijven", in dit onderzoek de term "internetdiensten" gebruikt om een analyse te maken van het juridisch kader voor bedrijven die een relevante rol spelen in de verspreiding van (des)informatie. Het gaat hier om een breed scala aan verschillende diensten, waaronder sociale media, zoekmachines en communicatiediensten, waaronder *direct messaging* diensten. In juridische termen gaat het om diensten van de informatiemaatschappij, zogenaamde *hosting* diensten met beperkte aansprakelijkheid, elektronische communicatiediensten of audiovisuele mediadiensten.

In het volgende wordt allereerst stilgestaan bij de wijze waarop de onderzoeksvragen in het rapport zijn beantwoord. Daaropvolgend worden per hoofdstuk van het rapport de conclusies besproken. Daarna volgt een verdere verdieping van deze conclusies en de aanbevelingen van dit rapport.

Vraag 1 verzoekt in essentie om een overzicht van het wettelijk kader wat van toepassing is op (des) informatie, en in het bijzonder wanneer verspreid via internetdiensten. **Vraag 2** is nauw verwant aan de eerst vraag. Waar vraag 1 om een overzicht van de relevante wetgeving vraagt, richt vraag 2 zich primair op de inhoud van deze wetgeving. Uit de uitgevoerde analyse blijkt, in de eerste plaats, dat er in Nederland geen wet- of regelgeving bestaat die specifiek desinformatie als onderwerp heeft, zoals bijvoorbeeld in Frankrijk wel het geval is. In de tweede plaats is het wettelijke kader dat wel van toepassing is zeer breed. Het doorsnijdt de klassieke rechtsgebieden van het privaatrecht, het strafrecht, en de grondrechtelijke bescherming. Het omvat ook sector specifieke wetgeving, waaronder het media- en telecommunicatierecht. Waar bij de verspreiding van (des)informatie gebruik gemaakt wordt van persoonsgegevens is ook het recht op de bescherming van persoonsgegevens van toepassing. Het overzicht van de relevante wetgeving is gegeven in hoofdstuk 4 (grondrechtelijk kader), hoofdstuk 5 (Europese regelgeving, alsmede Nederlandse implementatie) en hoofdstuk 6 (nationale regelgeving). In dit overzicht is steeds de vraag naar de juridische positie van verschillende soorten internetdiensten meegenomen, alsmede het vraagstuk naar de aansprakelijkheid en verantwoordelijkheid van zogenaamde internet tussenpersonen voor onrechtmatige en/of schadelijke inhoud.

Vraag 3 richt zich specifiek op het bestaan van transparantie verplichtingen voor sociale mediadiensten met betrekking tot de herkomst van informatie. Er zijn verschillende juridische transparantie verplichtingen, voornamelijk ten aanzien van commerciële communicatie. Het betreft normen die zich richten op de primaire bron van de informatie. Deze verschillende normen worden in hoofdstuk 5 en 6 besproken. In hoofdstuk 4 wordt ook uitgebreid stilgestaan bij de mogelijkheid van transparantie vereisten vanuit het perspectief van de vrijheid van meningsuiting en de bescherming van pluriformiteit. Vervolgens worden

de algemene wet- en regelgeving met betrekking tot buitenlandse invloeden en de nationale veiligheid in hoofdstuk 4 en hoofdstuk 6.C besproken. Vraag 3 kijkt ook naar politieke advertenties in het bijzonder. Er bestaat geen Nederlandse regulering op het gebied van transparantie over politieke advertenties. Hoofdstuk 5 bespreekt de relevante zelfregulering welke door een aantal aanbieders van sociale media is overeengekomen op Europees niveau. Deze zelfregulering omvat tevens regels over de transparantie ten aanzien van de herkomst van politieke advertenties. Hoofdstuk 7 bespreekt uitgebreid de verschillende opties voor betreft transparantieverplichtingen voor politieke advertenties op basis van de landenrapportages.

Vraag 4 richt zich op de toezichts- en handhavingsmogelijkheden ten aanzien van online manipulatie. Onder deze laatste term wordt verstaan het via technologische middelen heimelijk beïnvloeden van iemands besluitvorming. Vraag 4 sluit daarmee aan bij vraag 1 en 2 over de relevante wetgeving voor de verspreiding van (des)informatie en de inhoud hiervan. Bij de bespreking van de verschillende wettelijke normen in hoofdstuk 5 en 6 zijn telkens de relevante handavings- en toezichtsmogelijkheden besproken. Zo breed als het wettelijk kader zijn ook de handavingsregimes, nu het wettelijk kader het privaat-, straf-, en bestuursrecht doorsnijdt. Specifiek ten aanzien van “online manipulatie” zijn de ACM en de AP als toezichthouders relevant.

Vraag 5 richt zich op een specifieke sanctioneringsmogelijkheid voor (politieke) misleiding in de verkiezingscontext middels de strafrechtelijke bescherming van de integriteit van het verkiezingsproces. In hoofdstuk 6.B is de huidige strafbaarstelling van online manipulatie besproken in de context van artikel 127 Sr, artikel 138ab Sr en de verschillende verspreidingsdelicten.

Vraag 6 onderzoekt in essentie of het type dienst en de bedrijfsvorm van een internetdienst invloed heeft op de wettelijke verantwoordelijkheden ten aanzien van desinformatie. In hoofdstuk 3 zijn de verschillende internetdiensten besproken aan de hand van de relevante juridische definities, de relevante verdienmodellen en de handavingsmodaliteiten ten aanzien van de verspreiding van (des)informatie. In hoofdstuk 5 en 6 is vervolgens, waar relevant, bij de bespreking van de normen steeds aangegeven op welk type dienst zij van toepassing zijn.

Ten slotte richt **vraag 7** zich op de bescherming van burgers tegen desinformatie. Het grondrechtelijk kader, met de vrijheid van meningsuiting in het bijzonder, is in hoofdstuk 4 uitgebreid behandeld. Daarnaast is in hoofdstuk 5 onder andere bij de bespreking van de Richtlijn elektronische handel, de Algemene Verordening Gegevensbescherming en het consumentenrecht expliciet stilgestaan bij de vraag hoe de rechten van gebruikers beschermd worden.

Zoals aangegeven in de inleiding, is er gezien de breedte en diversiteit van de onderzoeksvragen voor gekozen om in de studie de structuur van het wettelijk kader te volgen. Binnen deze structuur zijn de onderzoeksvragen in de loop van de rapportage heen beantwoord. De uitkomsten van het onderzoek kunnen per hoofdstuk als volgt samengevat worden.

B. Samenvatting & conclusies

Uit de conceptuele inkadering van desinformatie in **hoofdstuk 2** blijkt de breedte en complexiteit van de problematiek. Er kan worden vastgesteld dat het concept zich voornamelijk leent voor de markering van een nieuw beleidsterrein en niet als afgebakende juridische categorie. Een eerste complicerende factor zijn de verschillende actoren die bij het proces van de verspreiding van desinformatie betrokken zijn: de maker of opdrachtgever van de desinformatie, de internetdienst via welke de informatie (verder) verspreid wordt en het publiek dat de desinformatie ontvangt en verder verspreidt. Een tweede laag van complexiteit is dat er niet één type bron van desinformatie is. Desinformatie kan gecreëerd worden door zowel statelijke actoren, politieke partijen of bijvoorbeeld individuele internetgebruikers. Een derde

complicerende factor is dat desinformatie niet onder te brengen is in één juridische categorie. Het omvat zowel illegale, onrechtmatige, als toegestane, doch mogelijk schadelijke uitingen. Vervolgens blijkt dat, als vierde relevante factor, het optreden van schadelijke gevolgen voornamelijk voorkomt bij groot-schalige verspreiding van desinformatie als gevolg van socio-technische processen. Een laatste compli-cerend element is dat desinformatie in uiteenlopende contexten voorkomt, zoals bijvoorbeeld nieuws, *hate speech*, commerciële uitingen, buitenlandse beïnvloeding en politieke advertenties. Deze contexten kennen alle hun eigen regulering en juridische logica.

In **hoofdstuk 3** is stilgestaan bij de verschillende internetdiensten die een centrale rol spelen bij de online verspreiding van desinformatie. Deze verschillende diensten kunnen beschouwd worden op basis van hun juridische kwalificatie, bedrijfsvormen en verdienmodellen, en op basis van de handhavingsmodaliteiten die een specifieke dienst ter beschikking staan. Vanuit juridisch perspectief zijn de volgende typen dien-sten relevant: diensten van de informatiemaatschappij, elektronische communicatiediensten en audiovi-suele mediadiensten. Ook is het begrip *hosting service provider* uit de Richtlijn elektronische handel van belang aangezien deze beperking van aansprakelijkheid door veel van de betreffende diensten inge-roepen kan worden. Van specifiek belang voor de problematiek rond desinformatie zijn de sociale medi-adiensten, die op basis van door hun gebruikers gegenereerde content werken en mogelijkheden aan-bieden voor data-gestuurde en gerichte advertenties. Ook relevant zijn de *direct messaging* diensten die gebruikers in staat stellen één op één of in groepsverband te communiceren. Door nieuwe mogelijkheden voor gerichte communicatie via deze platformen en de mogelijkheid van het grootschalig verspreiden van inhoud door gebruikers, kan de verspreiding van informatie via deze diensten een vergelijkbare maatschappelijke impact hebben als in het geval van de traditionele massamedia. De handhavingsmoge-lijkheden ten aanzien van desinformatie hangen samen met de technische inrichting van de specifieke dienst, het beleid van de dienst, en de daadwerkelijke handhaving van het gestelde beleid in de praktijk.

Het relevante wettelijke kader voor desinformatie verspreid via internetdiensten is vervolgens in **hoofd-stuk 4 tot en met 6** geanalyseerd, waaruit in de eerste plaats de breedte en diversiteit van de betrokken wetgeving opvalt en in de tweede plaats dat verschillende vormen van desinformatie door middel van deze wetgeving al op enige wijze gereguleerd is. De buitenste laag van het relevante juridisch kader wordt gevormd door de grondrechten en de vrijheid van meningsuiting in het bijzonder. Alle wet- en regelgeving moet zich immers binnen deze grenzen begeven. De analyse van de relevante jurisprudentie op het gebied van de vrijheid van meningsuiting in hoofdstuk vier benadrukt dat het recht op vrijheid van meningsuiting niet alleen inhoudt dat de staat bepaalde beperkingen niet mag opleggen, maar ook dat de staat positieve verplichtingen heeft om burgers in staat te stellen hun vrijheid van meningsuiting te kunnen uitoefenen. De meest relevante positieve verplichtingen zijn in dit opzicht de verplichting om een pluralistisch democratisch debat te waarborgen en om te voorkomen dat kapitaalkrachtige groepen de overhand krijgen in het politieke debat, bijvoorbeeld door middel van politieke advertenties. Transparantieplichtingen, in het bijzonder over de herkomst van (politieke) advertenties, kunnen in dit verband ook een positieve rol vervullen. Het juridisch verbieden van bepaalde informatie louter op grond van het feit dat informatie onjuist of misleidend is, zonder aanvullende eisen, moeilijk in overeenstemming te brengen met de vrijheid van meningsuiting. Hierbij is van belang dat desinformatie in sommige gevallen kwalificeert als politieke uiting en als zodanig brede bescherming geniet. Verder vallen specifiek politieke advertenties in beginsel tevens onder de uitgebreide bescherming van politieke uitingen onder Artikel 10 EVRM.

Vervolgens blijkt uit de analyse van het wettelijk kader voor de verspreiding van desinformatie op Euro-pees en nationaal niveau, in **hoofdstuk 5 en 6**, vooral de diversiteit en enorme omvang van de betrokken regelgeving. De regelgeving loopt dwars door de bestaande klassieke rechtsgebieden en sectorregu-leringen waarbij het relevante kader in een concreet geval afhangt van de specifieke context en de gebruikte technieken (bv. commercieel of politieke uiting, privé berichten of openbaar, hosting provider of dienst met redactionele controle en verantwoordelijkheid). Het EU-kader bestaat uit de Richtlijn Elek-

tronische handel, de AVMD-richtlijn, de e-Privacy Richtlijn, de richtlijnen met betrekking tot handelspraktijken en -reclame, de AVG en relevante zelfregulering. Het betreft een zeer dynamisch rechtskader. Veel elementen van het relevante Europese regelgevingskader zijn van erg recente datum (AVG & AVMD-richtlijn) of worden momenteel of binnenkort herzien (e-Privacy Richtlijn en de Richtlijn elektronische handel). Het relevante nationale juridisch kader voor desinformatie doorsnijdt zoals gezegd het privaatrecht, het staats- en bestuursrecht en het strafrecht. Binnen het privaatrecht is er het leerstuk van de onrechtmatige daad, onder meer relevant voor onrechtmatige publicaties, en het intellectueel eigendomsrecht, waaronder het portretrecht. Binnen het strafrecht zijn er de specifieke uitingsdelicten, de verkiezingsdelicten, het zich ontwikkelende leerstuk van de computercriminaliteit en de verspreidingsdelicten. Binnen het Nederlandse staats- en bestuursrecht bestaat er de reclameregulering, de regelgeving met betrekking tot de financiering van politieke partijen, en de wetgeving op het gebied van de nationale veiligheid en de kritische infrastructuur. Wat betreft de zelfregulering zijn vooral de Nederlandse Reclame Code en de Raad voor de Journalistiek van belang. Ook op nationaal niveau zijn er een aantal (zelf)reguleringsinitiatieven op het gebied van desinformatie die in hoofdstuk 6 zijn besproken.

Alvorens verder te gaan met hoofdstuk 7 zullen nu eerst de conclusies besproken worden die uit de analyse van het wettelijk kader in hoofdstuk 5 en 6 volgen.

Op basis van het geboden overzicht van het juridisch kader kan in algemene zin geconcludeerd worden dat een groot aantal typen desinformatie deels al onder een bestaande juridische categorie vallen (misleidende reclame, smaad, onrechtmatige perspublicatie etc.) en als zodanig dus al gereguleerd is. Ook blijkt de toepasselijke regelgeving afhankelijk van het type internetdienst, de inhoudelijke kwalificatie van eventuele (des)informatie en de context waarbinnen deze wordt verspreid (bv. commercieel, politiek, privé). Niet verwonderlijk, gezien de breedte van de problematiek, is er bij de handhaving van deze bestaande normen vervolgens ook een groot aantal verschillende toezichthouders betrokken. De voornaamste zijn de AP, de ACM, de AFM en het Commissariaat voor de Media. Deze algemene conclusies zullen nu verder uitgewerkt worden wat betreft de aansprakelijkheid van internet tussenpersonen, de bescherming van persoonsgegevens, de betrokken toezichthouders, de strafbaarstelling van online manipulatie en de relevante zelfregulering.

De **aansprakelijkheid van internetdiensten** voor illegale en onrechtmatige inhoud heeft een centrale positie in het juridisch kader. Centraal hierin staat de Richtlijn elektronische handel die op Europees niveau een voorwaardelijke horizontale uitsluiting van aansprakelijkheid biedt voor illegale en onrechtmatige inhoud. De exacte reikwijdte van deze normen zijn medebepalend voor de manier waarop internetdiensten vormgegeven zijn en hun aanpak van desinformatie, nu het in hun belang kan zijn aansprakelijkheid te vermijden. Daarnaast is het verbod voor lidstaten om internetdiensten algemene toezichtverplichtingen op te leggen een duidelijke beperking voor mogelijke regulering met betrekking tot desinformatie. Naast deze voorwaardelijke horizontale aansprakelijkheidsuitsluiting zijn er ook een aantal sectorspecifieke, verticale, aansprakelijkheidsgronden zoals uit de AVMD-richtlijn die al vormgeven zijn conform de ruimte waar internetdiensten zich in bewegen. Deze normen zijn allemaal op Europees niveau geformuleerd. De nieuwe Europese Commissie heeft aangekondigd het juridisch kader voor de aansprakelijkheid van tussenpersonen de komende jaren te willen herzien middels de *Digital Services Act*.

De **bescherming van persoonsgegevens** en de effectieve handhaving van de geldende regels is van groot belang voor de problematiek rond desinformatie. Nieuwe verspreidingsmethoden via internetdiensten leunen vaak op de verzameling, de analyse en het gebruik van persoonsgegevens van het publiek. Deze data-gestuurde vormen van online beïnvloeding vallen onder de AVG en kunnen op basis daarvan aangepakt worden. Dat geldt voor de afzenders van communicatie, zoals bijvoorbeeld een organisatie die gerichte campagnes voert via communicatiediensten en sociale media. Maar het geldt ook voor de internetdiensten zelf, waaronder de verzameling van gegevens over hun gebruikers, en de analyse en het gebruik van deze gegevens in het licht van de aan adverteerders en andere partijen geboden mogelijk-

heden tot gerichte communicatie met het publiek. Er is mede gezien het *Cambridge Analytica* schandaal al redelijk wat aandacht is voor desinformatie en micro-targeting in de literatuur over het gegevensbeschermingsrecht. Toezichthouders hebben het onderwerp ook op de agenda gezet. Toch is er momenteel nog weinig sprake van effectieve handhaving van het gegevensbeschermingsrecht, terwijl dit geldt als een belangrijke algemene waarborg tegen bepaalde aspecten van desinformatie.

Vervolgens is het **relevante toezicht op internetdiensten** gefragmenteerd en nog relatief zwak ontwikkeld, terwijl de complexiteit een grote mate van expertise en middelen vereist. Een groot aantal toezichthouders is betrokken, met in Nederland als hoofdrolspelers de ACM, de AP en het Commissariaat voor de Media. Afhankelijk van de specifieke context zijn daarnaast toezichthouders zoals de AFM en de Nederlandse Voedsel- en Warenautoriteit betrokken. Ook wordt in relevante gevallen het toezicht uitgeoefend door een ministerie, zoals in het geval van de Wet financiering politieke partijen of door bijvoorbeeld de Fiscale Inlichtingen- en Opsporingsdienst – Economische Controledienst voor de Nederlandse implementatie van de transparantieverplichtingen uit de Richtlijn elektronische handel.

De ACM zal veelal betrokken zijn in het kader van het beschermen van consumentenbelangen, de AP bij de bescherming van persoonsgegevens en het Commissariaat voor de Media wat betreft de mediaregulering. Het werkgebied van deze toezichthouders overlapt op enkele punten, bijvoorbeeld wat betreft de handhaving van het spamverbod in artikel 11.7 Telecommunicatiewet waar zowel de AP als de ACM bevoegdheden hebben. Voor de problematiek rond desinformatie zijn eventuele overlap wat betreft concrete wettelijke bepalingen niet het belangrijkste aandachtspunt. Meer van belang is meer de inhoudelijk overlap waar de toezichthouders verantwoordelijk zijn voor verschillende elementen van dezelfde problematiek. Zo zijn bijvoorbeeld de AP en de ACM bij verschillende aspecten van politieke micro-targeting betrokken: de AP wat betreft het gericht verspreiden op basis van persoonsgegevens en de ACM wat betreft de inhoud van de commerciële communicatie. Bij reclame verspreid op videoplatformen zijn alle drie de toezichthouders voor verschillende aspecten betrokken. Door deze inhoudelijke overlap is het van belang dat de verschillende toezichthouders samenwerken in hun aanpak.

	Autoriteit Persoonsgegevens	Commissariaat voor de Media	Autoriteit Consument en Markt
Typering	Bescherming persoonsgegevens, toezicht op de naleving van de AVG.	Mediaregulering, toezicht op de Mediawet en de Wet op de vaste boekenprijzen.	Bescherming consumentenrechten en toezicht op de mededinging.
Connectie desinformatie	Gerichte informatie- verspreiding op basis van persoonsgegevens (micro-targeting).	Desinformatie verspreid via traditionele media en reclame regulering.	Regulering commerciële communicatie en consumenten-bescherming.

Tabel 4

Voort zijn de inzet van het **strafrecht** en de **veiligheidsdiensten** een belangrijke component van het juridisch kader. Het strafrecht vormt de meest ingrijpende regulering van desinformatie en moet met het oog op de bescherming van de vrijheid van meningsuiting zeer terughoudend en slechts weloverwogen ingezet worden. Bij de aanpak van de verspreiding van desinformatie door buitenlandse staten is een rol weggelegd voor de veiligheidsdiensten. De zorg om oneigenlijke buitenlandse beïnvloeding en propaganda is niet nieuw. Er bestaat uitgebreide jurisprudentie over de toelaatbaarheid van mogelijke maatregelen. Van belang hierbij is dat artikel 10 EVRM het recht op vrijheid van meningsuiting nadrukkelijk garandeert "ongeacht grenzen".

Een specifiek onderdeel van dit onderzoek is de mogelijke strafrechtelijke normering van de online manipulatie van verkiezingen. De conclusie van dit rapport is dat er momenteel geen grond is om aanvullende

strafrechtelijke normen met betrekking tot misleidende of onjuiste online uitingen te stellen. In dit kader is artikel 127 Sr uitgebreid besproken. Aanleiding was de Motie Asscher/Van der Molen en de daarop gebaseerde vijfde onderzoeksvraag van deze rapportage.⁶⁰⁸ In sectie 6.B zijn de verschillende bestaande strafrechtelijke bepalingen die betrekking hebben op de oneigenlijke beïnvloeding van het verkiezingsproces besproken. Daarbij is ook stilgestaan bij computercriminaliteit, gezien de mogelijke integriteitsinbreuken op internetdiensten waarvan sprake kan zijn bij de verspreiding van desinformatie, en de verschillende strafrechtelijke verspreidingsdelicten. In relatie tot desinformatie en onlinemanipulatie bleek artikel 127 Sr de meest relevante strafbepaling. Het artikel stelt een “bedrieglijke handeling” strafbaar die als gevolg heeft of het “van onwaarde” maken van een stem of de *error in persona*. Wanneer het vereiste causaal verband extensief uitgelegd wordt, omvat de strafbepaling uitingen die als desinformatie gekwalificeerd kunnen worden. Telkens wanneer desinformatie als gevolg heeft dat een stem van onwaarde wordt, of een kiezer op een ander heeft gestemd dan hij of zij denkt, dan is dat verboden onder artikel 127 Sr. Gedacht moet worden aan situaties waarin een kiezer verkeerd geïnformeerd wordt over de vereiste stemwijze, waardoor zijn of haar stem ongeldig wordt verklaard. Hoewel de strafbepaling dus vormen van onlinemanipulatie of desinformatie omvat, vallen de meest bekende voorbeelden van desinformatie buiten de delictsommschrijving. Desinformatie die ertoe leidt dat mensen niet gaan stemmen of mensen voorliegt over het verkiezingsprogramma van een kandidaat worden niet door artikel 127 Sr strafbaar gesteld omdat de schade in deze voorbeelden niet door het artikel wordt gedekt.

Enige uitbreiding van de specifieke delictsommschrijving van artikel 127 Sr of andere normen die op de *inhoud* van een uiting zien, zijn problematisch vanuit het perspectief van de vrijheid van meningsuiting. Nu het om politieke uitingen gaat en het strafrecht beschouwd moet worden als ultimum remedium is er weinig ruimte voor uitbreiding. Dit is bij de invoering van de strafbepaling ook onderkend toen er nadrukkelijk op gewezen werd dat de rechter en de overheid buiten het politieke debat moeten blijven. Uit het een en ander volgt dat er geen grond is om nieuwe strafrechtelijke normen of delicten met betrekking tot onjuiste of misleidende inhoud te stellen.

Daarentegen is er wellicht wel ruimte in het kader van de verdere ontwikkeling van computercriminaliteit in combinatie met gegevensbeschermingsrecht. Misleidende en manipulerende processen op basis van data waarbij misbruik gemaakt wordt van een internetdienst en die het verkiezingsproces beïnvloeden, zijn onder het huidige recht niet effectief genormeerd. Bij de huidige computervrederebreukbepaling uit artikel 138a Sr is onduidelijk wat de rol is van de gebruiksvoorwaarden van een internetdienst om een handeling als “wederrechtelijk binnendringen” en daarmee als strafbaar te kwalificeren. Het is onwenselijk de strafbepaling van computervrederebreuk op die manier af te laten hangen van de gebruiksvoorwaarden die een internetdienst zelf stelt (integriteit van de dienst). Maar gezien het belang van deze internetdiensten voor het democratisch debat (integriteit van het publieke debat) is de mogelijkheid dat systematisch misbruik gemaakt wordt van dergelijke diensten om mensen te manipuleren daarentegen zo problematisch dat wel gedacht kan worden aan een mogelijke normstelling. Deze normstelling zou ook in combinatie gezien moeten worden met het gegevensbeschermingsrecht aangezien dit type beïnvloeding in de regel data-gestuurd is. Naar dergelijke specifieke normering van data-gestuurde systematische manipulatietechnieken is verder empirisch en rechtswetenschappelijk onderzoek nodig.

Ook de verschillende **zelfreguleringsinstrumenten** op het gebied van de informatiekwaliteit zijn belangrijk voor de bredere aanpak van desinformatie. In de Nederlandse context zijn de Nederlandse Reclame Code en de Raad voor de Journalistiek essentieel voor het stellen van sectorwijde normen die de kwaliteit van informatie bewaken en zo ook een belangrijke waarborg voor desinformatie vormen. Op Europees niveau zijn zelf-reguleringsinstrumenten zoals de *EU Code of Practice on Disinformation* van belang. Het individuele beleid van de internetdiensten zelf is tevens van grote invloed op de mogelijke verspreiding

608 Tweede Kamer, vergaderjaar 2018/2019 30 821, nr. 68.

van desinformatie. De regulering van de **financiering van politieke partijen** kan, als laatste punt, ook een belangrijke waarborg vormen voor de verspreiding van desinformatie in de vorm van politieke advertenties.

Ter afsluiting van de samenvatting en conclusies van het rapport moet nog stilgestaan worden bij **hoofdstuk 7**. Dit hoofdstuk bevat een synthese van het geldend juridisch kader in Nederland, de aanpak van desinformatie en de uitkomsten van de uitgevoerde landenstudies (Verenigd Koninkrijk, Frankrijk, Duitsland, Zweden, de Verenigde Staten en Canada). Het hoofdstuk geeft ook een overzicht van de manier waarop het huidige juridisch en beleidskader voor desinformatie en politieke advertenties in Nederland zich uitstrekt over recht en beleid op drie samenhangende niveaus: Europees, nationaal en zelfregulering. Er zijn op basis van de landenstudies verschillende mogelijke benaderingen te onderscheiden in de aanpak van desinformatie, waaronder (a) nieuwe programma's voor mediawijsheid, en aanvullende financiering voor bestaande programma's met als doel het kritisch vermogen van internetgebruikers ten aanzien van desinformatie te versterken, (b) nieuwe programma's voor de subsidiering van onafhankelijke media, (c) de aanpak van desinformatie in het kader van de nationale veiligheid, (d) specifieke nieuwe wetgeving met een verbod op desinformatie en onjuiste informatie tijdens verkiezingen, (e) nieuwe zorgplichten voor internetdiensten met betrekking tot het implementeren van maatregelen voor de aanpak van desinformatie, (f) een verplichting voor internetdiensten om desinformatie die kwalificeert als kennelijk onrechtmatige binnen 24 uur te verwijderen, (g) nieuwe wetgeving die zich richt op buitenlandse invloeden en een verbod oplegt aan buitenlanders om bijdragen te leveren of uitgaven te doen met betrekking tot verkiezingen; en (h) nieuwe regulering van bots en geautomatiseerde software.

In hoofdstuk 7 is ook stilgestaan bij de verschillende reguleringsmogelijkheden met betrekking tot politieke advertenties. Hoewel dit de bredere problematiek van desinformatie niet zal kunnen oplossen, kan het wel een uitkomst bieden voor de specifieke problematiek van desinformatie vervat in politieke advertenties. De uitkomst van de analyse was dat het rapport steun biedt voor het advies van de commissie over het Nederlandse parlementaire systeem en het voornemen van de regering om verdere financiële transparantie voor politieke partijen in de "Wet op de Politieke Partijen" op te nemen. Ook kunnen middels dezelfde wetgeving grenzen gesteld worden aan de mogelijkheid van buitenlandse actoren om Nederlandse politieke partijen te financieren.

C. Aanbevelingen

Uit het onderzoek kunnen een aantal concrete aanbevelingen gedestilleerd worden. Zo dient het begrip desinformatie te worden beschouwd als **beleidsterm** en niet als een afgebakend juridisch begrip. Dit blijkt ook duidelijk uit de landenstudies. In bijna alle landen waarnaar gekeken is – Zweden, de Verenigde Staten, het Verenigd Koninkrijk, Duitsland en Canada – is desinformatie niet juridisch gedefinieerd, maar wordt het wel gezien als beleidsgebied. Alleen Frankrijk, waar al sinds jaren een wet bestaat op "vals nieuws", heeft recentelijk nieuwe juridische definities aangenomen van "valse informatie" en "manipulatie van informatie" in het kader van verkiezingen.

Voor het stellen van **nieuwe normen** in Nederlands verband beveelt deze rapportage aan om verder onderzoek te doen naar het normeren van nieuwe vormen van manipulatie, waarbij gedacht kan worden aan het op grote schaal en data-gestuurd manipuleren van communicatieprocessen op relevantie internetdiensten. Het gaat hier niet om het verbieden van nieuwe vormen van onjuiste of misleidende informatie, maar om de regulering van communicatieprocessen en de integriteit van relevante communicatiemiddelen vanuit democratisch belang.

Verder is het onderkennen van de gelaagdheid en de **verschillende juridische beleidsniveaus** een van de belangrijkste uitgangspunten voor de verdere ontwikkeling van beleid met betrekking tot desinformatie. De rol en verantwoordelijkheid van verschillende soorten diensten bij de verspreiding van (des)informatie

is terecht een centraal aandachtspunt in het debat, maar vanuit juridisch oogpunt is het toepasselijke kader daarmee zeer gelaagd en complex. Een deel van de desinformatie problematiek hangt direct samen met de specifieke inrichting van internetdiensten, sociale media in het bijzonder, en de mogelijkheden die geboden worden voor de (verdere) verspreiding van (des)informatie. Het beleid van relevante diensten is mede onder druk van overheden volop in ontwikkeling, maar er is hier voornamelijk sprake van een internationale dynamiek. Het is daarbij steeds de vraag hoe de keuzes die door relevante diensten worden gemaakt en de zelfregulering die elders overeengekomen wordt vanuit Nederlands perspectief bekeken dienen te worden.

Verder kan gesproken worden van een **spanningsveld in de regulering** van verschillende aspecten van desinformatie tussen het Europese en Nederlandse niveau. Bij de relevante Europese regelgeving ligt de nadruk op marktordening en het veiligstellen van de Europese interne markt. Daaruit volgt ook logischerwijs dat de Europese wetgever een relatief dominante rol speelt in het stellen en harmoniseren van regels voor relevante internetdiensten. Op Europees niveau is daarbij echter sprake van een relatief gebrek aan competentie met betrekking tot het stellen van regels met betrekking tot de bescherming van het democratisch debat en nationale politieke processen. Het is echter juist deze dimensie die in de problematiek van desinformatie uiteindelijk centraal staat. Het is daarom van belang dat Europese regelgeving van sociale media en andere internetdiensten in relatie tot nationale problematiek een faciliterende rol speelt waarbij ruimte blijft bestaan voor eigen keuzes en afwegingen in de lidstaten. Zoals het Europees Hof voor de Rechten van de Mens heeft overwogen is er een “wealth of historical, cultural and political differences within Europe so that it is for each State to mould its own democratic vision”; en vanwege “their direct and continuous contact with the vital forces of their countries, their societies and their needs, the legislative and judicial authorities are best placed to assess the particular difficulties in safeguarding the democratic order in their State”.

Waar een Europese toezichthouder voor desinformatie niet voor de hand ligt, zou de Europese Unie bijvoorbeeld wel zorg kunnen dragen voor het (zo nodig dwingendrechtelijk) verbeteren van de informatieposities van nationale overheden en toezichthouders ten aanzien van relevante internetbedrijven. Hieraan gerelateerd dient uiteraard ook stilgestaan te worden bij de juridische, politieke en praktische beperkingen met betrekking tot jurisdictie van nationaal recht en daarmee samenhangende beperkingen op extraterritoriale werking. Er is internationaal geen eenduidig antwoord op de aanpak van desinformatie bij internetdiensten. In het licht van de vrijheid van meningsuiting dient voorkomen te worden dat de uiteindelijke normering en handhaving uitkomt op de kleinste gemene deler.

De beste algemene grondslag voor de regulering van en beleid met betrekking tot desinformatie en politieke advertenties is de **waarborg van pluralisme**. Artikel 10 EVRM staat toe, of beter gezegd vereist, via het leerstuk van positieve verplichtingen, dat in verband met de promotie van pluralisme van het mediaveld structurele maatregelen worden getroffen. Hierbij moet gedacht worden aan de regulering van massamediale aspecten van sociale media, het opleggen van beperkingen op politieke advertenties, in het bijzonder middels transparantievereisten, en de publieke financiering van (onafhankelijke) media. Verder onderzoek is nodig naar de vraag welke mogelijke maatregelen het meest geschikt en nodig zijn voor de aanpak van de verspreiding van desinformatie via internetdiensten. Hier zou gedacht kunnen worden aan bepaalde verplichtingen met betrekking tot de inrichting van de dienst (bv. mogelijkheden om onrechtmatige of schadelijke inhoud te rapporteren en de verplichting om adequaat op te reageren), alsmede aan verplichtingen tot (procedurele) transparantie met betrekking tot het gebruik van de betreffende dienst, alsook aan investeringen in de onlineactiviteiten van de publieke media.

Het stellen van strikte aansprakelijkheid voor illegale en onrechtmatige vormen van desinformatie levert problemen op met de vrijheid van meningsuiting en de richtlijn elektronische handel. Gestelde normen met betrekking tot de **verantwoordelijkheid van internettussenpersonen** dienen in elk geval aan te sluiten bij de maatschappelijke rol van de betreffende diensten en niet slechts de mogelijkheid van con-

trole door tussenpersonen te maximaliseren zonder oog voor de negatieve gevolgen. Een meer vruchtbare richting van normstelling is de mogelijkheid van algemene normen ten aanzien van de inrichting van de betreffende dienst en gerelateerde processen. Hier kan bijvoorbeeld gedacht worden aan een verplichting tot het aanbieden van een makkelijk vindbare mogelijkheid te rapporteren over desinformatie, het hier een antwoord op te krijgen binnen bepaalde tijd, duidelijke waarschuwingen met betrekking tot gebruiksvoorwaarden, toezicht op onrechtmatig gebruik van de dienst en rapportage daarover. Er is meer onderzoek nodig naar de mogelijkheid om dit soort normen te stellen en hand te haven met betrekking tot verschillende diensten.

Waar sprake is van verwijdering of blokkeren van inhoud door internetdiensten is er momenteel een gebrek aan duidelijke regels voor de **rechten van de gebruikers** wiens communicatie het betreft. Dit is een onderwerp dat zowel vanuit het consumentenrecht als de vrijheid van meningsuiting beschouwd kan worden. Het is een onderwerp dat aan de orde zal moeten komen in de geplande herziening van het Europese kader en ook reeds in de officiële beleidsstukken van de Europese Commissie over illegale en schadelijke inhoud gezien wordt.

Het relevante **toezicht** op de problematiek van desinformatie is gefragmenteerd. Verdergaande samenwerking tussen voornamelijk de ACM, de AP en het Commissariaat voor de Media is van belang voor effectief toezicht op bestaande regels en het versterken van relevante expertise. De bescherming van persoonsgegevens geldt als een belangrijke algemene waarborg voor bepaalde data-gerelateerde aspecten van desinformatie en online manipulatie. Er is echter momenteel nog weinig sprake van effectieve handhaving van het gegevensbeschermingsrecht op relevante aspecten.

Een algemene zorg is het gebrek aan **transparantie** ten aanzien van de communicatieprocessen op, alsmede de handhaving door internetdiensten met betrekking tot desinformatie. Daardoor is sprake van een relatief slechte informatiepositie van relevante overheden, alsmede het maatschappelijk veld. Vanuit de wetenschap en de journalistiek komen steeds sterkere signalen dat de toegang tot gegevens die noodzakelijk zijn voor de bestudering van desinformatie onvoldoende gewaarborgd zijn. Van belang bij het een en ander is dat verschillende maatschappelijke actoren verschillende informatiebehoeftes hebben in de uitvoering van hun taken en maatschappelijke functies. De overheid, de journalistiek, de wetenschap, NGO's, en toezichthouders hebben alle een eigen informatiebehoefte. Voor een effectieve transparantieregulering zou verder in kaart gebracht moeten worden wat deze behoeftes zijn en hoe aanvullende regulering middels transparantievereisten in deze behoeftes kan voorzien. Zelfreguleringsinitiatieven van sociale media schieten tot nog toe tekort in het ondervangen van deze problematiek. Gezien de democratische belangen die spelen bij het kunnen inschatten van de maatschappelijke impact van internetdiensten, en sociale media in het bijzonder, is dit een onderwerp waar een actievere houding van de overheid gewenst is.

Literatuurlijst

J. Aalberts, *Het mysterieuze voortbestaan van de zendtijd van politieke partijen*, Tijdschrift voor Media-geschiedenis, 16(2), p. 43.

Autoriteit Consument & Markt & Commissariaat voor de Media, *Digitalisering en nepnieuws, Een gezamenlijke verkenning van de Autoriteit Consument & Markt en het Commissariaat voor de Media*, <https://www.cvdm.nl/wp-content/uploads/2018/07/Rapport-Nepnieuws-en-digitalisering-CvdM-ACM.pdf>.

Advisory Opinion, *Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism*, Advisory Opinion OC-5/85. Series A, No. 5. 13 November 1985.

AIVD, *AIVD-jaarverslag 2018*, Bijlage bij Kamerbrief minister BZK bij openbaar jaarverslag AIVD 2018.

C. Alberdingk Thijm, *Kiezen uit twee hoogwaardige belangen*, C. Eradus, C. Brouwer, H. & Veraart, M. (red.) "Bodem kort geding", Amsterdam, 2013.

Amnesty International, *Brief of amici curiae Amnesty International, Article 19, Canadian Journalists for Free Expression, Committee to Protect Journalists, Freedom House, pen international (and its local chapters Pen Afrikaans, Pen American Center, Pen Eritrea In Exile, Pen Ghana, Pen Kenya, Pen Nigeria, Pen Sierra Leone, And Pen South Africa), Reporters Without Borders, And Right 2 Know Campaign South Africa*, <https://freedex.org/wp-content/blogs.dir/2015/files/2017/05/CONSOLIDATED-BRIEF-FINAL-May-18-C1.pdf>.

Angelopoulos, C., Brody, A., e.a. (2015) "Study of fundamental rights limitations for online enforcement through selfregulation", Institute for Information Law, via: <https://www.ivir.nl/publicaties/download/1796>.

Article 19, *Germany: The Act to Improve Enforcement of the Law in Social Networks: Legal Analysis* <https://www.article19.org/wp-content/uploads/2017/12/170901-Legal-Analysis-German-NetzDG-Act.pdf>.

Article 19, *France: ARTICLE 19 comments on interim report for social media* <https://www.article19.org/wp-content/uploads/2019/06/French-social-media-reg-proposal-briefing-FINAL.pdf>.

Article 19, *Response to the Consultations on the White Paper on Online Harms* <https://www.article19.org/wp-content/uploads/2019/07/White-Paper-Online-Harms-A19-response-1-July-19-FINAL.pdf>.

G. Asmology, *The Disconnective Power of Disinformation Campaigns*, Journal of International Affairs 71(1.5): Columbia, 18 September 2018, <https://jia.sipa.columbia.edu/disconnective-power-disinformation-campaigns>

L.F. Asscher, *Communicatiegrondrechten: een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*. Amsterdam: Otto Cramwinckel 2002.

Autoriteit Persoonsgegevens, *Verkenkend onderzoek naar gebruik persoonsgegevens in verkiezingscampagnes* 2019.

B. Baade, *Fake news and international law* (2018) 29(4) European Journal of International Law 1357-1376

P.M. Barrett, *Disinformation and the 2020 Election: how the Social Media Industry Should Prepare*, NYU Stern 2019.

J. Bayer, N. Bitiukova, P. Bárd, J. Szakács, A. Alemanno & E. Uszkiewicz., *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, beschikbaar via: [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

BBC Media Centre, *New collaboration steps up right against disinformation*, 7 september 2019, via: <https://www.bbc.co.uk/mediacentre/latestnews/2019/disinformation>.

BBC News, *Germany starts enforcing hate speech law*, 1 januari 2018.

Y. Benkler, *Election Advertising Disclosure: Part 1*, Harvard Law Review Blog, 31 October 2017, via: <https://blog.harvardlawreview.org/election-advertising-disclosure-part-1/>

L. Bershidsky, *Fake News Takes Its Toll on Sweden's Elections*, Bloomberg, 15 November 2018 via: <https://www.bloomberg.com/opinion/articles/2018-11-15/fake-news-roiled-sweden-s-elections-but-it-was-homegrown>.

M.J. Blitz, *Lies, Line Drawing, and Deep Fake News*, 71 Oklahoma Law Review 59-116.

A. Borell & J. Dkhlija, *Political Advertising in France: The Story and Effects of a Slow Liberalization* in: Holtz-Bacha, C. & Marion R. Just (eds), *"Routledge Handbook of Political Advertising"* Routledge, 2017, pp. 123-13

Samantha Bradshaw, Lisa-Maria Neudert, and Philip N. Howard, *Government Responses to Malicious Use of Social Media* (NATO, 2019), <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/01/Nato-Report.pdf>.

J. Brunner, *Facebook, Google to pay Washington \$450,000 to settle lawsuits over political-ad transparency*, The Seattle Times, 18 December 2018, <https://www.seattletimes.com/seattle-news/politics/facebook-google-to-pay-washington-450000-to-settle-lawsuits-over-political-ad-transparency/>

Bureau voor Democratische Instellingen en Mensenrechten, *Nederland: Parlementsverkiezingen 15 maart 2017: Eindrapport OVSE/ODIHR Verkiezingswaarnemingsmissie*, Warschau: OSCE 2017.

F. Camille, *Actors, Behaviours, Content: A Desinformation ABC. Highlighting three vectors of viral deception to guide industry & regulatory responses*", Transatlantic working group, september 20, 2019.

M. Cappello, *Media coverage of elections: the legal framework in Europe*, Straatsburg: European Audio-visual Observatory 2017.

M. Cappello (ed.), A. Alén-Savikko, E. Apa, M. Bassini, F. Javier Cabrera Blázquez, I. Cunningham, C. Etteldorf, A. Granchet, B. Klimkiewicz, R. Ó Fathaigh, J. Polák, T. Prosser, A. Richter, and N. Rodriguez, *Media reporting: facts, nothing but facts?, IRIS Special 2018-1* (European Audiovisual Observatory, 2018), <https://rm.coe.int/media-reporting-facts-nothing-but-facts/16808e3cda>.

T. Cardoso, *Google to ban political ads ahead of federal election, citing new transparency rules*, The Globe and Mail, 4 March 2019, <https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/>.

E. Coche, *"Fake news" en desinformatie in België: weinig zorgen, problemen voor morgen? Een analyse van dit mediafenomeen in België*, Mediaforum 185-189.

Committee of Ministers, *Recommendation No. R (99) 15 of the Committee of Ministers to member States on measures concerning media coverage of election campaigns*, beschikbaar via: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e3c6b.

Committee of Ministers, *Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of election campaigns*, beschikbaar via: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d4a3d.

Committee of Ministers, *Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet*, beschikbaar via: <https://wcd.coe.int/ViewDoc.jsp?id=2306649&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>.

Committee of Ministers, *Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors*, Adopted by the Committee of Ministers on 13 April 2016, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016806415d9#_ftn1.

Committee of Ministers, *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Media and Internet Division Directorate General of Human Rights and Rule of Law*, <https://rm.coe.int/1680645b44>

Committee of Ministers, *Recommendation CM/Rec(2017)8 of the Committee of Ministers to member States on Big Data for culture, literacy and democracy*, Adopted by the Committee of Ministers on 27 September 2017, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680750d68.

Committee of Ministers, *Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership*, Adopted by the Committee of Ministers on 7 March 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e13#_ftn1.

Committee of Ministers, *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*, Adopted by the Committee of Ministers on 7 March 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14.

Committee of Ministers, *Declaration by the Committee of Ministers on the financial sustainability of quality journalism in the digital age*, Adopted by the Committee of Ministers on 13 February 2019, https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4d.

Committee of Ministers, *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*, Adopted by the Committee of Ministers on 13 February 2019, https://search.coe.int/cm/pages/result_details.aspx?ObjectID=090000168092dd4b.

K. Conger, *Twitter will ban all political ads, C.E.O. Jack Dorsey says*, The New York Times, 30 October 2019, available at: <https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html>

Conclusions of the Council and of the Member States on securing free and fair European elections, as adopted by the Council on 19 February 2019, 6573/1/19 REV 1.

Council of Europe, Committee of Ministers" Recommendation CM/Rec(2018)1 to Member States on media pluralism and transparency of media ownership (7 March 2018). https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT0000202530_73&fastReqId=1760283217&fastPos=1.

Conseil supérieur de l'audiovisuel, "Recommendation no. 2019-03 of 15 May 2019 of the Conseil supérieur de l'audiovisuel to online platform operators in the context of the duty to cooperate to fight the dissemination of false information", http://www.csa.fr/content/download/254203/733091/version/1/file/CSA%20-%20Projet%20de%20recommandation%20aux%20op%C3%A9rateurs%202504_eng-GB.pdf.

R. Darnton, *The True History of Fake News*, *New York Review of Books* in: Bayer J. e.a., "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States", European Union, 2019, p. 24,

E. Denham, *Information Commissioner's Office: Guidance on political campaigning*, beschikbaar via: https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf.

E. Denham, *Information Commissioner's report brings the ICO's investigation into the use of data analytics in political campaigns up to date*, beschikbaar via: <https://ico.org.uk/about-the-ico/news-and-events/blog-information-commissioner-s-report-brings-the-ico-s-investigation-into-the-use-of-data-analytics-in-political-campaigns-up-to-date/>

A. Denton, *Fake News: The Legality of the Russian 2016 Facebook Influence Campaign*, 37(1) Boston University International Law Journal 183-210.

Deutschen Bundestag, *Regulierung von Hate Speech und Fake News in sozialen Netzwerken durch EU-Mitgliedstaaten*, beschikbaar via: <https://www.bundestag.de/resource/blob/566942/1a5eb997872bbe5dbca3f47112eb04c46/wd-10-032-18-pdf-data.pdf>.

T. Dobber, D. Trilling, N. Helberger & C.H de Vreese, *Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques*. Internet Policy Review, 6(4). doi:10.14763/2017.4.777.

E.J. Dommering, *De nieuwe Nederlandse Constitutie en de informatietechnologie* Computerrecht 2000 afl. 4, p. 182 – 183.

E.J. Dommering, *Het verschil van mening. Geschiedenis van een verkeerd begrepen idee*, Amsterdam: Uitgeverij Bert Bakker 2016

E.J. Dommering, *De Europese informatierechtsorde*, Amsterdam: deLex 2019

M.C. Dorf & S.G. Tarrow, *Fake News, the First Amendment, and the New Activist Journalism*, 20 Journal of Constitutional Law 1-32.

J. Downing & W. Ahmed, *#MacronLeaks as a "warning shot" for European democracies: challenges to election blackouts presented by social media and election meddling during the 2017 French presidential election*, beschikbaar via: <https://doi.org/10.1057/s4125>.

B.B. Duivenvoode, *Oneerlijke handelspraktijken*, TcVH 2016-1, p. 16-23.

EAVI, *Beyond fake news: 10 types of misleading news*, via https://eavi.eu/wp-content/uploads/2017/07/beyond-fake-news_COLOUR_WEB.pdf;

C. Edson, *Defining Fake News*, 2018, Digital Journalism

Electoral Commission, *The 2016 EU Referendum: Report on the regulation of campaigners at the referendum on the UK's membership of the European Union held on 23 June 2016*, beschikbaar via: https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Report-on-the-regulation-of-campaigners-at-the-EU-referendum.pdf.

Electoral Commission, *Digital campaigning: Increasing transparency for voters*, beschikbaar via: https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Digital-campaigning-improving-transparency-for-voters.pdf.

C. Etteldorf, "DE-Germany" in M. Cappello *Media coverage of elections: the legal framework in Europe*, beschikbaar via: https://www.ivir.nl/publicaties/download/IRIS_Special_2017_1.pdf.

European Broadcasting Union, *Position Paper Fake News and the Information Disorder*, https://www.ebu.ch/files/live/sites/ebu/files/Publications/Position%20papers/EBU-Position-EN-Fake_News_Disinformation-18.04.2018.pdf.

European Commission for Democracy Through Law, "Code of Good Practice in Electoral Matters", par. 3.3, [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2002\)023rev2-cor-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev2-cor-e).

European Commission for Democracy Through Law, "Compilation of Venice Commission Opinions and Reports concerning Media and Elections", CDL-PI(2018)006, 2018, p. 14, [https://www.venice.coe.int/webforms/documents/?pdf=CDL-PI\(2018\)006-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2018)006-e).

European Data Protection Board, *Annex 1 on national DPA guidance* beschikbaar via: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections-annexi_en.pdf.

European Data Protection Board, *Statement 2/2019 on the use of personal data in the course of political campaigns*, beschikbaar via: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

Europese Commissie, *Commissie aanbeveling van 19 september 2018*, beschikbaar via: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

Europese Commissie, *Communication on Securing free and fair European elections*, beschikbaar via: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0637:FIN>.

Europese Commissie, *Action Plan against Disinformation*, beschikbaar via: https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

Europese Commissie, *EU Code of Practice on Disinformation*, beschikbaar via: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

Europese Commissie, *Tackling online disinformation*, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

Europese Commissie, *Commission launches call to create the European Digital Media Observatory*, 7 October 2019, <https://ec.europa.eu/digital-single-market/en/news/commission-launches-call-to-create-european-digital-media-observatory>.

European Data Protection Board, *Statement 2/2019 on the use of personal data in the course of political campaigns*, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

EDPS Opinion on online manipulation and personal data, Opinion 3/2018", 19 March 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

European Values Centre, *2018 Ranking of countermeasures by the EU28 to the Kremlin's subversion operations*, *Kremlin Watch Report*, <https://www.kremlinwatch.eu/userfiles/2018-ranking-of-countermeasures-by-the-eu28-to-the-kremlin-subversion-operations.pdf>

Evaluatie- en adviescommissie Wet financiering politieke partijen, *Het Publieke belang van politieke partijen* 2018, p. 18-19. Bijlage bij: Tweede Kamer, vergaderjaar 2017-2018, 32752, nr. 50.

Externe Adviescommissie Vaccinatiebereidheid, *In gesprek over vaccineren*, Rijksvaccinatieprogramma Nederland 2018" RIVM ;

Facebook, *Facebook April report*, 2019.

A. Fanta & T. Rudl, *Leaked document: EU Commission mulls new law to regulate online platforms*, beschikbaar via: <https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms>.

R. Faris, H Roberts, B. Etling, N. Bourassa, E. Zuckerman, Y. Benkler, *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election*, Berkman Klein Center for Internet & Society Research Paper, <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33759251>.

Federal Election Commission, *AO 2017-12: Nonprofit must include disclaimers on its Facebook ads*, beschikbaar via: <https://www.fec.gov/updates/ao-2017-12-nonprofit-must-include-disclaimers-its-facebook-ads/>

Federal Office of Justice, Federal Office of Justice Issues Fine against Facebook, 3 July 2019, <https://perma.cc/9G3V-SJRN>. See <http://www.loc.gov/law/foreign-news/article/germany-facebook-found-in-violation-of-anti-fake-news-law/?loclr=eaglm>.

Financial Times, Facebook's fake numbers problem – lex in depth, 18 november 2019 van <https://www.ft.com/content/98454222-fef1-11e9-b7bc-f3fa4e77dd47>.

R. Fletcher, A. Cornia, L. Graves & R.K. Nielsen, *Measuring the reach of "fake news" and online disinformation in Europe*, Reuters Institute for the Study of Journalism Factsheet, <https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe>.

Fokkens, Noyon/Langemeijer/Rommelink Strafrecht, artikel 127 Sr, aant. 2.

Foreign & Commonwealth Office, *UK steps up fight against fake news*, <https://www.gov.uk/government/news/uk-steps-up-fight-against-fake-news>.

Foreign & Commonwealth Office, *Lord Neuberger and Amal Clooney announce Media Freedom Legal Panel members*, <https://www.gov.uk/government/news/lord-neuberger-and-amal-clooney-announce-media-freedom-legal-panel-members>.

D. Frau-Meigs, Societal costs of “fake news” in the Digital Single Market, European Union, [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/626087/IPOL_STU\(2018\)626087_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/626087/IPOL_STU(2018)626087_EN.pdf).

French Interministerial mission team, *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, Interim mission report - Regulation of social networks – Facebook experiment*, Submitted to the French Secretary of State for Digital Affairs https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf.

French Secretary of State for Digital Affairs, *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, Interim mission report - Regulation of social networks – Facebook experiment*, beschikbaar via: https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf.

D. Funke & D. Flamini, *A guide to anti-misinformation actions around the world*, beschikbaar via: <https://www.poynter.org/ifcn/anti-misinformation-actions>.

Full Fact, *Full Fact to start checking Facebook content as third-party factchecking initiative reaches the UK*, <https://fullfact.org/blog/2019/jan/full-fact-start-checking-facebook-content-third-party-factchecking-initiative-reaches-uk>.

Full Fact, *Tackling misinformation in an open society* https://fullfact.org/media/uploads/full_fact_tackling_misinformation_in_an_open_society.pdf.

General Secretariat of the Council, *Conclusions of the Council and of the Member States on securing free and fair European elections, as adopted by the Council on 19 February 2019*, 6573/1/19 beschikbaar via: <https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf>.

Gerritsma-Breur, C.M. & A.G. Nederlof, *Commentaar op Wetboek van Strafrecht art. 138ab* (strafrecht) (artikeltekst geldig vanaf 01-07-2015).

Ghosh, D., & Scott, B., *Digital Deceit. The Technologies Behind Precision Propaganda on the Internet*, 2018, p. 4 <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/>.

Google, *Google February report*, 2019.

Google, *Advertising Policy Help – Political content*, beschikbaar via: <https://support.google.com/adspolicy/answer/6014595?hl=en>.

Google, *An update on our political ads policy*, 20 november 2019 beschikbaar via: <https://blog.google/technology/ads/update-our-political-ads-policy/>

Google, *Election ads in Canada*, beschikbaar via: <https://support.google.com/adspolicy/answer/6014595?hl=en>.

W. Gorton, *Manipulating Citizens: How Political Campaigns: Use of Behavioral Social Science Harms Democracy*, New Political Science, no. 1, doi:10.1080/07393148.2015.1125119.

Government Communications Service, *RESIST: Counter-disinformation toolkit*, beschikbaar via: https://gcs.civilservice.gov.uk/wp-content/uploads/2019/03/RESIST_Toolkit.pdf.

Government of Canada, *Canada's Digital Charter: Trust in a digital world*, beschikbaar via: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

Government of Ireland, *First Report of the Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation*, <https://assets.gov.ie/2224/241018105815-07f6d4d3f6af-4c7eb710010f2ae09486.pdf>.

Government Offices of Sweden, "A practical approach on how to cope with disinformation", 6 October 2017,

A. Granchet, *FR - France*, in: M. Cappello, *Media coverage of elections: the legal framework in Europe*, beschikbaar via: https://www.ivir.nl/publicaties/download/IRIS_Special_2017_1.pdf.

GRECO, *Third Evaluation Round. Second Compliance Report on the Netherlands. Transparency of Party Funding*, 2012.

H.E.V. Guérend, *EU-Indonesia Seminar on Addressing Hate Speech and Disinformation with a Rights-Based Approach*, 2018, https://eeas.europa.eu/delegations/indonesia/52263/indonesia-and-eu-discuss-tackling-hate-speech-and-disinformation_en.

A. Guess, J. Nagler & J. Tucker, *Less than you think: Prevalence and predictors of fake news dissemination on Facebook*, 2019/ 5(1) Science Advances 1-8, DOI: 10.1126/sciadv.aau4586.

J. Harambam, *De/politisering van de Waarheid*". Sociologie, 2017/13(1), p. 73-92.

F. Hedman, F. Sivnert, B. Kollanyi, V. Narayanan, L.M. Neudert & P.H. Howard, *News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter*, *COMPROP Data Memo 2018.3*, beschikbaar via: <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/09/Hedman-et-al-2018.pdf>.

B. Heller & Joris van Hoboken, *Freedom of Expression: A Comparative Summary of United States and European Law*, Working Paper (Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2019). https://www.ivir.nl/publicaties/download/TWG_Freedom_of_Expression.pdf.

High Level Expert Group on Fake News and Online Disinformation, *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*, Luxemburg: Publications Office of the European Union 2018.

HM Government, *Online Harms White Paper* beschikbaar via: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

J. van Hoboken et al., *Hosting Intermediary Services and Illegal Content Online: An analysis of the scope of article 14 ECD in light of developments in the online service landscape*, z.p. : European Union 2018.

J. van Hoboken & D. Keller, *Design Principles for Intermediary Liability Laws, Transatlantic Working Group on Content Moderation Online and Freedom of Expression*, 8 October 2019, https://www.ivir.nl/publicaties/download/Intermediary_liability_Oct_2019.pdf.

House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and “fake news”*: Final Report, Eighth Report of Session 2017–19, House of Commons.

House of Commons, 1. “Democracy Under Threat: Risk and Solutions in the Era of Disinformation and Data Monopoly, Report of the Standing Committee on Access to Information, Privacy and Ethics”, 2018, <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf>.

House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and “fake news”*: Final Report, Eighth Report of Session 2017–19 beschikbaar via: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

Howard e.a., *Junk news and bots during the U.S. election: What were Michigan voters sharing over Twitter?* Computational Propaganda Data Memo, Oxford: Oxford Internet Institute.

Human Rights Committee, *Concluding Observations of the Human Rights Committee: Cameroon*, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2F%2F79%2FAdd.116&Lang=en.

International Institute for Democracy and Electoral Assistance (IDEA), *Online Political Crowdfunding*, Stockholm: International IDEA 2018.

Information Commissioner's Office, *Guidance on political campaigning*, beschikbaar via: https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf.

Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns: A report to Parliament*, beschikbaar via: <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>.

International Institute for Democracy and Electoral Assistance, “Online Political Crowdfunding”, 2018, <https://www.idea.int/sites/default/files/publications/online-political-crowdfunding.pdf>.

M. Isaaq, *Dissent Erupts at Facebook Over Hands-Off Stance on Political Ads*, The New York Times, 28 October 2019, <https://www.nytimes.com/2019/10/28/technology/facebook-mark-zuckerberg-political-ads.html?module=inline>

ISD & LSE, *Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election*, beschikbaar via: <http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf>.

J.-B. Jeangène Vilmer, A. Escorcía, M. Guillaume & J. Herrera, *Information Manipulation: A Challenge for Our Democracies*, Parijs: CAPS (Ministry for Europe and Foreign Affairs) & IRSEM (Ministry for the Armed Forces) 2018.

B. Johansson, *Sweden: Ten Years with Television Advertising* in C. Holtz-Bacha & M.R. Just, *Routledge Handbook of Political Advertising*, New York: Routledge 2017.

J. Katsirea, "Fake news": reconsidering the value of untruthful expression in the face of regulatory uncertainty, 2018/10, *Journal of Media Law* 159-188.

D. Keller, *Internet Platforms: Observations on Speech, Danger, and Money* (June 13, 2018). Hoover Institution's Aegis Paper Series, No. 1807, 2018. Available at SSRN: <https://ssrn.com/abstract=3262936>;

I. Van Keulen e.a. "Digitalisering van het nieuws—Online nieuwsgedrag, desinformatie en personalisatie in Nederland", 2018, Den Haag: Rathenau Instituut.

N. Khaliq, *Striking a Balance: Hate Speech, Freedom of Expression and Non-Discrimination*, Tolley's *Journal of Media Law and Practice*, vol. 15, no. 1, 1994, p. 27-28, <https://heinonline.org/HOL/P?h=hein.journal>

J. Killock & A. Shepherd, *UK: Online Harms Strategy must "design in" fundamental rights*, beschikbaar via: <https://edri.org/uk-online-harms-strategy-must-design-in-fundamental-rights>.

S. H. Kingma, *De botsing tussen IE- en privacyrechten. Het einde van het Lycos/Pessers-tijdperk*, P&I 2012/4 p. 171-177

F. Kistenkas, *Vrije straatcommunicatie. De rol van de lokale overheid bij de regulering van de uitingstvrijheid in rechtsvergelijkend perspectief*, Deventer/Arnhem: Kluwer/Gouda Quint 1989.

S. Kruscinski & A. Haller, "Restrictions on data-driven political microtargeting in Germany" *Internet Policy Review*, 6(4). DOI: 10.14763/2017.4.780.

F. La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, beschikbaar via: <https://undocs.org/A/HRC/26/30>.

Lage Drempeles, Hoge Dijken. Democratie en rechtstaat in balans (Eindrapport van de staatscommissie parlementair stelsel), bijlage bij Kamerstukken II 2018/19, 34430, nr. 9.

P. Leerssen, J. Ausloos, B. Zarouali, N. Helberger & C. de Vreese, *Platform Ad Archives: Promises and Pitfalls* beschikbaar via: <https://ssrn.com/abstract=3380409>.

Leidraad van de Raad voor Journalistiek, 2018 via <https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae>

M. Leiser, "AstroTurfing, "CyberTurfing" and other online persuasion campaigns" *European Journal of Law and Technology* 2016 afl. 1, p. 2.

Lili Levi, *Real Fake News and Fake Fake News*, 16 *First Amendment Law Review* 232-327.

U. von der Leyen, *A Union that strives for more - My agenda for Europe: Political Guidelines for the next European Commission 2019-2024* beschikbaar via: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

Chris Marsden and Trisha Meyer, *Regulating disinformation with artificial intelligence*, European Union, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU\(2019\)624279_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf).

T. McGonagle, *The Council of Europe against online hate speech: Conundrums and challenges*, Expert paper, Doc. No. MCM 2013(005), 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", Belgrade, 7-8 November 2013.

T. McGonagle, *Positive Obligations Concerning Freedom of Expression: Mere Potential or Real Power?* in O. Andreotti, *Journalism at Risk: Threats, Challenges and Perspectives*, Straatsburg: Council of Europe Publishing 2015, p. 9-35.

T. McGonagle, "De Raad van Europa en online desinformatie: laveren tussen zorgen en zorgplichten?", Mediaforum 2018 afl. 6, p. 180-186.

T. McGonagle e.a., "Inventarisatie methodes om "nepnieuws" tegen te gaan", Instituut voor Informatierecht, 2018, <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/25/inventarisatie-methodes-om-%E2%80%9Cnepnieuws%E2%80%9D-tegen-te-gaan/inventarisatie-methodes-om-%E2%80%9Cnepnieuws%E2%80%9D-tegen-te-gaan.pdf>

T. McGonagle, "Fake news": False fears or real concerns?, (2017) 35(4) Netherlands Quarterly of Human Rights 203-209.

T. McGonagle., "The Council of Europe and Internet Intermediaries: A Case-Study of Tentative Posturing", in Jorgensen, R., "Private Actors and Human Rights in the Online Domain", (MIT Publishing, forthcoming 2019).

T. McGonagle & Eugénie Coche, "Fake news" and online disinformation: Case study – Belgium (IViR, 2018), <https://www.ivir.nl/publicaties/download/Case-study-Fake-News-Belgium.pdf>.

T. McGonagle, M. Bednarski, M. Francese Coutinho and A. Zimin, Elections and Media in Digital Times, In-Focus edition of the World Trends in Freedom of Expression and Media Development Series, UNESCO 2019, https://www.ivir.nl/publicaties/download/elections_and_media_in_digital_times.pdf.

J.M. De Meij, G.A.I. Schuijt, A.W. Hins & A.J. Nieuwenhuis, *Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief*, Amsterdam: Cramwinckel 2000.

Microsoft, *Disallowed Content Policies - Political and religious content*, beschikbaar via: <https://about.ads.microsoft.com/en-us/resources/policies/disallowed-content-policies>.

Moeller, Helberger & Makhortykh, "Filterbubbels in Nederland" Instituut voor Informatierecht, 2019.

R. S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", 2019, Department of Justice , <https://www.justice.gov/storage/report.pdf>.

M. Murgia, S. Findlay & A. Schipani, *India: the WhatsApp election*, Financial Times 5 mei 2019.

J.S. Nan, *Commentaar op Wetboek van Strafrecht art. 126 (Strafrecht)* (artikeltekst geldig vanaf 01-05-1984).

P.M. Napoli, *What If More Speech Is No Longer the Solution: First Amendment Theory Meets Fake News and the Filter Bubble*, 2018/70 Federal Communications Law Journal 55-104.

V. Narayanan et al., *Russian Involvement and Junk News during Brexit*, <http://blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2017/12/Russia-and-Brexit-v27.pdf>.

Neudert, L.M.N., "Computational Propaganda in Germany: A Cautionary Tale", Computational Propaganda Working Paper, 2017.7, Oxford: Oxford Internet Institute; Rogers, R., & Niederer, S. "The politics of social media manipulation: A view from the Netherlands", 2019, p. 17; Bayer, J., et al., "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States", 2019, European Union, p. 22

Lisa-Maria Neudert, Bence Kollanyi and Philip N. Howard, "Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?", COMPROP Data Memo 2017.7, 19 September 2017, http://blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2017/09/ComProp_GermanElections_Sep2017v5.pdf.

A.C. Nicolas, *Taming the Trolls: The Need for an International Legal Framework to Regulate State Use of Disinformation on Social Media*, 107 Georgetown Law Journal Online 36-62.

R.K. Nielsen & L. Graves, *News you don't believe: Audience perspectives on fake news*, Reuters Institute for the Study of Journalism Factsheet, <https://reutersinstitute.politics.ox.ac.uk/our-research/news-you-dont-believe-audience-perspectives-fake-news>.

NOS, "Bits of Freedom: *Facebook gaat de fout in met politieke advertenties*", 20 mei 2019 <https://nos.nl/nieuwsuur/artikel/2285561-bits-of-freedom-facebook-gaat-de-fout-in-met-politieke-advertenties.html>.

Noyon, Langemeijer & Rammelink, *Strafrecht*, artikel 125 Sr, aant. 7.

ODIHR Election Expert Team, *Sweden General Elections 2018*, beschikbaar via: <https://www.osce.org/odihr/elections/sweden/403760?download=true>.

OFCOM, *Online market failures and harms: an economic perspective on the challenges and opportunities in regulating online services* (OFCOM, 2019)

OSCE, *Republic of France Presidential Election 23 April and 7 May 2017*, OSCE/ODIHR Election Expert Team Final Report, beschikbaar via: <https://www.osce.org/odihr/elections/france/337346?download=true>.

OSCE, *Election Expert Team, Elections to the Federal Parliament (Bundestag) 24 September 2017* beschikbaar via: <https://www.osce.org/odihr/elections/germany/358936?download=true>.

OSCE Representative on Freedom of the Media, *Law further restricting speech in Russia might negatively affect freedoms of media and of information on Internet*, says OSCE Representative, <https://www.osce.org/representative-on-freedom-of-media/406775>

OSCE Media Freedom Representative publishes legal review of French laws against manipulation of information, <https://www.osce.org/representative-on-freedom-of-media/408926>.

A. Park & K.H. Youm, *Fake News from a Legal Perspective: The United States and South Korea Compared*, 25 *Southwestern Journal of International Law* 100-119.

PEN International, *Russia: New laws threaten freedom of expression and media freedom*, 1 April 2019, <https://pen-international.org/news/russia-new-laws-threaten-freedom-of-expression-and-media-freedom>.

W. Philips, "This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture", MIT Press 2015.

R.H.M. Pierik, *Mandatory Vaccination: an Unqualified Defence*. Journal of Applied Philosophy, 35(2), 381-398. <https://doi.org/10.1111/japp.12215>.

R.H.M. Pierik, *Past een vaccinatieplicht binnen het EVRM-regime? Tijdschrift voor Gezondheidsrecht*, 43(4), 8-25. <https://doi.org/10.5553/TvGR/016508742019043004002>

C. Plaizier, *Micro-Targeting Consent: A Human Rights Perspective On Paid Political Advertising On Social Media*, LL.M. Thesis, Informatierecht, University of Amsterdam (2018), <http://www.scriptiesonline.uba.uva.nl/scriptie/650580>.

P. Pomerantsev, *The UK White Paper on Online Harms and the Dangers of Regulating Disinformation*, Transatlantic Working Group on Content Moderation Online and Freedom of Expression, 1 October 2019, https://www.ivir.nl/publicaties/download/Cycle_Censorship_Pomerantsev_Oct_2019.pdf.

Radio Sweden, "Media outlets to join forces to combat disinformation and fake news", 29 January 2018, <https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6870996>.

Reddit, *Reddit Advertising Policy – Political Advertisements*, beschikbaar via: <https://www.reddithelp.com/en/categories/advertising/policy-guidelines/reddit-advertising-policy>.

A. Renda, *The legal framework to address "fake news": possible policy actions at the EU level*, European Union.

A. Richter, *Fake News and Freedom of the Media*, (2018) 8(1) Journal of International Media & Entertainment Law 1-34.

A. Richter, *Russian Federation: False information amendments made*, IRIS 2019-5/24, <https://merlin.obs.coe.int/iris/2019/5/article24.en.html>.

B. Rieder, "From ranking algorithms to ranking cultures. Investigating the modulation of visibility in YouTube search results", *The International Journal of Research into New Media Technologies*, 2018 afl. 24/1.

L. Reppell & E. Shein, *Disinformation Campaigns and Hate Speech: Exploring the Relationship and Programming Interventions*, International Foundation for Electoral Systems, 2019, p. 1, https://www.ifes.org/sites/default/files/2019_ifes_disinformation_campaigns_and_hate_speech_briefing_paper.pdf.

R. Rogers & S. Niederer, *The politics of social media manipulation: A view from the Netherlands*, International Federation for Information Processing: z.p. 2019.

L. Rosenberger & B. Hanlon, "Countering Information Operations Demands A Common Democratic Strategy" (Alliance for Securing Democracy, 2019),

J. Rowbottom, *Lies, Manipulation and Elections - Controlling False Campaign Statements*, 2012, 32(3) Oxford Journal of Legal Studies, p. 507-535.

K. Sainsbury-Carter, *Changes to our Political Ads Policy*, beschikbaar via: <https://about.ads.microsoft.com/en-us/blog/post/october-2018/changes-to-our-political-ads-policy>.

R.J.B. Schutgens, "Jezus Redt. Beperking van de uitingsvrijheid door welstandseisen", *Ars Aequi* 2011, afl 2.

Secretary of State for Digital Affairs, *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, Interim mission report - "Regulation of social networks – Facebook experiment,"* Submitted to the French Secretary of State for Digital Affairs (May 2019), via https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf.

Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department, *Online Harms White Paper*, beschikbaar via: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

Service d'information du Gouvernement, *Combating the manipulation of information*, beschikbaar via: <https://www.gouvernement.fr/en/combating-the-manipulation-of-information>.

A. Shahbaz, U.S. Initiatives to Counter Harmful Speech and Disinformation on Social Media, Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 11 June 2019, https://www.ivir.nl/publicaties/download/US_Initiatives_Harmful_Speech_Disinformation-1.pdf.

Smearing Sweden, *International Influence Campaigns in the 2018 Swedish Election*, p. 6, <http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf>.

B. Smith-Meyer, L. Bayer & J. Hanke, *EU officials float €100B boost for European companies*, Politico 25 august 2019, via https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/08/clean_definite2.pdf,

Report of the Special Rapporteur on "The promotion and protection of the right to freedom of opinion and expression", Human Rights Council, 2014, par. 82, <https://undocs.org/A/HRC/26/30>.

United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint declaration on freedom of expression and "fake news", disinformation and propaganda*, FOM.GAL/3/17, 3 March 2017, <https://www.osce.org/fom/302796?download=true>.

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *A/HRC/38/35*, 6 April 2018, , <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>.

Stichting Reclame Code, *Jaarverslag Stichting Reclame Code 2017*, beschikbaar via: <https://www.reclamecode.nl/over-src/jaarverslagen/>.

Standing Committee on Access to Information, Privacy and Ethics 2018, *Democracy Under Threat: Risk and Solutions in the Era of Disinformation and Data Monopoly, Report of the Standing Committee on Access to Information, Privacy and Ethics* beschikbaar via: <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf>.

Swedish Civil Contingencies Agency, *Countering information influence activities – A handbook for communicators* (MSB, 2019), <https://rib.msb.se/filer/pdf/28698.pdf>.

Staatscommissie Parlementair Stelsel, *Lage Dremfels, Hoge Dijken. Democratie en rechtstaat in balans* Den Haag 2018, bijlage bij Tweede Kamer, vergaderjaar 2018-2019, 34 430, nr. 9.

J. Stuyck, E. Terryn & T. Van Dyck, *Confidence through fairness? The new directive on unfair business-to-consumer commercial practices in the internal market*, Common Market Law review 2006, 43, pp. 107; De Very, R.W., "Handelspraktijken en reclame", in: E.H. Hondius & G.J. Rijken, *Handboek Consumentenrecht*, 2015 Zutphen: uitgeverij Paris

D. Susser, B. Roessler & H. Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, Georgetown Law Technology Review, Forthcoming 2019, p. 24, <https://ssrn.com/abstract=3306006>.

Swedish Civil Contingencies Agency, "Countering information influence activities – A handbook for communicators", 2019, MSB, <https://rib.msb.se/filer/pdf/28698.pdf>.

Swedish Security Service, *Attempts to influence confidence in the election process*, 31 August 2018, <https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-08-31-attempts-to-influence-confidence-in-the-election-process.html>

E.C. Tandoc Jr., Z.W. Lim & R. Ling, *Defining "Fake News"*, 2018/6(2) Digital Journalism 137-153.

D. Tambini, *How advertising fuels fake news. LSE Media Policy Project Blog*, <http://blogs.lse.ac.uk/mediapolicyproject/2017/02/24/how-advertising-fuels-fake-news/>

The Electoral Commission, *Digital campaigning: Increasing transparency for voters*, beschikbaar via: https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Digital-campaigning-improving-transparency-for-voters.pdf.

V. Tommaso, *From Fake to Junk News, the Data Politics of Online Virality*, in: Bigo, D. Isin, E. & Ruppert, E. (eds), "Data Politics: Worlds, Subjects, Rights", London: Routledge, 2019,. <https://hal.archives-ouvertes.fr/hal-02003893>.

J.A. Tucker, A. Guess, P. Barberá, C. Vaccari, A. Siegel, S. Sanovich, D. Stukal & B. Nyhan, *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, Hewlett Foundation Report, <https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf>.

Twitter, *Political Content in the European Union*, beschikbaar via: <https://business.twitter.com/en/help/ads-policies/restricted-content-policies/political-content/eu-political-content.html>.

H. Tworek & P. Leerssen, *An Analysis of Germany's NetzDG Law*, Working Paper (Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2019), https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf

Government Communications Service, *(RESIST: Counter-disinformation toolkit*, https://gcs.civilservice.gov.uk/wp-content/uploads/2019/03/RESIST_Toolkit.pdf.

UK Government, *Online harms white paper*, 2019 via https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

UN Human Rights Committee, General comment No. 34, CCPR/C/GC/34, 12 September 2011, r.o. 1; Canataci, A. e.a., "Privacy, free expression and transparency" UNESCO, 2016, <https://unesdoc.unesco.org/ark:/48223/pf0000246610>.

The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and "Fake News"*, beschikbaar via: <https://www.osce.org/fom/302796?download=true>.

U.S. Department of Justice, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, beschikbaar via: <https://www.justice.gov/storage/report.pdf>.

Venice Commission, *Joint Report of the Venice Commission and of the Directorate of Information Society and Action Against Crime of the Directorate General of Human Rights and Rule of Law (DGI)*, beschikbaar via: [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2019\)016-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-e).

K. Verhoeven, *Actieplan Digitale Advertenties*, beschikbaar via: <https://d66.nl/digital-advertising/>.

Verkade, *Tekst & Commentaar Intellectuele eigendom*, Verspreidingsdelict, in voorraad hebben; culpoze variant bij: Auteurswet, Artikel 32.

J. B. Vilmer, *Information Manipulation: A Challenge for Our Democracies*

R. Vliegthart & S. Kruikemeier, *Political Advertising in the Netherlands: (Still) Little to do About (Almost) Nothing In*: Holz-Bacha, C., & Just, M.R. (ed.) Routledge Handbook of Political Advertising, New York: Routledge, p. 370 2017.

R. W. De Vrey, *Handelspraktijken en reclame*, in: Hondius, E.H. & Rijken, G.J., *Handboek Consumentenrecht*, 2015 Zutphen: uitgeverij Paris, p. 405.

Volkskrant, "Vaccinatieweigeraars: waarom anti-vaxxers zo veel weerstand oproepen" 2019, <https://www.volkskrant.nl/nieuws-achtergrond/vaccinatieweigeraars-waarom-anti-vaxxers-zo-veel-weerstand-oproepen~baad1ac0/>.

J. Wakefield, *Facebook employs UK fact-checkers to combat fake news*, BC News, 11 January 2019, <https://www.bbc.com/news/technology-46836897>

B. Wagner, *Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech*, in M. Moore & D. Tambini, *Digital Dominance the Power of Google, Amazon, Facebook, and Apple*, Oxford: Oxford University Press 2018.

C. Wardle, *Understanding Information Disorder*, First Draft, October 2019

C. Wardle & H. Derakhshan, *Information Disorder. Toward an interdisciplinary framework of research and policymaking*, Straatsburg: Strasbourg Cedex 2017.

B.E. Weeks, *Emotions, Partisanship, and Misperceptions: How Anger and Anxiety Moderate the Effect of Partisan Bias on Susceptibility to Political Misinformation*, 2015/65(4) Journal of Communication 699-719.

WhatsApp, "Bijdragen aan de veiligheid van verkiezingen in India",
<https://faq.whatsapp.com/en/26000233/https://faq.whatsapp.com/en/26000233/>.

J. Weinstein, *Climate Change Disinformation, Citizen Competence, and the First Amendment*, 89 University of Colorado Law Review 341-376.

Wetenschappelijke Raad voor het Regeringsbeleid, *Voorbereiden op digitale ontworping*, Den Haag: WRR 2019.

J.L. Williams, *Cavalier Bot Regulation and the First Amendment's Threat Model*, Knight First Amendment Institute, 21 August 2019, <https://knightcolumbia.org/content/cavalier-bot-regulation-and-the-first-amendments-threat-model>.

R.E. de Winter, *De heersende leer: honderd jaar verspreidingsjurisprudentie:1892-1992*, Den Haag: SDU 1993.

S. Wong, C. Shepherd & Q. Liu, *Old messages, new memes: Beijing's propaganda playbook on the Hong Kong protests*, Financial Times, 2019.

M.A.H. van der Woude, T&C Strafrecht, commentaar op artikel 126 Sr

A.K. Wood and A.M. Ravel, *Fool Me Once: Regulating "Fake News" and Other Online Advertising*, 2018/91 *Southern California Law Review* 1223-1278.

WRR rapport "Voorbereiden op Digitale Ontworping", September 2019.

Zuiderveen Borgesius et al 2018, *"Online Political Microtargeting: Promises and Threats for Democracy"*, Utrecht Law Review 2018.

Bijlage: Landenstudies

Per land wordt een algemeen overzicht gepresenteerd, gevolgd door een beschrijving van de desinformatieregelgeving (met inbegrip van de voorgestelde regelgeving) en regelgeving met betrekking tot politieke advertenties.

A. Inleiding tot de landenstudies

In de volgende paragrafen wordt de regulering van desinformatie en betaalde politieke advertenties in zes landen (VK, Frankrijk, Duitsland, Zweden, VS en Canada) beschreven.

Veel nationale regeringen, zoals het Verenigd Koninkrijk,⁶⁰⁹ Frankrijk⁶¹⁰ en Duitsland⁶¹¹ onderzoeken de kwestie van desinformatie en hebben daarover relevante rapporten gepubliceerd. Wat wetgeving betreft, is Frankrijk echter het enige land dat in 2018 met zijn Law on Manipulation of Information (zie hieronder) specifieke wetgeving heeft aangenomen om desinformatie tegen te gaan. Duitsland heeft in 2018 de Netzwerkdurchsetzungsgesetz uitgevaardigd, maar deze wet bevat geen specifieke bepaling over desinformatie, aangezien het gaat om 22 reeds bestaande strafbare feiten (zie hieronder).

Er zijn veel niet-wetgevende initiatieven van de overheid om desinformatie op te sporen en tegen te gaan, die niet zo ver gaan als wettelijke voorschriften, bijvoorbeeld door de publicatie van toolkits. Voorbeelden hiervan zijn de *toolkit* van de communicatiedienst van de Britse regering ten aanzien van *Counter-disinformation toolkit*⁶¹² of het handboek van het Zweedse Bureau voor civiele rampenbestrijding getiteld *Countering information influence activities*.⁶¹³ Het Poynter Institute for Media Studies onderhoudt een nuttige bijgewerkte wegwijzer op het gebied van *anti-misinformation actions around the world* met daarin een overzicht van de maatregelen in het Verenigd Koninkrijk, Frankrijk, Duitsland, Zweden, de Verenigde Staten en Canada.⁶¹⁴

Met betrekking tot politieke advertenties moet allereerst worden opgemerkt dat er zeer uiteenlopende regels gelden, afhankelijk van de vraag of de politieke advertenties in een krant worden geplaatst, op de televisie worden uitgezonden of via een internetdienst worden verspreid. De regels die van toepassing zijn op verschillende media zijn hieronder opgenomen om te helpen bij het verkennen van mogelijke beleidsopties voor de regulering van politieke advertenties die door internetdiensten in Nederland worden verspreid. Voorafgaand aan de analyse van de regulering van betaalde politieke advertenties wordt de stand van zaken van de desinformatieregelgeving gepresenteerd, evenals een algemene evaluatie van de behandeling van desinformatie en politieke advertenties door het betreffende rechtssysteem. De landenstudies richten zich op de specifieke kenmerken van elk land. Hierbij wordt niet ingegaan op de regels die op EU-niveau van toepassing zijn en die in de nationale wetgeving zijn omgezet, zoals de AVG, de e-Privacy Richtlijn of de AVMD.

609 House of Commons Digital, Culture, Media and Sport Committee, *'Disinformation and 'fake news': Final Report, Eighth Report of Session 2017–19'*, 2019; UK Government, *'Online Harms White Paper'*, 2019.

610 Jeangène Vilmer, J.B. et. al, *'Information Manipulation: A Challenge for Our Democracies'*, Ministry for Europe and Foreign Affairs and the Ministry for the Armed Forces, 2018, p. 173, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

611 Idem.

612 Government Communications Service, *'RESIST: Counter-disinformation toolkit, 2019'*, https://gcs.civilservice.gov.uk/wp-content/uploads/2019/03/RESIST_Toolkit.pdf.

613 Swedish Civil Contingencies Agency, *'Countering information influence activities – A handbook for communicators'* (MSB, 2019), <https://rib.msb.se/filer/pdf/28698.pdf>.

614 Funke, D. & Flamini, D., *'A guide to anti-misinformation actions around the world'*, Poynter, 27 October 2018, <https://www.poynter.org/ifcn/anti-misinformation-actions>.

In tegenstelling tot desinformatie zijn er wel een aantal voorbeelden van nieuwe wetgeving ten aanzien van politieke advertenties op internetdiensten. Sinds 2018 hebben Canada, Frankrijk en een aantal Amerikaanse staten (zie hieronder) wetgeving ingevoerd, vooral op het gebied van transparantie, en het effect is vrij significant: sommige internetdiensten staan in bepaalde landen en Amerikaanse staten geen politieke advertenties meer toe voor verkiezingen.

In de VS staat Google Inc. bijvoorbeeld niet langer politieke advertenties toe voor verkiezingen in Maryland, New Jersey, Nevada en Washington.⁶¹⁵ Microsoft Inc. accepteert ook niet langer politieke kandidaat- en stemmingsadvertenties in de VS, als gevolg van “regulators from states across the country have taken new steps to bring additional transparency and accountability to political advertising.”⁶¹⁶ Dit verbod is nu wereldwijd van kracht. Ook in Frankrijk staat Twitter Inc. geen politieke campagnes en issue advocacy ads toe.⁶¹⁷ In Canada kondigde Google Inc. aan dat tijdens de Canadese federale verkiezingen van juni tot oktober 2019 politieke advertenties op Google-platforms in Canada niet zou worden toegestaan.⁶¹⁸

B. Verenigd Koninkrijk

i. Algemene karakterisering

De kwestie van desinformatie en online politieke advertenties staat sinds het Brexit-referendum van 2016 hoog op de politieke agenda in het Verenigd Koninkrijk. Er zijn tal van rapporten over desinformatie en online politieke advertenties van de Britse regering,⁶¹⁹ het parlement⁶²⁰ en de Information Commissioner's Office (“ICO”)⁶²¹ en de Electoral Commission.⁶²² In juli 2019 kondigde de Britse regering aan dat zij 18 miljoen pond aan overheidsfinanciering willen uittrekken om de onafhankelijke media te versterken en desinformatie en fake news in Oost-Europa en de westelijke Balkan tegen te gaan.⁶²³ De Britse regering heeft in juli 2019 een panel van juridische deskundigen op het gebied van mediavrijheid opgericht, onder voorzitterschap van een voormalige voorzitter van het Britse Hooggerechtshof.⁶²⁴ Verder kondigden de BBC en de European Broadcasting Union in september 2019 een nieuwe samenwerking aan om desinformatie aan te pakken, onder meer in samenwerking met grote nieuwsuitgevers, Google, Twitter en Facebook. De nieuwe samenwerkingsinitiatieven omvatten: (a) creation of an Early Warning System, so organisations can alert each other rapidly when they discover disinformation which threatens human life or disrupts democracy during elections; (b) Media Education: a joint online media education campaign to support and promote media education messages; and (c) Voter Information: co-operation on civic information

615 Zie: Google, ‘Advertising Policy Help – Political content - State election ads in the United States’, <https://support.google.com/adspolicy/answer/6014595?hl=en> (accessed 14 August 2019).

616 Sainsbury-Carter, K., ‘Changes to our Political Ads Policy’, 2018 <https://about.ads.microsoft.com/en-us/blog/post/october-2018/changes-to-our-political-ads-policy>.

617 Twitter, ‘Political Content in the European Union’, <https://business.twitter.com/en/help/ads-policies/restricted-content-policies/political-content/eu-political-content.html>.

618 See, Google, Election ads in Canada, <https://support.google.com/adspolicy/answer/6014595?hl=en>. See also, Tom Cardoso, ‘Google to ban political ads ahead of federal election, citing new transparency rules’, The Globe and Mail, 4 March 2019, <https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/>.

619 UK Government, ‘Online Harms White Paper’, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

620 House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and ‘fake news’: Final Report, Eighth Report of Session 2017–19* (House of Commons, 2019).

621 Information Commissioner's Office, ‘Investigation into the use of data analytics in political campaigns: A report to Parliament’, 2018, p. 24, <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>.

622 Electoral Commission, ‘Digital campaigning: Increasing transparency for voters’, 2018, The Electoral Commission, p. 15, https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Digital-campaigning-improving-transparency-for-voters.pdf.

623 Foreign & Commonwealth Office, ‘UK steps up fight against fake news’, 7 July 2019, <https://www.gov.uk/government/news/uk-steps-up-fight-against-fake-news>.

624 Foreign & Commonwealth Office, ‘Lord Neuberger and Amal Clooney announce Media Freedom Legal Panel members’, 11 July 2019, <https://www.gov.uk/government/news/lord-neuberger-and-amal-clooney-announce-media-freedom-legal-panel-members>.

around elections, so there is a common way to explain how and where to vote.⁶²⁵ De *communications regulator* OFCOM heeft onlangs ook een rapport gepubliceerd over online marktfalen en internetdiensten.⁶²⁶

Met name met betrekking tot online politieke advertenties heeft het ICO verklaard dat het een “disturbing disregard for voters [personal privacy]” heeft gesignaleerd door spelers in het hele politieke ecosysteem - van databedrijven en datamakelaars tot sociale mediaplatforms, campagnegroepen en politieke partijen.⁶²⁷ De Electoral Commission heeft een aantal veranderingen van de toepasselijke kieswetten ten aanzien van online politieke advertenties aanbevolen, waaronder: (a) election and referendum adverts on social media platforms should be labelled to make the source clear; (b) campaigners should be required to provide more detailed and meaningful invoices from their digital suppliers to improve transparency, and (c) clarifying that spending on election or referendum campaigns by foreign organisations or individuals is not allowed.⁶²⁸

ii. Regulering van desinformatie

Ten eerste bestaat er een specifieke bepaling in de kieswetgeving met regels voor het afleggen van valse feitelijke verklaringen met betrekking tot een politieke kandidaat. In het kader van de Representation of the People Act 1983 is het een overtreding van de wet om met het doel van de terugkeer van een kandidaat bij de verkiezingen te beïnvloeden, een valse feitelijke verklaring met betrekking tot het persoonlijke karakter of het gedrag van de kandidaat te publiceren.⁶²⁹ In 2019 vernietigde de High Court een dagvaarding tegen de Britse politicus Boris Johnson voor wangedrag in een openbaar ambt wegens “endorsing and making statements which were false and misleading, without justification concerning the cost of European Union membership.”⁶³⁰ De High Court besprak de beperkte reikwijdte van False Statement Law en stelde dat het parlement opzettelijk “excluded any other form of false statement of fact, including those relating to publicly available statistics.”⁶³¹

Ten tweede moet de Britse overheid op grond van de Digital Economy Act 2017 een gedragscode uitvaardigen voor online sociale mediaplatforms met betrekking tot de wijze waarop platforms actie ondernemen tegen het gebruik van platforms voor bepaald schadelijk gedrag, waaronder pesten, beledigen of gedrag dat individuen kan intimideren of vernederen.⁶³² In 2019 werd na consultatie de gedragscode voor aanbieders van online sociale mediaplatforms gepubliceerd.⁶³³ De vier kernbeginselen van deze gedragscode zijn: (a) maintain a clear and accessible reporting process to enable individuals to notify social media providers of harmful conduct; (b) maintain efficient processes for dealing with notifications from users about harmful conduct, including acknowledgement within 24 hours, (c) have clear and accessible information about reporting processes in their terms and condition; and (d)

625 BBC Media Centre, ‘New collaboration steps up fight against disinformation’, 7 September 2019, <https://www.bbc.co.uk/mediacentre/latestnews/2019/disinformation>.

626 OFCOM, *Online market failures and harms: an economic perspective on the challenges and opportunities in regulating online services* (OFCOM, 2019), https://www.ofcom.org.uk/_data/assets/pdf_file/0025/174634/online-market-failures-and-harms.pdf.

627 Information Commissioner’s Office, ‘Information Commissioner’s report brings the ICO’s investigation into the use of data analytics in political campaigns up to date’, 2018, <https://ico.org.uk/about-the-ico/news-and-events/blog-information-commissioner-s-report-brings-the-ico-s-investigation-into-the-use-of-data-analytics-in-political-campaigns-up-to-date/>.

628 Electoral Commission, ‘Digital campaigning: Increasing transparency for voters’, 2018, p. 3.

629 Representation of the People Act 1983, section 106, <http://www.legislation.gov.uk/ukpga/1983/2>. For an analysis, see Rowbottom, J., ‘Lies, Manipulation and Elections - Controlling False Campaign Statements’, 2012, 32(3) Oxford Journal of Legal Studies, p. 507-535.

630 Johnson v Westminster Magistrates Court [2019] EWHC 1709 (Admin), par. 4.

631 Idem, par. 36.

632 Digital Economy Act 2017, section 103, <http://www.legislation.gov.uk/ukpga/2017/30/section/103/enacted>.

633 Department of Digital, Culture, Media and Sport, ‘Code of Practice for providers of online social media platforms’, 12 April 2019, <https://www.gov.uk/government/publications/code-of-practice-for-providers-of-online-social-media-platforms>.

give clear information to the public about action they take against harmful conduct. De code vormt de leidraad in de aanloop naar een nieuw regelgevend kader.

Ten derde heeft de Britse regering in april 2019 voorstellen gepubliceerd om een nieuw regelgevend kader te creëren om illegale en schadelijke online-inhoud, met inbegrip van desinformatie, aan te pakken⁶³⁴ (civil society heeft ook reacties op de *White Paper* gepubliceerd⁶³⁵). De regering verklaarde dat zij “particularly worried about disinformation (information which is created or disseminated with the deliberate intent to mislead; this could be to cause harm, or for personal, political or financial gain”. Het centrale element van het voorstel is om een nieuwe wettelijke zorgplicht op te leggen aan bepaalde technologiebedrijven tot het nemen van “reasonable steps to keep their users safe and tackle illegal and harmful activity on their services”.⁶³⁶ Van belang is dat de wettelijke zorgplicht door een onafhankelijke toezichthouder zou worden gehandhaafd en dat deze toezichthouder aangeeft hoe bedrijven hun wettelijke verplichtingen onder de nieuwe gedragscode zullen vervullen. De regelgeving zou zich richten op “companies of all sizes” die diensten aanbieden die gebruikers in staat stellen om door gebruikers gegenereerde inhoud te delen of om met elkaar interactie aan te gaan, met inbegrip van sociale-mediabedrijven en openbare discussiefora. Het kader zal een andere aanpak hanteren voor privé-communicatie, waarbij de eisen om inhoud te scannen of te controleren op nauwkeurig omschreven categorieën illegale inhoud niet van toepassing zullen zijn op dergelijke communicatiekanalen.⁶³⁷

De voorgestelde wettelijke zorgplicht zou van toepassing zijn op de aanpak van desinformatie door technologiebedrijven en deze verplichten tot het nemen van “proportionate and proactive measures to help users understand the nature and reliability of the information they are receiving, to minimise the spread of misleading and harmful disinformation and to increase the accessibility of trustworthy and varied news content”. De nieuwe toezichthouder zou de eisen in een gedragscode verder dienen in te vullen, met inbegrip van “(a) steps that companies should take in relation to users who deliberately misrepresent their identity to spread and strengthen disinformation; (b) making content which has been disputed by reputable fact-checking services less visible to users; (c) promoting authoritative news sources; and (d) ensuring that it is clear to users when they are dealing with automated accounts, and that automated dissemination of content is not abused”. Een specifiek element dat aandacht verdient is dat bedrijven zouden worden verplicht “[to] ensure that algorithms selecting content do not skew towards extreme and unreliable material in the pursuit of sustained user engagement”.⁶³⁸

Ten slotte worden in het voorstel de handhavingsbevoegdheden van de toezichthouder uiteengezet, waaronder de bevoegdheid om boetes op te leggen. Het voorstel kan echter ook aanvullende bevoegdheden introduceren, zoals de verplichtingen voor derde bedrijven om de door hen verleende diensten die direct of indirect de toegang tot de dienst vergemakkelijken, de verplichting tot het blokkeren van websites of apps die niet aan de voorschriften voldoen, en de mogelijke aansprakelijkheid van bestuurders. Ten aanzien van de vraag naar een algemene filterverplichting is in het voorstel opgenomen dat het nieuwe kader moet voorzien in effectief toezicht met betrekking tot de verwijdering van illegale inhoud en dat het nieuwe kader nieuwe specifieke toezichtverplichtingen zal introduceren voor nauw gedefinieerde categorieën van illegale inhoud.⁶³⁹

634 Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department ‘*Online Harms White Paper*’, April 2019, <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper>.

635 Article 19, ‘*Response to the Consultations on the White Paper on Online Harms*’, June 2019, <https://www.article19.org/resources/uk-article-19-response-to-online-harms-white-paper/>.

636 Idem, p. 42.

637 Idem, p. 50.

638 Idem, p. 72.

639 Idem, p. 63.

iii. Regelgeving inzake politieke advertenties

Er gelden verschillende regels voor politieke advertenties, afhankelijk van de vraag of het gaat om gedrukte advertenties, advertenties via omroepen of online advertenties.

1. Kranten en omroepen

Hoewel er geen specifieke regelgeving is voor betaalde politieke advertenties in kranten buiten de verkiezingsperiode, zijn tijdens de verkiezingsperiode bepaalde politieke advertenties in kranten onderworpen aan een transparantieregel. Volgens de Political Parties, Elections and Referendums Act 2000 moet "election material", dat een "advertisement" in een krant is, de naam en adres van de promotor van dit materiaal en de naam van de persoon in wiens belang het materiaal wordt gepubliceerd, bevatten.⁶⁴⁰

Daarentegen zijn betaalde politieke advertenties op televisie te allen tijde verboden, ook tijdens verkiezingen.⁶⁴¹ Belangrijk is dat het EHRM in 2013 heeft geoordeeld dat dit verbod op politieke advertenties, zoals dat van toepassing is op de politieke advertenties van een dierenrechtenorganisatie, geen schending inhoudt van het recht op vrijheid van meningsuiting in artikel 10 EVRM.⁶⁴² Het EHRM aanvaardde de argumentatie van de Britse regering voor het verbod, waaronder de noodzaak om het democratische debat en het democratisch proces te beschermen tegen verstoring door machtige financiële groepen. Het moet echter worden opgemerkt dat *niet-betaalde* partijpolitieke uitzendingen, alsmede uitzendingen van campagnes van de referendumcampagnegroepen op bepaalde tijdstippen in de vorm van gratis zendtijd zijn toegestaan, maar wel onderworpen zijn aan strenge regelgeving.⁶⁴³

2. Internet diensten

In Engeland en Wales is er geen specifieke regelgeving voor online betaalde politieke advertenties. Het verdient opmerking dat er in Schotland een speciale transparantieregel is toegevoegd in het kader van de Scottish Independence Referendum Act 2013, die alleen in Schotland van toepassing was en op grond waarvan alle inhoud, met inbegrip van online inhoud dat verband houdt met het Schotse referendum, de "name and address of the promoter of the material" moest bevatten.⁶⁴⁴ De Britse Electoral Commission heeft in 2017 aanbevolen om in het hele Verenigd Koninkrijk een soortgelijke regel in te voeren, om te waarborgen dat een "appropriate level of imprint information should be required on online and electronic referendum campaign material".⁶⁴⁵ De Commissie heeft in 2018 opnieuw aanbevolen om de Britse wetgeving zodanig te hervormen dat "digital material must have an imprint saying who is behind the campaign and who created it".⁶⁴⁶

Hoewel betaalde politieke advertenties online niet specifiek worden beperkt door middel van regelgeving, is een aantal belangrijke regels voor verkiezingsuitgaven van toepassing op uitgaven voor politieke advertenties. De Britse verkiezingscommissie heeft benadrukt dat de regels inzake verkiezingsuitgaven "cover the costs of placing adverts on digital platforms or websites. They include the costs of distributing and targeting digital campaign materials or developing and using databases for digital campaigning. This applies even if the original purchase of hardware or software materials falls outside the regulated period for reporting spending."⁶⁴⁷

⁶⁴⁰ Political Parties, Elections and Referendums Act 2000, section 143(5), <http://www.legislation.gov.uk/ukpga/2000/41/section/143>.

⁶⁴¹ Communications Act 2003, sections 319(2)(g) and 321(2), <http://www.legislation.gov.uk/ukpga/2003/21/section/321>.

⁶⁴² Animal Defenders International v. the United Kingdom (Application no. 48876/08) 22 April 2013 (Grand Chamber).

⁶⁴³ Communications Act 2003, sections 319(2)(g) and 321(2), <http://www.legislation.gov.uk/ukpga/2003/21/section/321>.

⁶⁴⁴ Scottish Independence Referendum Act 2013, section 27(1)(b), <http://www.legislation.gov.uk/asp/2013/14/enacted>.

⁶⁴⁵ The Electoral Commission, 'The 2016 EU Referendum: Report on the regulation of campaigners at the referendum on the UK's membership of the European Union held on 23 June 2016', 2017, p. 41, https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Report-on-the-regulation-of-campaigners-at-the-EU-referendum.pdf.

⁶⁴⁶ The Electoral Commission, 'Digital campaigning: Increasing transparency for voters', 2018, p. 9, https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Digital-campaigning-improving-transparency-for-voters.pdf.

⁶⁴⁷ The Electoral Commission, 'Digital campaigning: Increasing transparency for voters', 2018, p. 15.

Tot slot heeft de ICO richtlijnen opgesteld voor politieke campagnes, hoe de regels van de AVG- en de ePrivacy-richtlijn van toepassing zijn op politieke campagnes, of het nu gaat om online politieke advertenties, direct marketing of virale campagnes.⁶⁴⁸

C. Frankrijk⁶⁴⁹

i. Algemene kenmerken

Net als in het Verenigd Koninkrijk zijn desinformatie en online politieke advertenties in Frankrijk omstreden kwesties geweest, met name na de “#MacronLeaks” aan de vooravond van de Franse presidentsverkiezingen in 2017.⁶⁵⁰ Er zijn tal van overheidsrapporten verschenen over desinformatie en over de regulering van online platforms.⁶⁵¹ De Franse regering heeft Engelstalige rapporten gepubliceerd, waaronder *Information Manipulation: A Challenge to Our Democracies*. Dit rapport doet een aantal aanbevelingen, waaronder dat staten de volgende maatregelen moeten kunnen uitvoeren wanneer dat nodig is: (a) “adopt a law against “fake news” if there is none,” (b) “penalize more strictly the wrongdoings of the media,” and (c) “consider making registration compulsory for foreign media.”⁶⁵² In 2019 publiceerde de Franse regering ook een 34 pagina's tellend rapport getiteld “*Creating a French framework to make social media platforms more accountable: Acting in France with a European vision*.”⁶⁵³ Het rapport beveelt een publieke interventie aan om de grootste sociale media bedrijven te verplichten om een meer verantwoorde en beschermende houding aan te nemen ten aanzien van de sociale cohesie in Frankrijk.. De regelgeving zou zich richten op de verantwoording van sociale netwerken, uitgevoerd door een onafhankelijke toezichthouder en gebaseerd op drie verplichtingen voor de platforms: (a) een transparantie-verplichting met betrekking tot de functie van het ordenen van inhoud (b) een transparantieplichting met betrekking tot de functie van de implementatie van gebruiksvoorwaarden en de moderatie van inhoud (c) een zorgplicht in relatie tot de gebruikers. Het opleggen van een zorgplicht zou betekenen dat sociale medianetwerken “commit[ting] to be accountable for their users regarding abuses by other members and attempts to manipulate the platform by third parties”.⁶⁵⁴

ii. Regulering van desinformatie

Frankrijk is het enige land dat tot nu toe specifieke wetgeving heeft ingevoerd die gericht is op desinformatie. Er moet echter ook worden opgemerkt dat de Franse wet de publicatie van “nep nieuws” (“*nouvelles fausses*”) al vele jaren strafbaar stelt op grond van artikel 27 van de Freedom of the Press Law uit 1881.⁶⁵⁵ In 2018 werd de Law no. 2018-2012 on Manipulation of Information uitgevaardigd, die bepaalt dat een rechtbank in de drie maanden voorafgaand aan een verkiezing een online platform kan gelasten om “*des allégations ou imputations inexactes ou trompeuses d'un fait*” (“onjuiste of misleidende feitelijke beschuldigingen of aantijgingen”) te verwijderen die de oprechtheid van een aankomende verkiezing kunnen aantasten en welke opzettelijk op grote schaal, automatisch of kunstmatige wijze zijn

648 Information Commissioner's Office, 'Guidance on political campaigning', https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf.

649 For an overview, see Borrell, A. & Dakhli, J., 'Political Advertising in France: The Story and Effects of a Slow Liberalization' in: Holtz-Bacha, C. & Marion R. Just (eds), 'Routledge Handbook of Political Advertising' Routledge, 2017, pp. 123-138.

650 See Downing, J. and Ahmed, W., '#MacronLeaks as a “warning shot” for European democracies: challenges to election blackouts presented by social media and election meddling during the 2017 French presidential election', 2019, French Politics, p. 1-33, <https://doi.org/10.1057/s4125>.

651 See, eg., *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision*, Interim mission report - “Regulation of social networks – Facebook experiment,” Submitted to the French Secretary of State for Digital Affairs (May 2019), https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf.

652 J.-B. Jeangène Vilmer, A. Escorcía, M. Guillaume, J. Herrera, 'Information Manipulation: A Challenge for Our Democracies', Ministry for Europe and Foreign Affairs and the Ministry for the Armed Forces, 2018, p. 173, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

653 See, eg., Mission Members, 'Creating a French framework to make social media platforms more accountable: Acting in France with a European vision', Interim mission report - Regulation of social networks – Facebook experiment', Submitted to the French Secretary of State for Digital Affairs, 2019, https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf.

654 Idem, p. 21.

655 Loi du 29 juillet 1881 sur la liberté de la presse, Article 27, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722&dateTexte=vig>.

verspreid.⁶⁵⁶ De rechtbank moet binnen 48 uur een uitspraak doen en een eventuele beslissing op beroep moet binnen 48 uur worden genomen.

De eerste beslissing in het kader van deze nieuwe procedure is genomen in mei 2019. Daarin heeft het Parijse gewestelijke gerechtshof een verzoek van een Franse senator van de oppositie tegen Twitter om een tweet van de Franse minister van Binnenlandse Zaken te laten blokkeren afgewezen.⁶⁵⁷ Het Hof verduidelijkte dat het moet gaan om gesponsorde inhoud, dat wil zeggen een betaling van derde partijen voor het kunstmatig verbreden van de verspreiding van informatie, en inhoud waarvan de verspreiding wordt versterkt via geautomatiseerde hulpmiddelen zoals bots.⁶⁵⁸ Het Hof oordeelde verder dat onjuiste of misleidende beschuldigingen of uitspraken niet hetzelfde zijn als gedeeltelijke onjuistheden of simpele overdrijving, maar slechts beschuldigingen en uitspraken waarvan de onjuistheid objectief kan worden vastgesteld. Het onnauwkeurige of misleidende karakter van de beschuldigingen moeten “duidelijk” zijn, evenals het risico dat zij het stemgedrag bij verkiezingen buitensporig beïnvloeden.

Titel III van de Law on Manipulation of Information voert een verplichting tot samenwerking in voor bepaalde online platforms om de verspreiding van desinformatie tegen te gaan. De online platforms zijn de in Artikel L. 111-7 van de Consumer Code gedefinieerde platforms met meer dan vijf miljoen unieke bezoekers per maand, per platform, berekend op basis van het laatste kalenderjaar. Artikel 11 schrijft voor dat deze online platforms maatregelen moeten nemen tegen de verspreiding van desinformatie die de openbare orde kan verstoren of de oprechtheid van bepaalde verkiezingen kan aantasten. De platforms moeten met name een makkelijk toegankelijk en zichtbaar mechanisme hebben dat gebruikers in staat stelt om onjuiste informatie te rapporteren, waarvan te verwachten is dat het de publieke orde kan verstoren of de oprechtheid van de verkiezingen kan aantasten, in het bijzonder als het door derden gesponsorde inhoud betreft. Artikel 11 bepaalt ook dat de online platforms andere maatregelen moeten uitvoeren die kunnen omvatten: (a) transparantie van algoritmes; (b) het promoten van inhoud van de pers en persbureaus en van audiovisuele mediadiensten; (c) het bestrijden van accounts die op grote schaal onjuiste informatie verspreiden; (d) de identiteit van de personen die betalen voor het promoten van bepaalde inhoud; (e) informatie over de aard, bron en wijze van verspreiding van inhoud; en (f) het bevorderen van geletterdheid op het gebied van media en informatie. De platforms moeten jaarlijks aan de Franse toezichthouder voor de media (*Conseil Supérieur de l'Audiovisuel*) (CSA) een verklaring overleggen over de wijze waarop elk van de krachtens artikel 11 genomen maatregelen ten uitvoer wordt gelegd.

Krachtens artikel 12 kan de CSA aanbevelingen doen aan onlineplatforms om de strijd tegen de verspreiding van desinformatie die de openbare orde kan verstoren of de oprechtheid van de verkiezingen kan aantasten, te verbeteren. In mei 2019 publiceerde de CSA haar eerste aanbeveling aan de online platforms over de plicht tot samenwerking in de strijd tegen de verspreiding van desinformatie.⁶⁵⁹ Er zijn gedetailleerde aanbevelingen over de wijze waarop de platforms de maatregelen van artikel 11 ten uitvoer leggen.

Met name in het kader van de bestrijding van de grootschalige verspreiding van valse informatie via accounts worden de platforms aangemoedigd om “geschikte procedures in te richten voor het detec-

656 Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, article 1, <https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte>. See Blocman, A. 'Law on manipulation of information, validated by the Constitutional Council, is published', IRIS 2019-2, <http://merlin.obs.coe.int/iris/2019/2/article11.en.html>.

657 Tribunal de grande instance de Paris, (ord. réf.), 17 mai 2019, Mme V. et M. O. (see Blocman, A., 'First urgent application to block dissemination of a tweet under the Act on combating the manipulation of information', 2019, IRIS 2019-7, 14, <http://merlin.obs.coe.int/iris/2019/7/article14.en.html>).

658 Idem.

659 Conseil supérieur de l'audiovisuel, 'Recommendation no. 2019-03 of 15 May 2019 of the Conseil supérieur de l'audiovisuel to online platform operators in the context of the duty to cooperate to fight the dissemination of false information', http://www.csa.fr/content/download/254203/733091/version/1/file/CSA%20-%20Projet%20de%20recommandation%20aux%20op%C3%A9rateurs%202504_eng-GB.pdf.

teren van accounts die op grote schaal onjuiste informatie verspreiden”, en om “geschikte procedures in te richten met als doel het belemmeren van de activiteiten van deze accounts (waarschuwingen, verwijdering, quarantaine, beperkingen op gebruiksrechten of de reikwijdte van de verspreide inhoud, etc.) rekening houdend met de vrijheid van meningsuiting en de communicatievrijheid”.⁶⁶⁰ In de aanbeveling staat ook dat de platforms de gebruikers duidelijke en gedetailleerde informatie moeten verschaffen over praktijken die ertoe kunnen leiden dat de platform exploitant actie onderneemt (zoals abnormale accounts, het delen van inhoud tegen abnormale tarieven, het gebruik van valse, gestolen of misleidende informatie, enz).⁶⁶¹

Voorts beveelt de CSA met betrekking tot de promotie van inhoud van persbureaus aan dat platforms technologische middelen inzetten om informatie van deze bronnen onder de aandacht te brengen, in het bijzonder fact-checking van inhoud in zoekresultaten, newsfeeds en andere verspreidingskanalen met behulp van geautomatiseerde classificatie technieken.⁶⁶²

iii. Politieke advertenties

In tegenstelling tot alle andere onderzochte landen heeft Frankrijk wel wetgeving die politieke verkiezingsadvertenties in kranten, op de televisie en online beperkt. Buiten verkiezingstijd zijn er minder beperkingen.

1. *Kranten en uitzendingen*

Politieke advertenties zijn tijdens de verkiezingsperiode verboden in kranten, maar zijn wel toegestaan buiten de verkiezingsperiodes om. Artikel L. 52-1 van de Franse Kieswet (“Code électoral”) verbiedt, gedurende de zes maanden voorafgaand aan een verkiezing, “het gebruik, voor het doel van verkiezingspropaganda, van enige vorm van commercieel advertenteren in de pers of enige andere vorm van audiovisuele communicatie”.⁶⁶³ Verder mogen tijdens verkiezingsperiodes advertenties in de pers geen “verwijzingen, verbaal of visueel, naar kandidaten of verkiezingsgerelateerde onderwerpen” bevatten.⁶⁶⁴ Artikel L. 52-8 van de Electoral Code staat de kandidaten echter toe te “adverteren in de pers voor geautoriseerde donaties” om hun campagnes te financieren.

Evenzo verbiedt artikel L. 52-1 uitzendingen, het gebruik van commerciële advertenties in de pers of audiovisuele communicatiemiddelen voor verkiezingspropaganda in de zes maanden voorafgaand aan een verkiezing. De wet bepaalt ook de totale duur van de campagnes voor de verschillende verkiezingen en hoe de zendtijd tussen de verschillende kandidaten, partijen of groepen moet worden verdeeld. De Franse media toezichthouder stelt de regels vast betreffende de voorwaarden voor de productie, de programmering en de uitzending van programma’s tijdens de officiële campagne voor elke verkiezing.⁶⁶⁵

2. *Internet diensten*

Online politieke advertenties zijn tijdens de verkiezingen ook verboden en in 2018 zijn nieuwe transparantieregels vastgesteld. Ten eerste heeft het bovenstaande verbod uit artikel L. 52-1 ook betrekking op online openbare communicatie.⁶⁶⁶ Tijdens de Franse presidentiële zitting van 2017 merkte het rapport van het team van verkiezingsdeskundigen van de OSCE bijvoorbeeld op dat de onlinemedi

⁶⁶⁰ Idem, p. 4.

⁶⁶¹ Idem.

⁶⁶² Idem.

⁶⁶³ Code électoral, Version consolidée au 3 août 2019, Article 52-1, <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070239>.

⁶⁶⁴ Agnès Granchet, “FR - France”, in: Cappello, M., ‘Media coverage of elections: the legal framework in Europe’, European Audio-visual Observatory, 2017.

⁶⁶⁵ Article 14, para. 2 and 3, of Law no. 86-1067 of 30 September 1986 on the freedom of communication, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068930>.

⁶⁶⁶ Council of State, 3rd and 8th sub-sections combined, 13 February 2009, no. 317637, https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT0000202530_73&fastReqId=1760283217&fastPos=1.

onderworpen waren aan “een verbod op de inkoop en publicatie van betaalde politieke advertenties, hetgeen zich uitstrekt tot alle type media”.⁶⁶⁷

Verder zijn volgens artikel L. 48-1 van de Franse Kieswet de verbodsbepalingen inzake de verspreiding van verkiezingspropaganda uitdrukkelijk van toepassing op “elk bericht dat het karakter heeft van verkiezingspropaganda en verspreid wordt naar het publiek via enige methode van elektronische communicatie”. Het begrip verkiezingspropaganda (“propagande électorale”) wordt niet in de wetgeving gedefinieerd, maar zoals de OSCE heeft opgemerkt, kan verkiezingspropaganda worden vergeleken met betaalde politieke advertenties. Voorts verbiedt artikel 49 van de Kieswet *elke* vorm van verkiezingspropaganda op de dag van de verkiezingen en de dag ervoor.

Onlangs nog werd de Elecoral Code nr. 2018-1202 gewijzigd om in de drie maanden voorafgaand aan een verkiezing te bepalen dat bepaalde online platforms de gebruikers “eerlijke, duidelijke, en transparante informatie” moeten verstrekken over: (a) de identiteit van de persoon of de organisatie die het platform betaalt voor de promotie van inhoud gerelateerd aan een debat van algemeen belang”, en (b) het gebruik van persoonsgegevens voor de promotie van inhoud gerelateerd aan een debat van algemeen belang; en ook een openbaar register in te richten.⁶⁶⁸ Zo zijn tijdens de verkiezingstijd bepaalde betaalde inhoud met betrekking tot debatten van algemeen belang onderworpen aan transparantieregels.

Frankrijk heeft samengevat een van de meest interventionistische regelgevingskaders voor politieke advertenties. Er moet echter worden benadrukt dat deze regels beperkt zijn tot de verkiezingstijd.

D. Duitsland⁶⁶⁹

i. Algemene kenmerken

In de huidige discussies over desinformatie en politieke advertenties wordt Duitsland soms gelijkgesteld aan landen die wetgeving invoeren die gericht is op desinformatie en nepnieuws, vanwege de inwerkingtreding in 2018 van de Duitse wet op het gebied van de internethandhaving, het Netzwerkdurchsetzungsgesetz (NetzDG). Soms wordt gemeld dat de NetzDG van toepassing is op het verwijderen van “nepnieuws”.⁶⁷⁰ Het is daarom belangrijk om op te merken dat de wetgeving weliswaar gericht is op internetdiensten, in het bijzonder de sociale mediaplatforms, maar geen specifieke bepalingen bevat over nepnieuws, desinformatie of politieke advertenties. Zoals Tworek en Leerssen benadrukken, “[The NetzDG] does not actually create new categories of illegal content. Its purpose is to enforce 22 statutes in the online space that already existed in the German criminal code and to hold large social media platforms responsible for their enforcement”.⁶⁷¹ De wet is gericht op grote sociale netwerkplatforms met meer dan 2 miljoen gebruikers in Duitsland, en schrijft voor dat deze platforms een mechanisme moeten bieden waarmee gebruikers klachten over illegale inhoud kunnen indienen. Zodra een platform een klacht heeft ontvangen, moet het platform onderzoeken of de inhoud illegaal is. Als de inhoud “kennelijk onrechtmatig” is, moeten de platforms deze binnen 24 uur verwijderen. Andere illegale inhoud moet binnen 7 dagen worden verwijderd en platforms die niet aan de eisen voldoen, kunnen boetes tot 50 miljoen euro krijgen.⁶⁷²

667 OSCE, ‘Republic of France Presidential Election 23 April and 7 May 2017, OSCE/ODIHR Election Expert Team Final Report’, 2017, p. 8, <https://www.osce.org/odihr/elections/france/337346?download=true>.

668 Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l’information, article 1, <https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/loi/texte>.

669 See Etteldorf, C., ‘DE-Germany’ in: Cappello, M. (ed.), ‘Media coverage of elections: the legal framework in Europe’, 2017, European Audiovisual Observatory, p. 29-37, https://www.ivir.nl/publicaties/download/IRIS_Special_2017_1.pdf.

670 See, eg, “Germany starts enforcing hate speech law”, BBC News, 1 January 2018 (“Germany is set to start enforcing a law that demands social media sites move quickly to remove hate speech, fake news and illegal material”).

671 Idem, p. 2.

672 Tworek, H. & Leerssen, P., ‘An Analysis of Germany’s NetzDG Law’, 2019, Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

De Duitse regering heeft echter, in haar inzending voor de UN Special Rapporteur on freedom of expression verklaard dat de belangrijkste reden voor de NetzDG “[n]ot only hate speech, defamation and malicious gossip” is, maar ook “the spread of “fake news” on social media platforms”.⁶⁷³ De toepasselijkheid van de wet op de bestrijding van desinformatie wordt daarom hieronder besproken.

ii. Regulering van desinformatie

De NetzDG is van toepassing op op winst gerichte internet platforms die “gebruikers in staat stellen om enige inhoud te delen met andere gebruikers of deze inhoud voor het publiek toegankelijk te maken (sociale netwerken)” en die in Duitsland ten minste twee miljoen geregistreerde gebruikers hebben. De NetzDG is niet van toepassing op platforms die zijn ontworpen “voor individuele communicatie of the verspreiding van specifieke inhoud”. De NetzDG werkt als volgt: ten eerste legt artikel 3, lid 1, een verplichting op aan platforms om “effectieve en transparante procedures voor het behandelen van klachten over onrechtmatige inhoud” in te richten, en moet het platform “gebruikers een makkelijk herkenbare, direct toegankelijke en permanent bereikbare procedure voor het indienen van klachten over onrechtmatige inhoud aanbieden”.⁶⁷⁴ Onrechtmatige inhoud wordt gedefinieerd als inhoud in de zin van een 22-tal strafbare feiten in het Duitse Wetboek van Strafrecht. Het is nuttig om deze misdrijven te beschrijven, omdat ze van toepassing zijn op een enorme hoeveelheid uitingen:

belediging; laster; smaad; laster van godsdiensten, religieuze en ideologische verenigingen; verspreiding van afbeeldingen van geweld; verspreiding van propagandamateriaal van ongrondwettige organisaties; gebruik van symbolen van ongrondwettige organisaties; verraderlijke vervalsing; opruiing; aanzetten tot haat; voorbereiding van een ernstig gewelddadig delict dat de staat in gevaar brengt; aanmoediging van het plegen van een ernstig gewelddadig delict dat de staat in gevaar brengt; schending van de openbare orde door te dreigen met het plegen van delicten; belonen en goedkeuren van delicten; verspreiding, verwerving en bezit van kinderpornografie; dreigen met het plegen van een misdrijf; vervalsing van gegevens die bedoeld zijn om bewijs te leveren.

In paragraaf 3, lid 2, wordt vervolgens uiteengezet hoe de procedure dient te werken: eerst moeten de platforms onmiddellijk kennis nemen van een klacht en toetsten of de gerapporteerde inhoud onrechtmatig is, en verwijderd of de toegang er toe geblokkeerd dient te worden. Ten tweede, en dit is van cruciaal belang, moeten de platforms “inhoud die kennelijk onrechtmatig is binnen 24 uur na ontvangst van de klacht blokkeren. De wet bevat geen definitie van wat kennelijk onrechtmatig is.

Ten derde moeten de platforms toegang tot alle onrechtmatige inhoud onmiddellijk, en in de regel binnen 7 dagen na ontvangst van de klacht blokkeren of het materiaal verwijderen. De termijn van 7 dagen kan worden overschreden wanneer a) het besluit over de onrechtmatigheid van de inhoud afhankelijk is van de onjuistheid van feitelijke aantijgingen of duidelijk afhankelijk is van andere feitelijke omstandigheden (het sociale netwerk kan de gebruiker de gelegenheid geven een antwoord te geven op de klacht voor een besluit genomen wordt); of (b) het sociale netwerk het besluit over de onrechtmatigheid doorstuurt naar een erkend zelfreguleringsorgaan voor NetzDG binnen 7 dagen na ontvangst van de klacht, en er mee instemt het besluit van dit orgaan te aanvaarden. Artikel 3 lid 6 geeft voor de erkenning van een zelfreguleringsorgaan in dit kader de wettelijke vereisten, waaronder de onafhankelijkheid en het kunnen uitvoeren van een snelle analyse van onrechtmatige inhoud binnen 7 dagen.

Ten vierde legt de NetzDG aan platforms rapportageverplichtingen op. De platforms moeten rapporten publiceren over hun behandeling van klachten over illegale inhoud. De wetgeving bepaalt de vereiste inhoud van deze rapportages, met inbegrip van (a) een beschrijving van de mechanismes voor

⁶⁷³ <https://www.ohchr.org/Documents/Issues/Opinion/Legislation/GermanyReply9Aug2017.pdf>.

⁶⁷⁴ Act to Improve Enforcement of the Law in Social Networks (NetzDG) 2017, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2.

het indienen van klachten over onrechtmatige inhoud en de toegepaste criteria voor het besluiten over het verwijderen of blokkeren van onrechtmatige inhoud, (b) het aantal binnengekomen klachten over onrechtmatige inhoud, en (c) de tijd tussen de ontvangst van klachten die door het sociale netwerk zijn ontvangen en het verwijderen of blokkeren van de onrechtmatige inhoud.

Ten slotte maakt de wet het overtreden van de wet strafbaar en kunnen er boetes tot 5 miljoen euro worden opgelegd. Zoals hierboven vermeld, introduceert de NetzDG geen nieuwe strafbare feiten. Er dient echter op gewezen te worden dat de strafbare feiten die onder de NetzDG vallen, zeer ruim geformuleerd zijn en van toepassing zijn op desinformatie. De UN Special Rapporteur on freedom of expression heeft zorgen geuit ten aanzien van de onduidelijke en dubbelzinnige normen, zoals belediging en laster.⁶⁷⁵ Het Duitse Wetboek van Strafrecht stelt belediging strafbaar op grond van artikel 185 en geeft geen definitie, maar stelt alleen dat “belediging zal worden gestraft met een gevangenisstraf van niet meer dan een jaar of een boete”.⁶⁷⁶ Zelfs als een uitspraak waar is, kan het een belediging zijn, aangezien artikel 192 bepaalt dat “bewijs van de juistheid van de gestelde of verspreide feitelijkeheden doet niet af aan de strafmogelijkheid onder artikel 185 als de belediging het gevolg is van de wijze van het gestelde of de verspreiding of de omstandigheden waaronder deze gedaan zijn”. Het Duitse recht inzake belediging wordt vooral in de jurisprudentie uitgewerkt, maar het Wetboek van Strafrecht zelf biedt weinig houvast voor wat een belediging is.

Voorts is smaad op grond van artikel 186 strafbaar gesteld. Smaad wordt als volgt gedefinieerd: “het stellen of verspreiden van een feit jegens een andere persoon, die hem aantasten in de eer en goede naam of de publieke opinie over hem negatief beïnvloeden, tenzij de waarheid van dit feit bewezen kan worden”.⁶⁷⁷ Laster wordt op grond van artikel 187 strafbaar gesteld en wordt gedefinieerd als het bewust en opzettelijk verspreiden van onjuistheden jegens een andere persoon, welke deze aantasten in de eer en goede naam of de publieke opinie over hem negatief beïnvloeden.

Diverse platforms hebben ondertussen transparantieverslagen gepubliceerd over de werking van de wet, waaronder Facebook, YouTube en Twitter. In het laatste rapport van januari - juni 2019 meldt Facebook dat de meeste inhoud is geblokkeerd op grond van belediging (140), gevolgd door aanzetten tot haat (70) en laster (39).⁶⁷⁸ In het laatste rapport van YouTube over dezelfde periode wordt gemeld dat het grootste deel van de verwijderde of geblokkeerde inhoud betrekking heeft op het aanzetten tot haat en laster tegen religieuze, religieuze en ideologische verenigingen (23.567), gevolgd door laster en belediging (14.985). Verder werd 87% van de inhoud binnen 24 uur na de klacht verwijderd of geblokkeerd.⁶⁷⁹ In juli 2019 heeft het Federaal Justitieel Bureau een boete van 2 miljoen euro op Facebook opgelegd voor de onvolledige informatie in het rapport over het aantal klachten over illegale inhoud.⁶⁸⁰ Het Bureau stelt dat het NetzDG-rapportageformulier onvoldoende transparant is gemaakt.

iii. Politieke advertenties

1. Kranten en omroepen

In Duitsland bestaan er geen specifieke wettelijke bepalingen voor verkiezingsadvertenties of verkiezingsberichten in de gedrukte media. Politieke partijen mogen in principe advertenties uitzenden of

675 Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Communication No. OL DEU 1/2017, 1 June 2017, <http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf>.

676 German Criminal Code, Article 186, https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.German%20territory.&targetText=German%20criminal%20law%20shall%20apply%2C%20regardless%20of%20the%20law%20applicable,the%20Federal%20Republic%20of%20Germany.

677 German Criminal Code, Article 186, https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.German%20territory.&targetText=German%20criminal%20law%20shall%20apply%2C%20regardless%20of%20the%20law%20applicable,the%20Federal%20Republic%20of%20Germany.

678 https://fbnewsroomus.files.wordpress.com/2019/07/facebook_netzdg_july_2019_english.pdf

679 <https://transparencyreport.google.com/netzdg/youtube?hl=en>.

680 Federal Office of Justice Issues Fine against Facebook, 3 July 2019, <https://perma.cc/9G3V-SJRN>. See <http://www.loc.gov/law/foreign-news/article/germany-facebook-found-in-violation-of-anti-fake-news-law/?locl= eaglm>.

publiceren, aangezien de verantwoordelijke regionale wetgevers dit niet hebben verboden in de regionale perswetten.⁶⁸¹ Als verkiezingsadvertenties of -reportages in de geschreven pers verschijnen, is de uitgever - in tegenstelling tot de omroepen - niet verplicht om de gelijke kansen van de partijen of de partijpolitieke neutraliteit te respecteren.⁶⁸²

Artikel 7, lid 9, eerste alinea, van de *Rundfunkstaatsvertrag* (RstV) verbiedt daarentegen advertenties van politieke, ideologische of religieuze aard.⁶⁸³ Er gelden echter vrijstellingen tijdens verkiezingscampagnes. Zo zijn bijvoorbeeld alle publieke omroepen, met uitzondering van Radio Bremen, Radio Berlin-Brandenburg en Saarländischer Rundfunk, verplicht om gratis zendtijd voor verkiezingsadvertenties toe te wijzen. Wat de nationale omroepen betreft, is deze verplichting voor Zweites Deutsches Fernsehen (ZDF) vastgelegd in artikel 11, lid 1, van de ZDF, op grond waarvan de partijen recht hebben op een redelijke hoeveelheid zendtijd in de aanloop naar de verkiezingen voor de Bundestag en het Europees Parlement, indien zij op ten minste één staatslijst of nominatie voorkomen.⁶⁸⁴

2. Internet diensten

De regulering van verkiezingsadvertenties en verkiezingsrapportages in de online omgeving is niet alleen afhankelijk van de internetdienst zelf, maar ook van de aanbieder ervan. Het Duitse recht maakt een onderscheid tussen omroepen (ofwel: broadcasting) en telemedia. De uitzending van een lineair programma volgens een vastgesteld schema (met name rechtstreekse streamingdiensten) via het internet wordt als omroepuitzending aangemerkt en moet voldoen aan het verbod op politieke advertenties.⁶⁸⁵ Telemedia-inhoud daarentegen valt onder de artikelen 54 e.v. van de RStV. Verkiezingsadvertenties via audiovisuele mediadiensten op aanvraag zijn verboden op grond van artikel 58, lid 3, onder 1, juncto artikel 7, lid 9, van de RStV en moeten in andere telemedia worden gescheiden van andere inhoud, overeenkomstig artikel 58, lid 1, van de RStV. De UWG (Wet op de Oneerlijke Mededinging), die verreweg het belangrijkste instrument is voor de regulering van internetadvertenties in Duitsland, is echter niet van toepassing op politieke advertenties. Voor journalistieke telemedia - met name de online diensten van kranten en omroepen op aanvraag - bepaalt artikel 54, lid 2, van de RStV ook dat erkende journalistieke beginselen van toepassing moeten zijn. Dit geldt echter niet voor telemedia die niet binnen de journalistieke criteria vallen, waaronder doorgaans ook sociale mediaplatforms zoals Facebook en YouTube en het online aanbod van de politieke partijen zelf.⁶⁸⁶

Verder bevat de NetzDG, zoals hierboven vermeld, geen specifieke bepalingen met betrekking tot politieke advertenties, hoewel de wet wel van toepassing is op online platforms.⁶⁸⁷ Kruschinski en Haller hebben een overzicht van hoe het Duitse recht inzake gegevensbescherming van toepassing is op online politieke microtargeting gepubliceerd.⁶⁸⁸

681 Etteldorf, C. "DE-Germany" in Cappello, M. (ed.), 'Media coverage of elections: the legal framework in Europe', European Audio-visual Observatory, 2017, p. 33.

682 Idem.

683 Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag – RStV / Interstate Treaty on Broadcasting and Telemedia (Interstate Broadcasting Treaty) in the version of the 19th Amendment to the Interstate Broadcasting Treaties, entry into force: 01 October 2016, http://www.diemedienanstalten.de/fileadmin/Download/Rechtsgrundlagen/Gesetze_aktuell/19_RfAendStV_medienanstalten_Layout_final.pdf (An English version is available at: https://www.wen.uni.lu/content/download/31281/371474/file/Germany_translation_1.pdf).

684 Idem.

685 Idem., p. 32.

686 Idem.

687 Zie: Tworek, H. & Leerssen, P., 'An Analysis of Germany's NetzDG Law,' Working Paper Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2019, https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

688 Kruschinski, S. & Haller, A., 'Restrictions on data-driven political microtargeting in Germany', 2017, Internet Policy Review, 6(4). DOI: 10.14763/2017.4.780.

In tegenstelling tot landen als het Verenigd Koninkrijk moet worden opgemerkt dat in het rapport van het OSCE-verkiezingsdeskundigenteam van 2017 over de verkiezingen voor het Duitse federale parlement wordt benadrukt dat “[t]here are no limits set to campaign expenditures for parties and candidates,” en dat “[the] bulk of campaign expenses were allotted to media advertising, including on social media. The legislation lacks provisions regulating campaign activities by third-parties”.⁶⁸⁹

E. Zweden

i. Algemene kenmerken

Er is veel onderzoek gedaan en gediscussieerd over desinformatie in Zweden, met name in verband met desinformatie tijdens verkiezingsperioden.⁶⁹⁰ De Zweedse regering behandelt desinformatie als een nationale veiligheidskwestie en de bestrijding van desinformatie tijdens verkiezingen maakt deel uit van de nationale veiligheidsstrategie van de Zweedse regering.⁶⁹¹ Zweden heeft echter gekozen voor een duidelijk niet-regelgevende aanpak, die door de European Parliament's Committee on Civil Liberties, Justice and Home Affairs is omschreven als een “proactieve benadering” van desinformatie in haar studie getiteld *Disinformation and propaganda: impact on the functioning of the rule of law in the EU and its Member States*.⁶⁹² Ook het verslag van de Franse regering getiteld *Information Manipulation: A Challenge to Our Democracies*, wijst op het Zweedse beleid als methode om desinformatie tegen te gaan.⁶⁹³ Er is ook empirisch onderzoek gedaan naar het beleid van Zweden, zoals de studie van het Oxford Internet Institute over *junk news* op Twitter tijdens de Zweedse verkiezingen,⁶⁹⁴ en een studie van de London School of Economics over de Zweedse over bots en amplificatie tijdens de verkiezingen van 2018.⁶⁹⁵

Verder is Zweden, met betrekking tot online politieke advertenties, een opmerkelijke casestudy voor zijn benadering van politieke advertenties in het algemeen, waar er weinig regelgeving is en waar er de laatste tijd inderdaad sprake is geweest van deregulering van politieke advertenties op televisie.

ii. Regulering van desinformatie

Zweden heeft geen wetgeving aangenomen die gericht is op desinformatie, maar een aantal opmerkelijke niet-wetgevende maatregelen zijn ten uitvoer gelegd. Ten eerste zijn er informatiecampagnes. In 2019 publiceerde het Civil Contingencies Agency bijvoorbeeld een handboek van 50 pagina's getiteld *Countering information influence activities*, met onder meer methoden voor het tegengaan van desinformatie en andere methoden van “information influence techniques” zoals “[m]alicious rhetoric”.⁶⁹⁶ Het Europees Parlement heeft de nadruk gelegd op de aankondiging van de Zweedse regering om een autoriteit in het leven te roepen om desinformatie en buitenlandse beïnvloeding tegen te gaan. Het hoofddoel

689 OSCE/ODIHR, ‘Election Expert Team, Elections to the Federal Parliament (Bundestag)’, 2017, OSCE, p. 6, <https://www.osce.org/odihr/elections/germany/358936?download=true>.

690 See, eg, Hedman, F. et al., ‘News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter, COMPROP Data Memo 2018.3’, 2018, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/09/Hedman-et-al-2018.pdf>; and Leonid Bershidsky, Fake News Takes Its Toll on Sweden's Elections, Bloomberg, 15 November 2018, <https://www.bloomberg.com/opinion/articles/2018-11-15/fake-news-roiled-sweden-s-elections-but-it-was-homegrown>.

691 Government Offices of Sweden, National Security Strategy, <https://www.government.se/4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf>. See also Swedish Security Service, ‘Attempts to influence confidence in the election process’, 31 August 2018, <https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-08-31-attempts-to-influence-confidence-in-the-election-process.html>.

692 Bayer, J., Bitiukova, N., Bárd, P., Szakács, J., Alemanno, A., Uszkiewicz, E., *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States* (European Union, 2019), [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

693 Jeangène Vilmer, J.B., Escorcía, A., Guillaume, M., Herrera, J., ‘Information Manipulation: A Challenge for Our Democracies’ (Ministry for Europe and Foreign Affairs and the Ministry for the Armed Forces 2018), p. 173, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

694 Hedman, F. et al., ‘News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter, COMPROP Data Memo 2018.3’, 2018, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/09/Hedman-et-al-2018.pdf>.

695 Smearing Sweden, ‘International Influence Campaigns in the 2018 Swedish Election’, p. 6, <http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf>.

696 Swedish Civil Contingencies Agency, ‘Countering information influence activities – A handbook for communicators’, 2019, MSB, <https://rib.msb.se/filer/pdf/28698.pdf>.

van de autoriteit is het versterken van de veerkracht tegen desinformatie en het bieden van “mentale verdediging” (psykologisch försvar) voor de bevolking.⁶⁹⁷ Het Zweedse bureau voor civiele rampenbestrijding heeft samengewerkt met de Zweedse verkiezingsautoriteit, de veiligheidspolitie en de nationale politie om buitenlandse inmenging bij de verkiezingen van 2018 aan te pakken.⁶⁹⁸

Ten tweede is er meer aandacht voor en aanvullende financiering van programma's voor mediageletterdheid. Zo is de Zweedse regering in 2018 een nationaal initiatief gestart om de mediageletterdheid te vergroten.⁶⁹⁹ Verder heeft de Zweedse regering in september 2019 de Zweedse Raad voor de Media opgedragen om de mediageletterdheid te vergroten door middel van een programma om desinformatie en propaganda tegen te gaan.⁷⁰⁰ Zoals uit de studie van het Europees Parlement is gebleken, heeft Zweden meer geld uitgetrokken voor programma's in het kader van nieuwe media-educatie, waarbij in het schoolonderwijs in Zweden middelen worden uitgetrokken voor de opleiding van toekomstige kiezers en burgers door middel van de ontwikkeling van hun kritische denkwijze en kritische perceptie van propaganda en desinformatie.⁷⁰¹

Ten derde zijn er gezamenlijke mediaprogramma's om desinformatie tegen te gaan. De Zweedse televisie en twee van de grootste Zweedse kranten, Dagens Nyheter en Svenska Dagbladet en de Zweedse radio, werken samen om desinformatie te bestrijden en het bewustzijn over de evaluatie van informatie en de bronnen waaruit deze afkomstig is te vergroten.⁷⁰² De Zweedse regering heeft ook, via de Swedish Innovation Authority, Vinnova, 13,5 miljoen kronen (1,3 miljoen euro) in een nieuw digitaal platform gestoken om de verspreiding van online nepnieuws te voorkomen. Gefinancierd in samenwerking met de Zweedse televisie en andere Zweedse omroepen, bevat het platform drie functies om burgers te helpen bij het filteren van nieuws: Een “automated news assessment service” voor het evalueren van nieuws, een “personalized engine” voor het tegengaan van filterbubbles, en een “fact assistant” voor het automatiseren van feitencontroleprocessen en het wegfilteren van vals en irrelevant nieuws.⁷⁰³

Tot slot zijn er nog de nationale veiligheidsprogramma's. De Zweedse veiligheidsdienst heeft een verslag uitgebracht over zijn activiteiten in de aanloop naar de verkiezingen van 2018 en probeert het vertrouwen in het verkiezingsproces te vergroten. Dit omvatte fake accounts op sociale media, en desinformatie die via sociale media werd verspreid met als doel de samenleving voor de verkiezingen te polariseren. De veiligheidsdienst heeft uitgebreide middelen uitgetrokken voor informatie, onderwijs en samenwerking om het bewustzijn te vergroten dat er invloed kan worden uitgeoefend op operaties die het vertrouwen van het publiek in het verkiezingsproces en het democratisch systeem kunnen schaden.⁷⁰⁴ Ten vierde heeft de Swedish Defence Research Agency onderzoek gedaan naar de rol van geautomatiseerde accounts op Twitter tijdens de verkiezingscampagnes, waarbij een aanzienlijke aanwezigheid van bots in het Zweedse politieke debat werd vastgesteld.⁷⁰⁵

697 Bayer, J. et al., *'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States'*, European Union, 2019, p. 109.

698 Government Offices of Sweden, *'A practical approach on how to cope with disinformation'*, 6 October 2017, <https://www.government.se/articles/2017/10/a-practical-approach-on-how-to-cope-with-disinformation/>

699 <https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2018/08/dir.-201888/>.

700 Uppdrag till Statens medieråd att förstärka arbetet för ökad medie- och informationskunnighet, Diarienummer: Ku2019/01659/MD, 27 September 2019, <https://www.regeringen.se/regeringsuppdrag/2019/09/uppdag-till-statens-medierad-att-forstarka-arbetet-for-okad-medie-och-informationskunnighet/>.

701 Iden., p. 111.

702 Radio Sweden, *'Media outlets to join forces to combat disinformation and fake news'*, 29 January 2018, <https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6870996>.

703 La Cour, C., *'Governments Countering Disinformation: The Case of Sweden'*, 31 July 2019, <https://disinfoportal.org/governments-countering-disinformation-the-case-of-sweden/>.

704 Swedish Security Service, *'Attempts to influence confidence in the election process'*, 31 August 2018, <https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-08-31-attempts-to-influence-confidence-in-the-election-process.html>

705 <https://www.foi.se/rapportsammanfattning?reportNo=FOI%20MEMO%206458>.

iii. Politieke advertenties⁷⁰⁶

1. Kranten en omroepen

Johansson heeft opgemerkt dat er weinig regulering is voor verkiezingscampagnes in Zweden in het algemeen en weinig voor politieke advertenties in het bijzonder.⁷⁰⁷ Er is geen specifieke regelgeving voor politieke advertenties in kranten, maar de pers is wel gebonden aan de Wet op de persvrijheid, die regels bevat voor laster. Verder moeten politieke advertenties in overeenstemming zijn met de Zweedse grondwet inzake de vrijheid van meningsuiting, die bepalingen bevat over het uiten van minachting voor groepen op basis van ras, enzovoort.

Zweden heeft een lange geschiedenis van een verbod op politieke advertenties in de omroepensector. In 2006, na de overgang naar een digitaal omroepsysteem, werden politieke advertenties toegestaan op de commerciële omroep TV4. Sindsdien zijn politieke advertenties op televisie op grond van de Radio- en Televisiewet 2010 niet meer gereguleerd, tenzij de advertenties deel uitmaken van de licentie.⁷⁰⁸ Zo bepaalt de Radio- en Televisiewet 2010 dat bij uitzendingen die onder de voorwaarden voor onpartijdigheid vallen, er geen sprake mag zijn van berichten die worden uitgezonden met als doel de steun te verkrijgen voor politieke of religieuze standpunten of standpunten over de arbeidsmarkt.⁷⁰⁹

Verder bevat de Zweedse Kieswet geen specifieke bepalingen met betrekking tot politieke advertenties.⁷¹⁰ Johansson heeft de Zweedse ervaring met politieke advertenties op televisie sinds de deregulering in 2006 uitvoerig toegelicht.

2. Internet diensten

Er is ook geen specifieke regelgeving ten aanzien van politieke advertenties die door internetdiensten worden verspreid. In het rapport van het OSCE Election Expert Team over de Zweedse verkiezingen van 2018 werd opgemerkt dat de uitgaven van politieke partijen “related to campaigning in social media are much higher than in previous election[s]”.⁷¹¹ Een academisch rapport van de London School of Economics over de Zweedse verkiezingen van 2018 stelde vast “[n]o bots or amplification tactics that could be tied to the Kremlin were detected”,⁷¹² en er werd geen melding gemaakt van het gebruik van politieke advertenties door kwaadaardige belangen.

F. Verenigde Staten⁷¹³

i. Algemene kenmerken

De huidige wereldwijde discussie over desinformatie kan vooral worden teruggevoerd op de Amerikaanse presidentsverkiezingen van 2016. Zoals beschreven in het rapport van de US Special Counsel over inmenging in de Amerikaanse presidentsverkiezingen van 2016, was er buitenlandse inmenging in de verkiezingen via het gebruik van internetdiensten.⁷¹⁴ Van cruciaal belang is dat in het rapport gedetail-

⁷⁰⁶ Johansson, B., ‘Sweden: Ten Years with Television Advertising’ in: Holtz-Bacha, C. & Marion, R. (eds), ‘Routledge Handbook of Political Advertising’, Routledge, 2017, p. 269-278.

⁷⁰⁷ Johansson, B., ‘Sweden: Ten Years with Television Advertising’ in: Holtz-Bacha, C. & Just, M.R. (eds), ‘Routledge Handbook of Political Advertising’, 2017, Routledge, p. 271.

⁷⁰⁸ Idem., p. 271.

⁷⁰⁹ Radio and Television Act 2010:696, Chapter 5, section 6, <http://www.mpr.se/documents/styrdokument/radio%20and%20television%20act.pdf/>.

⁷¹⁰ The Elections Act (2005:837), <https://www.government.se/49150c/contentassets/4e2fdee5a8e342e88289496d34701aed/the-elections-act-2005837>.

⁷¹¹ ODIHR Election Expert Team, ‘Sweden General Elections 2018’, 9 September 2019 (OSCE, 2018), <https://www.osce.org/odihr/elections/sweden/403760?download=true>.

⁷¹² Smearing Sweden, ‘International Influence Campaigns in the 2018 Swedish Election’, p. 6, <http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf>.

⁷¹³ Federal Election Commission, Federal Election Campaign Law (FTC, 2019), <https://www.fec.gov/resources/cms-content/documents/feca.pdf>. See also, Congressional Research Service, ‘Online Political Advertising: Disclaimers and Policy Issues’, 2019, <https://crsreports.congress.gov/product/pdf/IF/IF10758>.

⁷¹⁴ Mueller, R.S., ‘Report On The Investigation Into Russian Interference In The 2016 Presidential Election’, 2019, Department of Justice, <https://www.justice.gov/storage/report.pdf>.

leerd wordt beschreven hoe een in Rusland gevestigde groep een campagne op sociale media had ontworpen “to provoke and amplify political and social discord in the United States”, en dat de groep onder meer deed aan de “purchase of political advertisements on social media in the names of U.S. persons and entities”.⁷¹⁵ De groep beheerde Facebook-groepen en Instagram-accounts met “honderdduizenden Amerikaanse deelnemers” en beheerde Twitter-accounts met “tienduizenden” volgers.⁷¹⁶ Daarnaast gebruikt de huidige Amerikaanse president Donald Trump de term “fake news” routinematig om de media tijdens de verkiezingscampagne en ook tijdens zijn presidentschap in diskrediet te brengen.

Wat betreft de politieke advertenties die door internetdiensten worden verspreid, moet worden opgemerkt dat er in de Verenigde Staten veel wetten op het niveau van de afzonderlijke deelstaten zijn die transparantieregels opleggen voor online politieke advertenties. Belangrijk is dat, hoewel algemeen bekend is dat de bescherming van de vrijheid van meningsuiting onder het *First Amendment* aantoonbaar een van de sterkste ter wereld is, moet worden benadrukt dat de Amerikaanse Supreme Court heeft geoordeeld dat de transparantieregels volledig in overeenstemming zijn met het Eerste Amendement: transparantievereisten “may burden the ability to speak, but they do not prevent anyone from speaking”,⁷¹⁷ en in plaats daarvan zorgen zij ervoor dat “voters are fully informed about the person or group who is speaking”.⁷¹⁸

ii. Regulering van desinformatie

De VS beschouwt desinformatie als een nationale veiligheidskwestie, hoewel er ook maatregelen op staatsniveau worden genomen met betrekking tot programma's voor mediageletterdheid.⁷¹⁹ Eind 2016 vaardigde de VS de *Countering Foreign Propaganda and Disinformation Act* uit, als onderdeel van de *National Defense Authorization Act* 2016. De wet reguleert desinformatie niet, maar kent 120 miljoen dollar aan financiering toe aan het Amerikaanse ministerie van Buitenlandse Zaken om een agentschap op te richten “[to] develop and synchronize government initiatives to expose and counter foreign information operations directed against U.S. national security interests and advance fact-based narratives that support U.S. allies and interests”.

Er is momenteel een nieuw voorstel gedaan, met name om de doeltreffendheid van de inspanningen van buitenlandse entiteiten om de verkiezingen in de Verenigde Staten te beïnvloeden door het gebruik van sociale mediabots om verkeerde informatie en propaganda te verspreiden, uitdrukkelijk te beperken.⁷²⁰ De Bot Disclosure and Accountability Act is ontworpen om het gebruik van geautomatiseerde softwareprogramma's te reguleren die bedoeld zijn om menselijke activiteiten op sociale media na te bootsen.⁷²¹ De wet zou de Federal Trade Commission (FTC) belasten met het definiëren van de term “automated software program or process intended to impersonate or replicate human activity online” in ruime zin, zodat de definitie niet beperkt blijft tot de huidige stand van technologie. De wet verplicht de FTC er ook voor om ervoor te zorgen dat sociale media-aanbieders beleid en procedures vaststellen en toepassen om gebruikers te verplichten het gebruik van geautomatiseerde softwareprogramma's of -processen die bedoeld zijn om zich voor te doen als of menselijke activiteiten na te bootsen openbaar te maken. Naast gebonden te zijn aan de openbaarmakingsregel zouden sociale mediabedrijven verplicht worden om processen in te richten (a) om redelijke preventieve en correctieve maatregelen te nemen ter mitigatie van pogingen van een gebruiker om een geautomatiseerd software programma te gebruiken of handelingen

⁷¹⁵ Idem, p. 4.

⁷¹⁶ Idem, p. 14-15.

⁷¹⁷ *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010), 366 (internal quotations omitted).

⁷¹⁸ *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010), 368.

⁷¹⁹ See Adrian Shahbaz, U.S. Initiatives to Counter Harmful Speech and Disinformation on Social Media, Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 11 June 2019, https://www.ivir.nl/publicaties/download/US_Initiatives_Harmful_Speech_Disinformation-1.pdf.

⁷²⁰ H.R.5181 - Countering Foreign Propaganda and Disinformation Act of 2016, <https://www.govtrack.us/congress/bills/114/s2943/text>.

⁷²¹ S.3127 - Bot Disclosure and Accountability Act of 2018, <https://www.congress.gov/bill/115th-congress/senate-bill/3127/text>.

met als doel iemand te verpersoonlijken of menselijk gedrag te na te bootsen zonder melding daarvan; en (b) voor het verwijderen van berichten, afbeeldingen of enige andere online activiteit van een gebruiker of profiel, gebruikmakend van een geautomatiseerd software programma of proces dat als doel heeft iemand te verpersoonlijken of menselijk gedrag te na te bootsen, zich niet houdend aan de regel hiervan melding te maken.

Op staatsniveau gelden er een aantal nieuwe wetten die gericht zijn op het gebruik van bots, zoals de SB 1001 wet in Californië, waardoor het onrechtmatig is “to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order ... to influence a vote in an election”.⁷²² Er is echter geen enkele aansprakelijkheid wanneer de persoon “discloses that it is a bot”. De wet legt ook geen verplichting op aan dienstverleners van onlineplatforms, met inbegrip van, maar niet beperkt tot, webhosting partijen en internetproviders.

Verder bestaat er aanzienlijke hoeveelheid wetgeving inzake buitenlandse invloeden. Ten eerste verbiedt het wettelijk kader voor campagnefinanciering dat buitenlanders bijdragen, donaties, uitgaven of andere betalingen doen in verband met verkiezingen voor federale, staats- of lokale kandidaten en verbiedt de wet iedereen om dergelijke bijdragen of donaties te vragen of te ontvangen.⁷²³ Ten tweede mogen buitenlanders ook geen “expenditure, independent expenditure, or disbursement for an electioneering communication” doen.⁷²⁴ Hieronder valt niet het verspreiden van een nieuwsbericht, commentaar of redactioneel materiaal via de faciliteiten van een omroep, krant, tijdschrift of andere periodieke publicatie, tenzij deze faciliteiten eigendom zijn van of gecontroleerd worden door een politieke partij, politieke commissie of kandidaat.⁷²⁵

Tot slot is er in de Verenigde Staten een apart taskforce opgericht om onder andere de verspreiding van desinformatie door buitenlandse invloeden tegen te gaan, het Foreign Influence Task Force.⁷²⁶ In de Verenigde Staten heeft de Department of Justice de Russische vrouw Elena Alekseevna Khusyaynova strafrechtelijk vervolgd voor inmenging met de presidentsverkiezingen in 2016.⁷²⁷ De delictomschrijving is getiteld “*Conspiracy to defraud the United States*”.⁷²⁸ Voluit is er sprake van een *federal crime*, indien: “two or more persons conspire ... to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy”. Hieronder valt ook het beïnvloeden van de verkiezingen. Elena Alekseevna Khusyaynova werkte als financieel medewerker voor onder andere de IRA en GlavSet, Russische trollfarms. De vrouw wordt als lid van de samenzwering verdacht van het opstellen van nep accounts, “to address divisive U.S. political and social issues or advocate for the election or electoral defeat or particular candidates”.⁷²⁹ De zaak loopt nog en de ondernemingen zelf worden ook vervolgd door de FBI.

iii. Politieke advertenties

Op grond van de Amerikaanse federale en staatswetten is het voor bepaalde betaalde politieke advertenties verplicht om een zogenaamde “disclaimer” op te nemen. De disclaimer identificeert de persoon die

722 An act to add Chapter 6 (commencing with Section 17940) to Part 3 of Division 7 of the Business and Professions Code, relating to bots, 28 September 2018 (became operative on 1 July 2019), https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180&bill=1001. See Williams, J.L., ‘*Cavalier Bot Regulation and the First Amendment’s Threat Model*’, Knight First Amendment Institute, 21 August 2019, <https://knightcolumbia.org/content/cavalier-bot-regulation-and-the-first-amendments-threat-model>.

723 52 U.S.C. § 30121(a)(1)(A), (a)(2).

724 52 U.S.C. § 30121(a)(1)(C).

725 52 U.S.C. § 30101(9)(B)(i)-(ii).

726 <https://www.fbi.gov/investigate/counterintelligence/foreign-influence>.

727 United States District Court, Criminal Complaint, Case No. 1:18-MJ-464, <https://www.justice.gov/usao-edva/press-release/file/1102591/download>.

728 Title 18 United States Code, Section 371.

729 United States District Court, Criminal Complaint, Case No. 1:18-MJ-464, r.o. 16. <https://www.justice.gov/usao-edva/press-release/file/1102591/download>.

voor een communicatie heeft betaald. De disclaimer bevat ook informatie over de vraag of de communicatie werd goedgekeurd door een politieke kandidaat.⁷³⁰ Zoals hierboven vermeld heeft het Supreme Court geoordeeld dat disclaimer-eisen volledig in overeenstemming zijn met het First Amendment: disclaimer-eisen “may burden the ability to speak, but they do not prevent anyone from speaking,”⁷³¹ maar in plaats daarvan zorgt een disclaimer ervoor dat “voters are fully informed about the person or group who is speaking”.⁷³²

1. *Kranten en omroepen*

Betaalde politieke advertenties zijn toegestaan in kranten. Op grond van de *Federal Election Campaign Act* en de *Federal Election Commission* (FEC) Regulations moeten bepaalde politieke advertenties in kranten echter wel een disclaimer bevatten die de persoon identificeert die voor de politieke advertentie heeft betaald en of de boodschap is goedgekeurd door een kandidaat.⁷³³ Voorts geldt dat: “[n]o person who sells space in a newspaper or magazine to a candidate or to the agent of a candidate, for use in connection with such candidate’s campaign, may charge any amount for such space which exceeds the amount charged for comparable use of such space for other purposes”.⁷³⁴

Betaalde politieke advertenties zijn toegestaan op televisie. In het kader van de *Federal Election Campaign Act*, de FEC en de Federal Communications Commission (FCC)⁷³⁵ zijn er echter regels voor de bekendmaking van politieke advertenties op televisie, waaronder de volgende audioverklaring: “[the political committee or other person paying for the communication and the name of any connected organization of the payor who] is responsible for the content of this advertising.”⁷³⁶

2. *Internetdiensten*

Online betaalde politieke advertenties zijn toegestaan. Onder de *Federal Election Campaign Act*, en de FEC Regulations is echter vereist dat alle “public communications” die uitdrukkelijk de verkiezing van een geïdentificeerde kandidaat promoten, dienen een disclaimer te bevatten.⁷³⁷ Openbare communicatie omvat ook communicatie over verkiezingen en elke andere vorm van openbare politieke advertenties, met inbegrip van “communications placed for a fee on another person’s website”.⁷³⁸ In het bijzonder schreef de FEC in zijn Advisory Opinion 2017-12 dat een organisatie zonder winstoogmerk ook disclaimers op zijn betaalde Facebook advertenties moet plaatsen die uitdrukkelijk de verkiezing van een geïdentificeerde kandidaten bepleit.⁷³⁹

In juni 2019 publiceerde de FEC een voorstel voor een nieuwe regeling voor online politieke disclaimers bij advertenties. De voorgestelde regeling breidt de definitie van algemene openbare politieke advertenties uit tot “(1) communications produced for a fee and those placed or promoted for a fee on another person’s website or digital device, application, service, or platform, and (2) such communications included in section (1) that are then shared by or to a website or digital device, application, service, or platform”.⁷⁴⁰

730 Zie 11 CFR § 110.11, <https://www.law.cornell.edu/cfr/text/11/110.11>; and Federal Elections Commission, Advertising and disclaimers, <https://www.fec.gov/help-candidates-and-committees/making-disbursements/advertising/>.

731 Citizens United v. Federal Election Commission, 558 U.S. 310 (2010), 366 (interne citaten weggelaten).

732 Citizens United v. Federal Election Commission, 558 U.S. 310 (2010), 368.

733 52 U.S. Code § 30120, <https://www.law.cornell.edu/uscode/text/52/30120>. Zie ook: Federal Election Commission, Advertising and disclaimers, <https://www.fec.gov/help-candidates-and-committees/making-disbursements/advertising/>.

734 52 U.S. Code § 30120, <https://www.law.cornell.edu/uscode/text/52/30120>.

735 47 CFR § 73.1212, <https://www.fcc.gov/media/policy/statutes-and-rules-candidate-appearances-advertising>.

736 52 U.S. Code § 30120, <https://www.law.cornell.edu/uscode/text/52/30120>.

737 11 CFR 110.11, <https://www.fec.gov/regulations/110-11/2019-annual-110#110-11>

738 11 CFR § 100.26 - Public communication (52 U.S.C. 30101(22)), <https://www.law.cornell.edu/cfr/text/11/100.26>.

739 Federal Election Commission, “AO 2017-12: Nonprofit must include disclaimers on its Facebook ads”, 18 December 2017, <https://www.fec.gov/updates/ao-2017-12-nonprofit-must-include-disclaimers-its-facebook-ads/>.

740 https://www.fec.gov/resources/cms-content/documents/mtgdoc_19-26-a.pdf.

Ook werd in mei 2019 een Honest Ads Act gepubliceerd, die bedoeld is om de “disclosure requirements for online political advertisement” te verbeteren.⁷⁴¹

3. Staatsregulering van politieke advertenties

Naast de federale wetgeving van de Verenigde Staten heeft een aantal staten van de Verenigde Staten nieuwe wetgeving ingevoerd die gericht is op politieke advertenties via internetdiensten. Sommige internetdiensten staan politieke advertenties voor verkiezingen in Amerikaanse staten niet langer toe, zoals Google Inc. Google staat niet langer politieke advertenties toe op het platform voor staats- en lokale verkiezingen in Maryland, New Jersey, Nevada en Washington.⁷⁴² Microsoft kondigde ook aan dat het niet langer politieke kandidaat- en verkiezingsadvertenties in de Verenigde Staten accepteert, aangezien “regulators from states across the country have taken new steps to bring additional transparency and accountability to political advertising.”⁷⁴³ In april 2019 kondigde Microsoft aan dat het de beslissing had genomen “[to] disallow advertising for election related content, political parties, candidates, and ballot measures globally”.⁷⁴⁴ Verder betaalden Facebook Inc. en Google Inc. in december 2018 een boete van 455.000 dollar om een rechtszaak te schikken die door de Washington State Attorney Genral was aangespannen wegens het niet naleven van de wetten van de staat Washington op het gebied van transparantie met betrekking tot politieke advertenties.⁷⁴⁵

Drie voorbeelden van staatswetten zijn tenslotte illustratief: in 2018 heeft Californië de *Social Media Disclosure Act* gepubliceerd,⁷⁴⁶ die vereist dat politieke advertenties op online platforms een disclaimer bevatten met daarin informatie over wie voor de advertentie heeft betaald. Bovendien vereist de wet dat platforms een openbaar toegankelijke database van de politieke advertenties bijhouden. In 2018 heeft Maryland een soortgelijke wet ingevoerd, namelijk de *Online Electioneering Transparency and Accountability Act*.⁷⁴⁷ De staat New York heeft de *Democracy Protection Act*⁷⁴⁸ gewijzigd, waardoor voor betaalde online politieke advertenties dezelfde normen gelden voor openbaarmaking en disclaimers als voor traditionele mediakanalen.

Deze nationale wetten in de VS geven bruikbare wettelijke definities van onlineplatforms en mogelijke beleidsopties voor de regulering van politieke advertenties, waaronder transparantieregels.

G. Canada

i. Algemene kenmerken

Net als andere regeringen beschouwt de Canadese regering de aanpak van desinformatie als een “prioriteit”.⁷⁴⁹ De maatregelen omvatten onder meer de toewijzing van financiële middelen aan het *Digital Citizen Initiative*, een strategie die uit meerdere componenten bestaat en gericht is op de ondersteuning van de democratie en de sociale cohesie in Canada door het vergroten van de veerkracht van de burgers

741 S. 1356: Honest Ads Act, <https://www.govtrack.us/congress/bills/116/s1356/text>. See also Barrett, P.M. ‘Disinformation and the 2020 Election: How the Social Media Industry Should Prepare’ NYU, 2019, <https://bhr.stern.nyu.edu/tech-disinfo-and-2020-election>.

742 Zie: Google, ‘Advertising Policy Help – Political content - State election ads in the United States’ <https://support.google.com/adspolicy/answer/6014595?hl=en> (accessed 14 August 2019).

743 Sainsbury-Carter, K., ‘Changes to our Political Ads Policy’, 2018, Microsoft, <https://about.ads.microsoft.com/en-us/blog/post/october-2018/changes-to-our-political-ads-policy>.

744 Idem.

745 Brunner, J., ‘Facebook, Google to pay Washington \$450,000 to settle lawsuits over political-ad transparency’, The Seattle Times, 18 December 2018, <https://www.seattletimes.com/seattle-news/politics/facebook-google-to-pay-washington-450000-to-settle-lawsuits-over-political-ad-transparency/>.

746 An act to amend Sections 84504.3, 84504.4, and 84510 of, and to add Sections 84503.5 and 84504.6 to, the Government Code, relating to the Political Reform Act of 1974, http://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2188.

747 Zie: <http://mgaleg.maryland.gov/webmgal/frmMain.aspx?id=sb0875&stab=01&pid=billpage&tab=subject3&ys=2018rs>.

748 Democracy Protection Act (A9930), https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=A09930&term=2017&Summary=Y&Actions=Y&Memo=Y&Text=Y.

749 Government of Canada, ‘Online disinformation’, <https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html>.

tegen online desinformatie.⁷⁵⁰ Verder werd eind 2018 ook een parlementair rapport gepubliceerd met de titel *Democracy Under Threat: Risk and Solutions in the Era of Disinformation and Data Monopoly*.⁷⁵¹ Met name Canada heeft in 2018 wetgeving uitgevaardigd met betrekking tot online politieke advertenties in het kader van de *Elections Modernization Act*, die hieronder wordt besproken.

ii. Regulering van desinformatie

In bovengenoemde parlementair rapport is een aantal aanbevelingen gedaan met betrekking tot desinformatie. Ten eerste moet de regering “enact legislation imposing a duty on social media platforms to remove manifestly illegal content in a timely fashion, including hate speech, harassment and disinformation, or risk monetary sanctions commensurate with the dominance and significance of the social platform, and allowing for judicial oversight of takedown decisions and a right of appeal”.⁷⁵² Ten tweede moeten platforms de verplichting krijgen om (a) inhoud die geautomatiseerd of middels algoritmes is geproduceerd (bv. middels bots) duidelijk te labelen (b) niet-authentieke en frauduleuze accounts die zich als anderen voordoen te identificeren en verwijderen; (c) aan een gedragscode te voldoen die misleidende en oneerlijke praktijken verbiedt, en snelle behandeling vereist van klachten over intimidatie, bedreigingen en haatzaaien, en de verwijdering vereist van smadelijke, frauduleuze en met kwade opzet gemanipuleerde inhoud (bv. *deep fake* videos). De regering lanceerde in 2019 een digitaal handvest, waarin staat dat de Canadese regering de vrijheid van meningsuiting zal verdedigen en bescherming zal bieden tegen online bedreigingen en desinformatie die de integriteit van de verkiezingen en de democratische instellingen ondermijnen.⁷⁵³ Het *Department of Canadian Heritage* heeft verder 19,4 miljoen dollar uitgetrokken voor een periode van vier jaar om een nieuw *Digital Citizen Research Program* op te starten om Canadezen te helpen inzicht te krijgen in online desinformatie en 7 miljoen dollar om burger-, nieuws- en digitale mediageletterdheid te bevorderen.⁷⁵⁴

iii. Politieke advertenties

1. Kranten en omroepen

Betaalde politieke advertenties zijn toegestaan in kranten. Artikel 282.4 van de *Canada Elections Act* (geïntroduceerd door de *Elections Modernization Act* 2018) verbiedt echter de verkoop van “advertising space to [foreign individuals, corporations, or governments] for the purpose of enabling that person or entity to transmit an election advertising message or to cause an election advertising message to be transmitted”.⁷⁵⁵ Ook betaalde politieke advertenties zijn toegestaan op televisie, maar wanneer zendtijd voor advertenties wordt verkocht aan een partij of kandidaat, moet de deze tijd op een billijke basis beschikbaar worden gesteld aan concurrerende partijen en kandidaten.⁷⁵⁶

2. Internetdiensten

Zoals hierboven vermeld, heeft Canada eind 2018 de *Elections Modernization Act* uitgevaardigd, die nieuwe verplichtingen voor online platforms met betrekking tot het inrichten van registers voor online politieke advertenties.⁷⁵⁷ De wet bepaalt dat een online platform “[that] sells, directly or indirectly, advertising space to [political parties, candidates, and groups] shall publish on the platform a registry of the persons’ and groups’ partisan advertising messages and election advertising messages published on the platform during that period”.⁷⁵⁸ Google kondigde met name aan dat politieke advertenties op

⁷⁵⁰ Idem.

⁷⁵¹ *Democracy Under Threat: Risk and Solutions in the Era of Disinformation and Data Monopoly, Report of the Standing Committee on Access to Information, Privacy and Ethics*, 2018, <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf>.

⁷⁵² Ibid., p. 42

⁷⁵³ https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

⁷⁵⁴ <https://www.canada.ca/en/canadian-heritage/news/2019/07/helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html>. Zie ook: <https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html>.

⁷⁵⁵ <https://laws-lois.justice.gc.ca/eng/acts/e-2.01/FullText.html>.

⁷⁵⁶ <https://crtc.gc.ca/eng/industr/tvradio/guidelec.htm>.

⁷⁵⁷ Elections Modernization Act 2018, c. 31, <https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=9808070>.

⁷⁵⁸ Paragraaf 325.1(2).

Google-platforms niet zou worden toegestaan tijdens de Canadese federale verkiezingen van juni - oktober 2019.⁷⁵⁹

De *Elections Modernization Act* bevat ook een aantal regels voor de verslaglegging over de uitgaven, waaronder rapportageverplichtingen voor derde partijen die zich bezighouden met partijpolitieke activiteiten, partijadvertenties en verkiezingsadvertenties. De wet bevat ook regels over oneigenlijke buitenlandse invloed die de toegestane verkiezingsactiviteiten van buitenlandse individuen, politieke partijen, groepen en regeringen beperkt.⁷⁶⁰ Tot slot verbiedt de Canadese *Elections Modernization Act* de verkoop van advertentieruimte (ook op online platforms) voor verkiezingsadvertenties aan buitenlandse partijen, groepen of overheden.⁷⁶¹

⁷⁵⁹ Zie: Google, 'Election ads in Canada' <https://support.google.com/adspolicy/answer/6014595?hl=en>. See also, Cardoso, T., 'Google to ban political ads ahead of federal election, citing new transparency rules', The Globe and Mail, 4 March 2019, <https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/>

⁷⁶⁰ Elections Modernization Act, 282.4 (1)

⁷⁶¹ Elections Modernization Act, section 282.4(5) - Selling advertising space. See also Section 319 (*online platform* includes an Internet site or Internet application whose owner or operator, in the course of their commercial activities, sells, directly or indirectly, advertising space on the site or application to persons or groups).

IViR - Instituut voor Informatierecht
Postbus 15514, 1001 NA Amsterdam, Nederland

<https://www.ivir.nl/>