University of Amsterdam

IViR (Institute for Information Law)

The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising

Final report, December 2019

Institute for Information Law (IViR),
University of Amsterdam, 2019

A report for the
Ministry of the Interior and Kingdom Relations

Institute for Information Law
Faculty of Law
University of Amsterdam
Nieuwe Achtergracht 166
1018 WV Amsterdam

The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising

Final report

Joris van Hoboken
Naomi Appelman
Ronan Ó Fathaigh
Paddy Leerssen
Tarlach McGonagle
Nico van Eijk (involved until 31 October 2019)
Natali Helberger

Amsterdam, December 2019

Contents

1. Introduction

A. General introduction

The spread of disinformation online and the potentially harmful consequences for a free democratic society have been the subject of considerable political debate and scientific research in recent years. The potentially undermining effect of disinformation on (confidence in) the democratic process and the media has been explicitly inscribed in the public consciousness by a number of international incidents.[1] The European Commission argues that disinformation can undermine confidence in the media and democracies, limit citizens' free access to information and cause an increase in radical and extremist ideas.[2] In this way, the problem associated with disinformation potentially touches on the core of Dutch society, which makes it necessary to examine the existing legal framework and possible safeguards.

The problem of disinformation has arisen in the context of a greatly changed media landscape in which the traditional, linear mass media are increasingly losing their influence at the expense of often individualised online services such as social media. The harmful effects of disinformation can also be directly linked to this changed media landscape, as these are mainly the result of new possibilities to spread disinformation on a large scale and in previously unimaginable ways.[3] Social actors seeking to profit from the dissemination of false and misleading information have always existed, but the rapid, targeted, large-scale and often personalised dissemination via internet services is new.

In this changed media landscape, a relatively small group of internationally operating internet services are central, which can therefore also have a major impact on local democratic processes.[4] What further complicates this problem are the socio-technological dissemination processes that come into play when disseminating disinformation via internet services. These include micro-targeting, astroturfing, the use of bots, trolls and other online manipulation techniques.

The problem also poses the challenge for governments to tackle disinformation in such a way as to protect an open, free and democratic society while at the same time not unnecessarily restricting fundamental rights such as, in particular, freedom of expression. Many legislators have taken up this challenge and, in response to the problem of disinformation, several initiatives have been developed at both European and national level to regulate aspects of the spread of disinformation via these Internet services.[5] However, the complexity of the problem of disinformation and the importance of the national context for regulation affecting the public debate mean that a single measure will not be sufficient.

---

1 For example, Russian interference through, among others, the Internet Research Agency in the US presidential elections 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 European Commission, *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 See, *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. 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.

B. The Dutch situation

The problem of disinformation also receives a great deal of attention in the Dutch context.[6] As far as the actual situation is concerned, recent research has shown that there is an increasingly polarised media atmosphere in the Netherlands. In addition, the disinformation-related concept of 'junk news' was found to be widespread in the Netherlands.[7] From a political point of view, the phenomenon now enjoys a great deal of political attention, with a large number of House of Representatives (*Tweede Kamer*) motions asking the government to address specific disinformation or related problems.[8] The Dutch government has also launched an awareness-raising campaign on disinformation, and recently presented its disinformation strategy to the House of Representatives.[9]

Despite the extensive attention paid to the phenomenon and the various regulatory initiatives, there are still many questions about how to deal with disinformation in the Dutch context. For example, the extent and impact of disinformation on Dutch society is still not entirely clear. There are also many uncertainties from a legal point of view. For example, 'disinformation' itself does not have an unambiguous, let alone a delineated legal definition and, given the breadth of the phenomenon, the applicable legal framework has not been properly established. It also follows that it is not always clear where the scope for national regulation lies in relation to the European regulatory frameworks. This is closely related to the fact that in terms of distribution and the amount of disinformation, there is a large asymmetry of information between Internet services on the one hand, and the legislator, researchers and wider society on the other.

This lack of clarity, which still persists with regard to the legal qualification of the phenomenon, the relevant legal framework and the possible regulatory options, together with these House of Representatives motions, is the reason for this legal investigation. Although the wider media landscape is relevant, this research only focuses on the spread of disinformation through internet services. The fact that these services play a special role in facilitating disinformation, as well as the questions that arise with regard to their responsibility, and sometimes major information asymmetry with regard to these services, makes this focus obvious. The overarching aim is to create clarity in the legal framework involved with regard to the distribution of disinformation via internet services in the Netherlands, and to indicate where there may be room for regulation.[10]

C. Research questions

The research is based on seven research questions submitted by the Ministry. The questions range from very general to very specific, but all relate to the broader issue of disinformation, the existing legal framework, and the possibility of further regulation. These seven questions are therefore all answered in the context of this broad analysis in the report of the relevant legal framework for the dissemination of disinformation through Internet services and possible regulatory options. The seven research questions are as follows:

1. What are the current laws and regulations aimed at/related to preventing the dissemination of (dis)information, and specifically for/by tech companies?
2. What are the legal and regulatory requirements for the dissemination of information? Are these described independently of the technology?

---

6 See, for example: Lower House of Parliament, session year 2018-2019, 30821, no. 51.
7 Rogers, R., & Niederer, S. '*The politics of social media manipulation: A view from the Netherlands',* 2019, p. 16.
8 See, for example: Motion Asscher en Buitenweg, Lower House, session year 2018-2019, 35 078, no. 21; Motion Asscher- Van der Molen, Lower House, session year 2018/19, 30821, no. 60; Motion Kuiken en Verhoeven, Lower House, session year 2018-2019, 32 761, no. 145.
9 See also: Lower House, session year 2018-2019, 30 821, no. 51, p. 5; Lower House, session year 2019-2020, 30821, no. 91 (also based on the interim report).
10 Motion Asscher/Van Der Molen, Tweede Kamer, 2018/19, 30821, nr. 61, nr. 62, nr. 68.

3. How does current legislation take into account the transparency of the origin of information on social media platforms? Are there limits to possible foreign influences, e.g. with regard to the placing of political advertisements (Asscher/Vd Molen motion)?
4. What supervisory options and sanctions do laws and regulations offer with regard to online manipulation (Asscher/Vd Molen motion, 62)?
5. Could deliberate online manipulation be brought under the descriptions of offences in criminal law relating to the manipulation of elections? (Asscher- Van der Molen motion, *Kamerstukken* II, 2018/19, 30821, no. 68).
6. What significance does the legal form have for the measures that tech companies can or must take with regard to content moderation, promotion of transparency and protection of citizens' rights? What is the responsibility of tech companies for dissemination through their search engines, social platforms, etc.?
7. How are citizens' rights protected against deliberately misleading information? Also in the context of the use of personal data (privacy) and freedom of expression (also with regard to the removal of content).

Since, as stated above, a number of other countries have already taken measures in the context of disinformation in recent years, it is worth analysing the choices made in these countries in order to be able to see what might be appropriate for the Dutch context. Therefore, country studies were carried out as part of the study, which included the following countries: the United Kingdom, France, Germany, Sweden, the United States, and Canada. The approach to disinformation in these countries was viewed from the perspective of the possibility of incorporating the specific choices made in these countries into the Dutch legal framework. The country studies are attached to the report. Throughout the report, reference will be made to the country studies where relevant.

D. Interim report: disinformation and political advertisements

This study was carried out in two phases. The first phase, and the accompanying interim report, focused on the first three research questions and, in particular, the specific issue of political advertising.[11] The additional question that was central to the interim report was what the regulatory framework for the distribution of political advertisements via Internet services is, and what are the possibilities for regulation (transparency in particular) in the light of the applicable normative frameworks and the country studies. This final report explicitly builds on the results of the interim report and, although this report discusses disinformation across the board, the problem of disinformation in relation to political advertisements is still taken into account in its entirety.

The focus for the interim report on political advertisements reflects the fact that the approach to disinformation in general is often linked to the possible regulation of online political advertisements. In the Netherlands, too, there have been calls for new regulations, particularly with regard to online political advertising.[12] The idea is that the advertising products of internet services facilitate a disinformation-related problem. The possibility of conducting targeted and software-driven political campaigns, without the limitations of national borders or other restrictions that apply to traditional media, creates opportunities for undue influence on the democratic process. Online political advertisements, for example, can become disinformation in the event of improper interference in the national political process by foreign actors. Subsequently, the creation of targeted political advertisements (*'micro-targeting')* also raises

11 This interim report has now been published as an appendix to the letter to the House of Representatives from the Minister of the Interior and Kingdom Relations, 'Beleidsinzet bescherming democratie tegen disinformatie', dated 18 October 2019.

12 Asscher- Van der Molen motion, Lower House, session year 2018-2019, 30821, no. 68; Kuiken en Verhoeven motion, Lower House, session year 2018-2019, 32 761, no. 145; Asscher en Buitenweg motion, Lower House, session year 2018-2019, 35 078, no. 21; Staatscommissie parlementair stelsel, '*Lage Drempels, Hoge Dijken. Democratie en rechtstaat in balans*' The Hague, 2018, p. 18.

questions about the possibility that data-driven campaigns can be used to manipulate the political debate at an individual level. However, although the distribution and impact of online political advertisements may be related to the broader problem of disinformation, both phenomena must be distinguished in both a practical and a legal sense. This final report therefore deals with the problem of disinformation across the board, covering all seven research questions.

E. Structure of the study

It was decided that the study should follow the structure of the legal framework. Within this structure, the research questions lend themselves to being answered in the course of the report. Where necessary, the conclusions will explicitly consider the answer to a specific question.

This report has the following structure. First, a number of crucial concepts will be defined. In **chapter 2,** the term "disinformation" will be dissected on the basis of the applicable legal framework, available scientific literature, reports and policy documents. Then, in **chapter 3,** we will look at the diversity of Internet services (tech companies) that need to be considered in the debate on the problem of the spread of disinformation. This involves a wide range of different services, including social media, search engines and communication services. In this report, the choice was made to use the term 'internet services' instead of the term 'tech companies'. After this conceptual framing of the central concepts, the report provides insight into the relevant legal framework for dealing with disinformation applicable in the Netherlands. This will be divided into three parts. First, we will consider the constitutional standards at Dutch and European level (**chapter 4**); secondly, we will discuss the framework applicable to internet services under European law (**chapter 5);** and thirdly, we will provide an overview of the specific legislation and (self-) regulation in the Netherlands (**chapter 6)**. The discussion of the European legal framework will also consider relevant policy developments at European level with regard to disinformation.

In the final part of the report, In the final part of the report, the insights provided by the analysis of the problem and the legal framework are summarized and brought together. (**chapter 7**). The insights from the country studies are also taken into account. These country studies are attached. Finally, the relevant conclusions resulting from the research are discussed in summary form in order to arrive at a final conclusion with regard to the research questions (**chapter 8**).

2. Disinformation

- Disinformation is verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm;
- Mainly useful as a policy term, not as a legally defined concept.
- It includes many existing legal categories (illegal & unlawful) but also unregulated harmful expressions;
- Different actors are involved: the creator, the medium of distribution and the public;
- Dissemination is technologically enhanced (micro-targeting / astroturfing, etc.).
- Disinformation occurs in different contexts with each time unique problems: e.g. news, hate-speech, commercial and political campaigns.

A. Conceptual framework

The concept of disinformation has now become the leading concept in policy circles for identifying a wide range of problems in the field of information quality and the media landscape. It is the term that, from a scientific and normative point of view, is preferable to more problematic terms such as 'fake news'.[13] In this context, it remains very important, particularly in the case of policy measures and/or new forms of regulation, that the concept of disinformation and the underlying problems are clearly defined, framed and empirically substantiated. This conceptual framework will be discussed in this section, after which both the actual problems and the different contexts in which disinformation is relevant will be discussed.

i. Definitions

A variety of definitions and descriptions of disinformation are available in the relevant literature. The following approaches have been particularly influential in providing a conceptual framework for the issue.

In the report *Information Disorder* for the Council of Europe, Wardle and Derakhshan present a broad conceptual framework in which they distinguish between the concepts of dis-information, mis-information, and mal-information. They stress the importance of distinguishing between correct and incorrect messages, between messages created, produced or distributed by actors who want to cause damage, and messages for which this is not the case. The specific definitions chosen by Wardle and Derakhshan are as follows:

- "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]

The European Commission, in its 2018 Communication entitled 'Tackling online disinformation: a European approach', has opted for a related but broader definition. The Commission defines disinformation as "verifiably false or misleading information that is created, presented and disseminated for economic gain

13 See McGonagle 2018. See also McGonagle and others 2018.
14 Wardle, C., & Derakhshan, H. 'Information Disorder. Toward an interdisciplinary framework of research and policymaking', z.p., 2017 p. 20.

or to intentionally deceive the public, and may cause public harm ".[15] Two notable differences are the role played by the actor's *intent* and whether *economic gain* is important. The definition of Wardle and Derakhshan requires that disinformation is always created with the intention of causing harm. On the other hand, in the Commission's definition, this intention only comes into play when it comes to deceiving the public and not when it comes to economic gain. When economic gain is at stake, the Commission's definition only requires that the information is factually inaccurate or misleading in order to qualify as disinformation, while Wardle and Derakhshan do not include profit interest at all. The Commission's definition in this respect is a clear extension of the concept of disinformation. The Commission's definition includes incorrect or misleading commercial advertisements and incorrect news items which do not fall under the definition of Wardle and Derakhshan. The value of such a broad definition may lie in the fact that it recognises how the commercial success of inaccurate information may overshadow qualitatively better information. The Commission uses the same definition in the EU Code of Practice on Disinformation.[16]

The Commission's definition is based on the independent High Level Expert Group (**"HLEG")** established by the European Commission, which also uses such a broad definition. The report from January 2018, *'A multi-dimensional approach to disinformation'*, speaks about "false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit".[17] In this case, therefore, intention does not play a role either when economic considerations are at stake. In addition, the HLEG adds that debates on "fake news" cover a "spectrum of information types". They include " relatively low-risk forms such as honest mistakes made by reporters, partisan political discourse, and the use of click bait headlines, to high-risk forms such as for instance foreign states or domestic groups that would try to undermine the political process in European Member States and the European Union, through the use of various forms of malicious fabrications, infiltration of grassroots groups, and automated amplification techniques".[18] A recently published report by Wardle contains an extensive discussion of the various forms of disinformation on a spectrum from 'low harm' such as satire and parody to 'high harm' such as fabricated information.[19]

The *European Broadcasting Union* has opted for a definition close to that of Wardle and Derakhshan. In their position paper, disinformation is defined as "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] Furthermore, in a recent study of February 2019, Bayer et al. offered the European Parliament's Committee on Civil Liberties, Justice and Home Affairs a balanced definition in which disinformation is approached as a phenomenon characterised by specific elements. Disinformation is information (i) designed to be false, manipulative or misleading, (ii) with the intention of generating insecurity, tearing cohesion or inciting hostility, or directly to disrupt democratic processes, (iii) on a topic of public interest and (iv) often uses automated dissemination techniques to amplify the effect of the communication t.[21] Particularly interesting is the emphasis in this definition on the method of dissemination.

The Dutch government's definition of disinformation is narrower than the European Commission's definition. In the recent parliamentary letter in which the government sets out its policy on disinformation, disinformation is defined as "the deliberate, often covert, dissemination of misleading information, with

15 European Commission, 'Tackling online disinformation: a European approach', COM(2018) 236 final, point 2.1. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018DC0236rom=EN

16 European Commission, *'Code of Practice on Disinformation,* preamble, 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.

the aim of damaging public debate, democratic processes, the open economy or national security".[22] What is striking about this definition compared to that of the European Commission is that it only covers misleading information and not also incorrect (but possibly not misleading) information. Furthermore, the profit element is missing, which means, for example, that *clickbait* does not fall under the definition of the Dutch government, but does fall under the definition of the European Commission.

It is clear that there is no clear legal qualification of the concept of disinformation. However, there are a number of aspects that can be identified that are consistently reflected in all definitions: (i) the information must be **incorrect** or **misleading**. Furthermore, (ii) any definition also includes the element of **social harm**. It is not always clear or well worked out what role this harm criterion plays. Should the information actually be harmful, or is the intention to disseminate information in a harmful way sufficient? It is also unclear what this harmfulness means in terms of content. The European Commission talks about " public harm" while Wardle and Derakhshan look at harm to a person, social group, organisation or country. In any case, it remains unclear what exactly is meant by this. These broad and vaguely defined concepts of harm create a clear field of tension with freedom of expression, which, in principle, also protects the publication and dissemination of inaccurate information.[23] Disinformation is the deliberate, often covert, dissemination of misleading information, with the aim of damaging public debate, democratic processes, the open economy or national security.

Furthermore, (iii) **intention** of the actor, or whether something was deliberate, also plays a role in each definition. However, here too there is no consensus on the object of this intention. In the definition of the HLEG, the intention must relate to "public harm", and in the case of Wardle and Derakhshan, the intention must also be to cause harm, while in the case of the Commission, the intention must relate to deceiving the public. Finally (iv) the **economic gain** of the actor often plays a role, although it is not part of the definition of Wardle and Derakhshan.

This study is in line with the European Commission's definition as set out in the 2018 Communication: disinformation is "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm ".[24] From the point of view of policy making, it is preferable to follow this authoritative definition, which people often seem to agree with.[25] Where necessary, this definition will be further qualified along the lines of the four factors mentioned above, in particular with regard to the social harm and the actor's intention. The specific interpretation of these two factors in particular is decisive for a legal qualification in a specific case. The choice was made to follow the broad European definition rather than the more limited Dutch definition, because an analysis based on a broader European definition gives a more comprehensive picture of the regulatory landscape. For the same reason, the choice is also made to include illegal statements and *hate speech* in disinformation, whereas many studies do not.[26] In addition to this general definition of disinformation used by the European Commission, this report will also make use of the threefold division of Wardle and Derakhshan. Their definition of disinformation will be referred to as 'disinformation in the narrow sense' and to the definition of the EC as 'disinformation' or 'disinformation in the broad sense'.

22 Tweede Kamer, 2019-2020, 30 821 nr. 91, dd. 18 October 2019 (kamerbrief) p. 3.
23 See for a discussion: 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 See Section 2.A.II.

Disinformation is "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".[27]

ii. Scope: type of statements & legal qualification

In addition to the lack of a clear legal definition, it is also clear that each definition covers a wide range of forms of communication. Even if information is only considered in a digital context, the concept of disinformation covers a wide variety of media and forms of communication. The definition of the EC includes statements ranging from commercial advertisements, political discussion, news articles, medical claims, conspiracy theories, blog posts, political advertisements, e-mails, posts on social media, vlogs and private messages via media such as WhatsApp, Telegram or Facebook.

These different forms also have widely differing legal qualifications. Many of the expressions that fall under the heading of disinformation are already regulated by law. First of all, this could include illegal and therefore punishable expressions such as defamation, slander, insulting behaviour and certain forms of electoral fraud. Then there are unlawful expressions such as misleading advertisements, unfair commercial practices, intellectual property infringements, or unlawful press publications, that can be addressed via the private law route. Thirdly, we could also consider public-law regulated expressions such as the various advertising bans and media regulation.

While many of the expressions covered by the concept of disinformation are therefore already regulated by law, this is not the case in all cases. Crucial here is the distinction between illegal and unlawful information on the one hand, and harmful information on the other. Although these terms are often mentioned in one sentence, it is important for the legal framework to have a clear understanding of the distinction.[28] As can be seen from the above, illegal and unlawful information are both sanctioned by law, whereas in principle harmful information is not. Illegal information constitutes a violation of a criminal law prohibition, and unlawful information leads to private liability or measures. On the other hand, harmful information is not legally regulated and comes under the protection of freedom of expression. Harmful information often refers to things that, although within the limits of the law, are seen as socially undesirable. This may include fabricated conspiracy theories, extreme political views, erroneous medical theories such as in the anti-vaccination movement, or misleading news reports. It should be emphasised that many of these statements, which are not regulated but are perceived to be harmful, are not regulated because, in principle, they are part of a healthy social debate where there must also be room for erroneous information that is protected by freedom of expression.[29] Thus, under the umbrella of disinformation, we find expressions that are regulated or prohibited by law, but also unregulated expressions that enjoy the protection of the right to freedom of expression. In this way, the term covers both the classical doctrines, framed by detailed case law, such as libel and unlawful press publications, and non-standard phenomena such as conspiracy theories or erroneous press releases.

This broad legal classification is not always followed in the literature. For example, the HLEG explicitly excludes all illegal or unlawful information from disinformation,[30] in order to further sharpen the concept.[31] In the LIBE study by Bayer *et al.,* hate speech, for example, also falls outside the definition of

27 European Commission, 'Tackling online disinformation: a European Approach', COM(2018) 236 final, par. 2.1.
28 See further 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 See further chapter 4.
30 HLEG, *'A multi-dimensional approach to disinformation'*, p. 12.
31 According to 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.

disinformation, mainly in order to limit the scope of the study.[32] This report does, however, explicitly use the broad scope set out above. This is firstly because the research questions explicitly demand that the legal dimensions be interpreted, and secondly because this broad discussion of disinformation is necessary to see how different jurisdictions and current regulatory instruments intertwine, or where there are gaps. This is also why, as explained above, this report follows the broad definition of disinformation.

The possible approach and enforcement tools depend on the legal qualifications of the underlying act. A complicating factor in this is that in many cases an actual determination of the existence of illegal and/or unlawful information by designated authorities does not take place and any actions with regard to this information are taken by relevant services on the basis of the terms of use. This fact is, of course, closely related to the way in which disinformation is actually disseminated and has an impact.

iii. Actors

One of the defining characteristics of the problem of disinformation is the wide variety of actors involved. According to Wardle and Derakhshan, the involvement of different actors at different stages of the spread of disinformation is one of the three key elements of disinformation.[33] Wardle and Derakhshan distinguish three phases: the creation of disinformation, the production - when the message is turned into a media product and, thirdly, the dissemination or distribution of the information.[34] In these three phases, different actors are relevant: the creator or client of the disinformation, the medium through which the disinformation is disseminated and the public that receives and further distributes the disinformation.

The first category is the creator of, or instructing party behind, the disinformation. This is the actor who, according to the definition of disinformation, has the intention to cause public harm and deliberately spreads false or misleading information. The potential actors behind the disinformation are as broad as the problem itself. They may be individuals, trolls, political parties, state actors, social interest groups or commercial companies, for example.[35] This distinction is particularly relevant in view of the fact that the resources available to the various parties are highly variable, and that possible regulation must be tailored to the relevant actor; the same measures are not appropriate for a commercial company and a state actor. In the literature, much attention is paid to disinformation campaigns designed by state actors, as these can potentially have a very high impact and can be particularly worrying from a democratic point of view.[36] Another type of actor that can be placed in this category are the so-called 'trolls' that - whether or not on assignment - spread disinformation, in order to create divisions and provoke reactions.[37] These trolls are "(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] In order to be able to categorise a creator of disinformation correctly, five factors can be used, drawn up by Wardle and Derakhshan: the type of actor (state, commercial, political party, etc.), the degree of organisation, motivation, target group of disinformation (national, international, specific ethnic group, etc.) and

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.

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.

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

the use of automated technology.[39] The European Association for Viewers Interests (**"EAVI")** has identified money, political influence, humour and passion or ideological beliefs as possible sources of motivation for disinformation.[40] One of the major challenges with regard to the creator of disinformation is not only that the group is very diverse, but also that the deception often lies in who the creator is. Misrepresentation of the speaker is one of the most important vectors through which disinformation operates. Disinformation is often spread under a false name, for example by false accounts.[41]

A second important actor in the context of this research is the channel through which the disinformation is disseminated. Within the scope of this research, these are specific internet services such as platforms, direct messaging services or search engines. These services, which are characterised by a lack of traditional editorial control, in many cases also facilitate the dissemination of disinformation through sponsored content channels. These channels are important because disinformation campaigns often operate on the same logic as the classic advertising industry: the goal is to hold people's attention for as long as possible and to influence their behaviour towards a specific goal.[42] In addition to the use of sponsored channels, disinformation is also often spread via the regular channels of such internet services. The policy of internet services with regard to advertisements or the use of the regular channel can therefore have a major influence on the possibilities that the creators of disinformation have at their disposal to spread disinformation.

Next, a very crucial actor for the dissemination of disinformation is the general public, and regular users of Internet services. The European Commission states that the fact disinformation is shared on a large scale by unsuspecting users is a unique aspect of the problem.[43] The general public is on the one hand the recipient and the target group of the disinformation, but because of the organisation of the various internet services they are in most cases also the disseminators of the information in question by sharing, liking, retweeting or otherwise.[44] This is also referred to as the 'participatory nature' of disinformation, and is one of the major challenges for the possible approach to disinformation.[45]

The relationships between these different actors also show how much the problem of disinformation is linked to the actual means of technological dissemination. This is therefore the starting point for concluding the conceptual framework for disinformation, and switching to the way in which disinformation is disseminated in practice and what the actual social influence is.

B. Problem and factual situation

After this conceptual framing of the concept of disinformation, on the basis of which it is clear how broad and comprehensive the concept is, it is important to further clarify the actual problems. In the above-mentioned 2018 Communication, the Commission identified six possible harmful effects of the widespread dissemination of disinformation. Most importantly, there is a risk that disinformation (i) "erodes trust in institutions and in digital and traditional media, and harms our democracies by hampering the ability of

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 Disinformation 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; 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 European Commission, *Tackling online disinformation: a European Approach* COM(2018) 236 final, p. 6. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236.
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

citizens to take informed decisions". Because of this influence on the media, disinformation can (ii) have an impact on freedom of expression because it hampers the ability of citizens to take informed decisions.. It can also lead to (iii) reduced trust in science and (iv) increased popularity of radical and extremist ideas and activities. Disinformation is also problematic in an international context. It can be used by foreign actors (v) to influence specific social debates or even (vi) to influence the national election process and jeopardise national security.[46]

These harmful effects do not stem directly from the disinformation as such, but mainly from its widespread distribution via Internet services.[47] This is also where the explanation can be found for the current political attention on the phenomenon. The kind of expressions themselves are generally not a new development. This is clear from the fact that many of the issues covered by the concept have long been regulated. On the other hand, the widespread loss of editorial control, as well as the scale and speed of the dissemination of false or misleading information, mediated by Internet services and often enhanced by automated dissemination methods, are new.[48] The rapid online distribution by means of the normal channels of, for example, social media, or artificially amplified by means of automated bots, makes it often difficult to determine where the disinformation comes from.[49] In this way, Internet services form the central pivot that play a mediating and facilitating role in the spread of disinformation. As a result, Internet services and the way they are designed are crucial to the spread and potential impact of disinformation.[50]

In its Communication, the Commission identifies three categories of methods that facilitate the dissemination of disinformation:

- " *Algorithm-based*: (...) By facilitating the sharing of personalised content among like-minded users, algorithms indirectly heighten polarisation and strengthen the effects of disinformation;
- *Advertising-driven*: Today's digital advertising model is often click-based, which rewards sensational and viral content. This model relies on advertising networks operated by agencies that ensure real-time placement of ads based on algorithmic decision-making. This facilitates the placement of advertisements on websites that publish sensationalist content appealing to users' emotions, including disinformation;
- *Technology-enabled*: Online technologies such as automated services (referred to as "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 (referred to as "troll factories")."[51]

With regard to the dissemination of disinformation on the basis of advertising, the channels and techniques offered by Internet services for commercial advertising (e.g. sponsored content by means of real time bidding) will be used, as indicated above, and will also be operated on the basis of the same logic. After all, commercial advertising and disinformation both aim to grab people's attention and influence their behaviour.[52] As indicated above, the disseminators of disinformation and some Internet services have

46 European Commission, '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.
50 Rogers, R., & Niederer, S. '*The politics of social media manipulation: A view from the Netherlands',* 9 april 2019, p. 17.
51 European Commission, COM(2018) 236 final, point 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; 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/ .

interests that are in line with each other. The fact that the dissemination of disinformation via Internet services operates on the same logic as the online advertising industry also partly explains the success of the dissemination of disinformation via these services.[53]

With regard to algorithm-based dissemination, disinformation also takes advantage of the structure of many Internet services, particularly social media, which can benefit from giving priority to personalised or sensational information. In this way, the disseminators of disinformation make use (or abuse) of the organic methods of dissemination via these Internet services. An example of this is search engine optimisation in which the algorithms on the basis of which search results are displayed and arranged are manipulated in order to make certain (dis)information the most visible.[54] On the other hand, when using bots and fake accounts, it can rather be said that the structure of a particular Internet service is being abused. An example of such techniques is astroturfing. Bots or fake accounts are used to create the impression of broad public support or of a grassroots movement. The underlying objective is often economic gain or the promotion of a political point of view.[55] These three categories of methods to facilitate the spread of disinformation are what Neudert calls 'computational propaganda': 'the assemblage of social media, autonomous agents and algorithms tasked with the manipulation of opinion'.[56] Methods that fall under this category are micro-targeting, bots, troll factories, astroturfing and search engine optimisation.[57]

This overview of the various technologically mediated and manipulative ways from which disinformation is disseminated also clearly demonstrates the connection with the concept of online manipulation. The issue of disinformation is tied to new forms of online manipulation that have recently come to the attention of researchers and policy makers. Indeed, the European Commission makes a specific link between manipulation and disinformation, as disinformation is spread by the manipulative use of online platforms' infrastructures.[58] Scholars have defined online manipulation as the use of information technology to "covertly influence another person's decision-making," and online manipulative practices as applications of information technology that "impose hidden influences on users, by targeting and exploiting their vulnerabilities".[59] One of the harms caused by online manipulation is that it subverts an individual's decision-making power and undermines autonomy.[60] Thus, the essential elements of problematic online manipulation are the covert and hidden nature of the influencing, playing on a person's vulnerabilities. Indeed, the Council of Europe's Committee of Ministers (COM) has also focused on the subliminal nature of online manipulation. In its 2019 *Declaration on the Manipulative Capabilities of Algorithmic Processes*, the COM draws a distinction between "permissible persuasion" and "unacceptable manipulation". Problematic manipulation takes the form of influence that is "subliminal, exploits existing vulnerabilities or cognitive biases, and/or encroaches on the independence and authenticity of individual decision-making".[61] The COM highlight the dangers for democratic societies from online manipulation facilitated by technology companies, including that they have the capacity not only to predict choices but also to "influence emotions and thoughts and alter an anticipated course of action, sometimes subliminally".[62] Crucially, this can also include the manipulation of political behaviour. In light of this danger, the COM emphasises that there is a need to assess regulatory frameworks related to political communication

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.
55 See Leiser, M., *'AstroTurfing, 'CyberTurfing' and other online persuasion campaigns',* European Journal of Law and Technology 2016, p. 2.
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.

and electoral processes to safeguard the fairness and integrity of elections offline as well as online in line with established principles. In particular it should be ensured that voters have access to comparable levels of information across the political spectrum, that voters are aware of the dangers of political redlining, which occurs when political campaigning is limited to those most likely to be influenced, and that voters are protected effectively against unfair practices and manipulation.

This problem of disinformation also receives a great deal of attention in the Dutch context.[63] As far as the actual situation in the Netherlands is concerned, Rogers and Niederer recently conducted research into disinformation and 'junk news' on social media in the Netherlands. This research does not provide any evidence for foreign disinformation campaigns around the 2019 Provincial Council and European Parliamentary elections. It turned out, however, that the Dutch media sphere is increasingly polarised and that so-called 'junk news' is widespread with regard to issues such as Zwarte Piet, MH17, the climate and the European Union.[64] The term 'junk news' used in the research is broader than the definition of disinformation used here and also includes sensational information, click-bait and politically extreme expressions, which are not distributed with the intention of causing social damage.[65] Furthermore, a study conducted by the Rathenau Institute in 2018 concludes that, for the time being, disinformation has not had a major negative impact on Dutch society.[66] In addition, recent research for the Commissariaat voor de Media has also shown that the problem of 'filter bubbles' reinforced by algorithmic processes is not widespread in the Netherlands, although there is reason to keep a close eye on the influence of filtering technologies on the media landscape. The Dutch public still mainly makes use of channels that offer news that are not filtered through algorithms.[67]

C. The Context of disinformation

Since disinformation covers a wide range of subjects, it is helpful to place different forms of disinformation in a concrete context. Disinformation is so often seen in connection with the distribution of news, or junk news, in relation to hate speech and extremist expression, linked to commercial expression, and in the context of improper foreign influence. These are very different contexts, all of which raise unique social and policy issues, and have their own relationship to freedom of expression.[68] In this way, commercial statements are protected to a lesser extent,[69] while political statements, including political advertisements, can rely on the greatest possible protection of freedom of expression.[70] Hate speech, on the other hand, falls partly outside the protection,[71] and with regard to the media landscape, the state has significant positive obligations to protect pluralism and free newsgathering.[72] When talking about possible regulation 'of disinformation', it is therefore important to have a clear picture of the specific context in which disinformation is discussed. As the interim report focused on the relationship between disinformation and political advertisements, this is discussed separately in section 2.D below.

63 See, for example, Lower House of Parliament, session year 2018-2019, 30821, no. 51; Letter to Parliament from the Minister of Justice and Security, 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.

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

66 Cologne, I. van e.a. '*Digitisation of the news-Online news behaviour, disinformation and personalisation in the Netherlands*', 2018, The Hague: Rathenau Institute.

67 Moeller, J., Helberger, N. & Makhortykh, M., 'Filterbubbels *in Nederland*' Institute for Information Law, 2019.

68 See further chapter 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, at paragraph 31; Article 7(4) of the Constitution.

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

71 Seurot v France (No 57383/00) 18 May 2004.

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

i. Disinformation and news

Much of the discussion and existing research on disinformation focuses on production, dissemination and access to news. This is logical in view of the crucial role that a free, independent and high-quality media plays for the functioning of a democracy. Pluralism and free newsgathering are necessary for the democratic process and it is feared that the dissemination of disinformation through news articles will undermine this by, among other things, undermining general trust in the media. Disinformation related to news is often referred to as 'fake news'. However, this term has fallen into disuse in research and policy circles. This is in the first place the case because the problems that were indicated with it are broader than just news, and are better covered by the term 'disinformation'. Secondly, the term is strongly associated with political and historical strategies to discredit journalists.[73] As discussed above, another term used to refer to this diverse problem of disinformation in the context of news is 'junk news'.[74]

There is a lot of literature available on the interface between disinformation and news. A wide range of news forms are relevant, from blog posts, tabloid news to investigative journalism. What always matters is that reporting presents itself as a reliable source of news, when it is actually a form of disinformation. See, for example, the definition of McGonagle *et al*.: 'Information deliberately manufactured and distributed with the intention of deceiving and misleading others in order to believe in untruths or question verifiable facts; it is misinformation that is presented as news or is likely to be seen as news' ('*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*') .[75]

With regard to the various forms of news that could be included, Tandoc *et al.* made a typology in 2017 of all the definitions of 'fake news' that have been in circulation in the past 15 years. The categories are news parody, fabricated news, news satire, manipulated photos, advertising and propaganda.[76] In the same year, EAVI developed an influential 'infographic' in which different types of misleading news are divided into ten categories and then analysed according to motivation and influence. The ten categories that EAVI distinguishes are: propaganda, click-bait, sponsored content, satire and hoax, error, partisan, conspiracy theories, pseudoscience, misinformation and bogus.[77] Wardle also indicates that it is important to distinguish between the different news items that can relate to disinformation. It proposes the following categories: satire or parody, misleading content, imposter content, fabricated content, false connection, false contexts or manipulated content.[78] The HLEG report can then be recalled where it was emphasized that 'fake news' includes a spectrum of information types that can be placed on a scale from low to high risk.[79] What clearly emerges from all these different typologies is again the breadth of the problem, even when the focus is on disinformation in the context of the news. It is also worth noting that the different forms of appearance also have different legal qualifications. Satire and parody, for example, are explicitly protected by freedom of speech.[80]

---

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.

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 and others, '*Inventarisatie methodes om "nepnieuws" tegen te gaan'*, Institute for Information Law, 2018, p. 12 with reference to: the Ethical Journalism Network: http://ethicaljournalismnetwork.org/tag/fake-news.

76 Edson, C. Tandoc, and others, *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 and others, '*Inventory of methods to combat 'fake news"*, Institute for Information Law, 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. Unification of Bildender Künstler by Austria, 25 January 2007

For the empirical situation in the Netherlands with regard to the spread of junk news and the societal influence, we can again refer to the study by Rogers *et al.*, and the study by the Rathenau Institute, which showed that the Netherlands has an increasingly polarised media landscape with a broad spread of junk news, but that the impact on Dutch society so far seems limited.[81]

ii. Disinformation and hate speech

Further, the distribution of disinformation via internet services is often linked to the distribution of hate speech.[82] Disinformation itself can also qualify as hate speech and the combination of these dynamics in practice can be extremely dangerous and harmful. It is striking that the HLEG explicitly excludes hate speech from the concept of disinformation in its study. As indicated earlier, the HLEG even goes so far as to exclude all forms of illegal or unlawful statements from disinformation.[83] Bayer *et al.* also explicitly do not include hate speech in their research. They do not exclude it from the definition of disinformation itself, only from the scope of their research.[84] In their report, Wardle and Derakshan do not consider hate speech to be part of disinformation, but they do classify it as misinformation. This is because hate speech usually uses a reality-based fact (e.g. skin colour, sex, sexual orientation or religion) to harm someone.[85] The Commission does not express an explicit opinion on this point, but it does explicitly include illegal and unlawful statements in its definition of disinformation.[86]

Although the fact that hate speech is not consistently included in research into disinformation, it is important to consider the problem of disinformation explicitly from the perspective of hate speech. It is precisely this perspective that clearly reveals the complexity of the legal issues and the challenges that any additional regulation will have to face. After all, the boundary between illegal or unlawful hate speech on the one hand, and only harmful or shocking expression on the other, is notoriously difficult to draw. This combined with the rapid distribution on scale via internet services makes the combination of hate speech and disinformation in an online context a special challenge.

iii. Disinformation and commercial communications

The link between disinformation and commercial interests is not always explicitly considered, although it is precisely this link that is responsible for extending the scope of the of the concept of disinformation in the European Commission's definition. This link should take into account the commercial interests of the disseminator (see also the role of 'economic gain' in the Commission's definition), but also the commercial interests of the Internet services that mediate the dissemination. The two are closely linked now that disinformation can be spread for commercial gain using the sponsored channels of many social media companies intended for commercial advertising. In this way, the online advertising industry and the dissemination of disinformation are closely linked.[87] It is particularly relevant to make this link with commercial interests explicit, as it means that regulation of commercial practices in general and commercial advertising in particular may apply. This type of regulation is specific to the commercial context, and often

81 Rogers, R., & Niederer, S. 'The *politics of social media manipulation: A view from the Netherlands', 2019*, p. 4 & p. 16; Cologne, I. van e.a. 'Digitisation of *the News-Online news behaviour, disinformation and personalisation in the Netherlands', 2018*, The Hague: Rathenau Institute, p. 4.

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 See also the introduction to this report.

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

86 European Commission, *'Tackling online disinformation: a European approach'*, COM(2018) 236 final, point 2.1. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018DC0236rom=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/

only applies in the case of commercial practices aimed at consumers. On the other hand, it does not apply, for example, to disinformation in the context of news dissemination and journalism.

iv. Disinformation and foreign influence

There is currently a particular focus on disinformation and foreign influence, and according to the European Commission, mass online disinformation campaigns are being used by "foreign" actors, "foreign" governments, and "third countries".[88] The purpose of these campaigns is to sow distrust and create societal tensions in countries, influence political decisions in the EU; manipulate policy, societal debates; and may be part of hybrid threats to internal security, including election processes.[89] As such, there are policy debates at national and European level about how to counter disinformation from aboard, and a specific focus on foreign influence. In the Netherlands, for example, disinformation by foreign actors is an explicit part of national security policy.[90] Indeed, as discussed in Chapter 4, it should be remembered there have been previous periods when fear of foreign influence has come to fore, including in relation to disinformation and propaganda, and has long animated discussions about freedom of expression, particularly during the Cold War period. This has been especially so for the broadcasting sector for many years, including the jamming of signals.

Given this renewed focus on the *foreign* element of disinformation, the four special international mandates on freedom of expression in their Joint Declaration on Fake News, Disinformation and Propaganda, reiterated two specific fundamental principles under international freedom of expression standards in relation to foreign influence: first, freedom of expression is guaranteed "regardless of frontiers", and freedom of expression standards limit any restrictions not only within a jurisdiction, "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] And second, the jamming of signals from a broadcaster based in another jurisdiction, or the withdrawal of rebroadcasting rights in relation to that broadcaster's programmes, is legitimate "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]

Thus, there is very limited room under international human rights standards to target the dissemination of information merely on the basis that it is of *foreign* origin, and any restriction on information from abroad must satisfy the very strict test under freedom of expression standards that they provided for by law, serve one of the legitimate interests recognised under international law, and be necessary and proportionate to protect that interest.

D. Disinformation and political advertising

In the current diverse debate around disinformation, the distinct issue of "political advertising" has become a prominent part of the policy debate. For example, the European Commission has linked the issues of disinformation and political advertising in its 2018 Communication on *Tackling online disinformation: a European Approach.* The European Commission argues that online platforms have not made 'sufficient information available on the use of strategic dissemination techniques, such as paid human influencers and/or robots to market messages', and have not provided 'sufficient transparency on political

88 European Commission, *'Tackling online disinformation: a European Approach',* COM(2018) 236 final, par. 1 & 3.5.
89 Second Chamber, 2019-2020, 30 821 no. 91, dd. 18 October 2019 (letter of assembly) p. 4.
90 Parliamentary Papers II 2018/19, 30821, no. 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.

advertising and sponsored content'.[93] The Commission recommended that online platforms should '[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', and '[e]nsure transparency about sponsored content, in particular political and issue-based advertising'.[94] In relation to bots, online platforms should establish 'clear marking systems and rules', to ensure no confusion with human interactions.[95]

However, there is no definition of political advertising in the 2018 Communication, and a number of different types of money-driven methods to distribute political communication are arguably conflated and not explained, such as paid influencers, use of bots, sponsored content, (targeted) political advertising, and issue-based advertising. Further, the Communication first draws a distinction between political advertising and sponsored content, and then later, mentions political advertising and issue-based advertising as being examples of sponsored content. And yet, it is not clear from the Communication what the exact connection is between the distinct issue of disinformation, and political advertising. As such, it is important to set out what can be understood as political advertising facilitated or carried by internet services. Also, because political advertising necessarily involves *political* content, any possible regulation of political advertising needs to take account of the fact that political advertising is legitimately used by political parties and campaigners.

The qualification 'political' in the concept political advertising and political communications can have a number of different meanings. Political could be understood in the narrow sense of the word as referring to communications by political parties, in particular during election time. In the narrowest sense, this would mean that political advertising amounts to the promotion of candidates for elections. In the broader sense, political advertising consists of paid political communications on issues of public concern, for instance through what are also called 'issue ads'. Notably, this distinction is not just a matter of content, but also a matter of the variety of actors involved. Whereas election ads are most likely to be sponsored by specific political parties and/or candidates themselves, issue ads and paid-for political communications involve a much larger and diverse landscape of actors that are paying to find effective distribution of their viewpoints and political interventions. As a result, undue influence on and manipulation of the democratic debate is most likely connected to the latter and more broadly defined form of paid political communication. From a legal perspective, any definitions by a regulatory approach to political advertising (in contrast to commercial advertising) should be informed by the relevant normative distinctions in the jurisprudence of the European Court of Human Rights, discussed in detail in chapter 4.

A first type of paid political communications that can be distinguished is *sponsored* and *promoted* content. This is a distinction that is based on the paid-for communications channel that is offered by particular internet services, in addition to their channel for 'organic' user content. A classic example would be a political party making an advertisement informing voters about its policies, and using Google's advertising platform (Google Ads) to generate impressions for visitors of websites in the Google Ads network, pay to have the advertisement displayed in Google Search results for particular search queries, or pay to have it inserted in the viewing experience of on an online media platform like YouTube. Other examples would be paying for sponsored tweets on Twitter, or a sponsored post on Instagram or Facebook.

This type of advertising is in a sense similar to *paid* political advertising in newspapers or on television, where the newspaper or broadcasters sells advertising space to a political party or group. However, a distinctive feature of internet services is to facilitate much more fine-grained targeting measures and tools and the ability to engage in political microtargeting, by 'creating finely honed messages targeted at

93 Idem, par. 3.1.1.
94 Idem, par. 3.1.1.
95 Idem, par. 2.1.

narrow categories of voters' based on data analysis 'garnered from individuals' demographic characteristics and consumer and lifestyle habits.[96] For example, Facebook's service Facebook Audience allows the targeting of advertisements based on a user's age and gender, lifestyle, education, relationship status, job role, online purchases activity, and location. A variety of sophisticated tools for targeting audiences on platforms have emerged, including for example *look-a-like targeting*.[97] Besides the additional exposure that can be paid for by using the sponsored and promoted content services, the use of this channel tends to involve additional metrics on subsequent audience exposure and interactions, facilitating programmatic engagement and data-driven evaluations by advertisers. Targeting can also be used by governments to reach certain communities and diasporas from abroad.[98]

Indeed, political parties and associated campaign operations themselves may also combine voter information they gather or pay for, and combine this information with the services offered by internet services. Whereas such data-driven practices can facilitate the political process and political participation, these practices have raised some clear issues and attracted the attention of regulators. For example, the Information Commissioner's Office, in its investigation of the Cambridge Analytica scandal, detailed how political parties had purchased "marketing lists and lifestyle information from data brokers", and combined this with "electoral data sets they hold".[99] Thus, the issue of microtargeting not only involves paying for services offered by online platforms, but also buying data from data brokers and obtained electoral data and using this data and additional services to optimize campaigns and communications. Political microtargeting raises a distinct set of regulatory issues, ranging from data protection and privacy, to manipulation, political participation and the integrity of elections.[100]

Second, there is political communications that proliferates as *organic content*. This could be where a political party simply makes a campaign video itself, and publishes the video on its YouTube channel; or where the political party writes a campaign message, publishes the post on its Facebook page, or tweets from its own Twitter account. Crucially, political campaigns can, with or without the use of sponsored content, engage in certain amplification techniques, which are a large and legitimate part of modern political campaigning. This is a type of *organic* reach, where campaigners spread their messages through Facebook, Instagram, and Twitter, and encourage supporters to share with their friends, family, and followers. Some of these practices will involve the use of money to fund activities of end-users and/or pay for specialized services, some of which may be considered illegitimate by relevant internet services or even unlawful from a legal perspective, but it's much harder to draw a line between organic content that involved payment and 'normal' organic content.

The optimization of organic reach of relevant messages can take place through a wide variety of techniques, tools and practices. Indeed, bot software can be used, and on the use of bots in political campaigning, the UK Electoral Commission has stated that it does not think "that there is anything wrong with campaigners using bots to post messages telling voters about their policies and political views", or campaigners telling staff to post campaign messages.[101] However, it becomes problematic when these techniques are used to "deceive voters about a campaigner's identity or their true level of support, or

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 For a discussion of some of these instruments and how they can lead to discrimination, see Amit, D., Makagon, J., Mulligan, D.C., & Tschantz, M.C., '*Discrimination in Online Personalization: A Multidisciplinary Inquiry' 2018*, p. 20-34.

98 See 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. See also: Gibney, E. 'The scant science behind Cambridge Analytica's controversial marketing techniques', Nature, 2018, https://www.nature.com/articles/d41586-018-03880-4.

100 See the discussion below in section 5(b) on the AVG.

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.

used to abuse people".[102] Indeed, some jurisdictions have introduced transparency rules on the use of bots to influence an election.[103] However, as Williams has noted, well-intentioned bot transparency proposals must be 'meticulously crafted', or otherwise, they may 'enable censorship and silence less powerful communities, threaten online anonymity, and result in the takedown of lawful human speech expression'.[104]

An example of problematic techniques is *astroturfing*, which involves using social media bots, fake accounts and paid trolls (or influencers) to 'amplify' campaign messages, which creates the 'appearance of grassroots support', with the aim to make a campaign appear popular with the public.[105] Indeed, *astroturfing* is designed to create the false impression that a campaign has developed *organically*.[106] Therefore, an important consideration when examining astroturfing or other types of deceptive political communication is whether election spending rules apply, as political parties and groups need to detail how money is spent on campaigning. A related question is arising whether astroturfing should be considered, and defined as such in relevant regulatory frameworks, as a form of political advertising. It does not involve payment to a technology company such as Facebook, and Twitter, but it may involve paying others to spread and amplify a political message using Facebook and Twitter.

Finally, another form of organic content is simply sending a political message *directly* to a particular individual, for example through a messaging service, such as WhatsApp, or Facebook Messenger. This may be part of a viral political campaign, including political crowdfunding.[107] Some internet services allow users to collect payments by other users, something that is quite popular in certain user-created content categories like gaming, creating new entanglements between online media and money.[108] Further, political messages can be sent directly through a messaging service using a fake account or false identity.

Given these methods of sponsored and organic content, the question arises as to which qualify as political advertising. Helpfully from a legal perspective, the European Court of Human Rights ("**ECtHR**") has considered the issue of *paid* political advertising in its case law.[109] While the ECtHR has not laid down a hard-and-fast definition, it instead takes a broad view of what constitutes paid political advertising, which not only includes paid advertisements from political parties seeking votes, but also paid advertisements from campaign groups on matters of public interest. Indeed, the ECtHR has emphasised the absence of a *paid-for* element when considering whether a publication was a political advertisement or ordinary journalist expression.

Thus, the crucial element is the paid-for aspect, and as such, sponsored and promoted content would seem to come within the ECtHR's view on paid political advertising. The more difficult question is how to view organic content, amplification and viral-campaign techniques, which may also involve money – whether to political campaign staff, bot software services, or more nefariously, to troll farm workers. Further, due to the lack of editorial control on communications by relevant internet services, the classic distinction between editorial and advertising content is harder to make. One could say that advertising is simply an additional way to reach audiences, with additional tools and efficiency. In other words, advertisement products of internet services allow users to buy additional exposure opportunities, on top of the opportunities for normal users of the service.

---

102 Idem.
103 See Country studies, part 1(e) - United States.
104 See 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 See 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 Such payments can become very problematic if they are caused by illegal and harmful statements and communications, such as *hate speech.*
109 See chapter 4, for an in-depth discussion.

E. Summary & Conclusion

Disinformation is a broad and complicated concept with many different definitions in circulation. However, all definitions include in some form that (i) the information is **false** or **misleading**, (ii) causes some type of **harm** and (iii) that **intent** with regard to either this harm or the counterfactual nature of the information should play a role. Finally, (iv) **economic profit** plays a significant role in most definitions. In following the definition of the European Commission, this report defines disinformation as:

> **Disinformation** is "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".[110]

One of the complicating aspects of the spread of disinformation is the many different possible actors involved. First, the different actors where the disinformation campaign might originate ranges from an individual, to a political party, all the way to state actors. Secondly, the channel through which the disinformation is spread, the internet service, plays an important part in how much impact disinformation might have. Thirdly, the general public functions both as receivers and intended audience of the disinformation as well as spreaders of the information by liking or sharing the particular content. Fourthly, the way traditional and editorial media respond to certain instances of disinformation might greatly influence its impact.

Implicit in all this is the major role played by different possible forms of socio-technical amplification of disinformation. In many instances the disinformation itself is not the core of the problem, but the large scale spread via relevant internet services, which typically do not impose editorial control. This socio-technical amplification of disinformation involves a variety of techniques and processes, including user activity (liking, sharing), data-driven targeting and the use of automated engagement through platforms (bots). The use of these technological and manipulative methods makes disinformation closely connected to the concept of online manipulation that can be defined as the use of information technology to covertly influence another person's decision-making, and online manipulative practices as applications of information technology that impose hidden influences on users, by targeting and exploiting their vulnerabilities.

Thus, disinformation cuts across many of the traditional legal fields and from the perspective on the content of the communications can involve harmful, unlawful as well as illegal content. It covers a wide range of different expressions that can fall into many different types of existing legal categories. As depicted in the image below, the broad range of different types of expressions that can contain disinformation can often be qualified with respect to an existing legal category such as slander or misleading advertisement, or fall within the category of harmful speech that is unregulated.

110 European Commission, '*Tackling online disinformation: a European Approach*', COM(2018) 236 final, par. 2.1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236.

Possible legal qualification of disinformation				
Regulated speech				free speech
Misleading advertising	Unlawful press publication	Direct messaging	Discrimination	Untrue news articles
Slander	Illegal commercial conduct	Hate speech	Unfair commercial practice	Conspiracy theories
Election fraud	Intellectual property	Illegal health claims		Hyper partisan speech
Types of expressions				
Personal	Commercial practices	News articles	Political	advertisement

Figure 1

Furthermore, disinformation as a phenomenon is usually not discussed in isolation, but in relation to a specific context. Most notably disinformation is discussed in relation to news, hate speech, commercial communication, foreign influence or political advertising. In each of these contexts, disinformation has its distinct logic and different actors are involved. For the purpose of this study it is important to note that the applicable legal framework shifts depending on the context disinformation is discussed in.

The general conclusion that can be drawn from this analysis of the concept of disinformation are firstly that the phenomenon is broad, containing a large number of types of expression and touching upon a broad range of actors. Consequently, giving a precise and clear definition is not always feasible. Notably with regard to the harm of disinformation, current definitions differ and contain relatively vague and open terms such as 'societal' or 'public' harm. Therefore, 'disinformation' should be regarded more as a policy area as opposed to a legal category. A second conclusion is that the concept of disinformation cuts right across many legal fields and encompasses a large group of otherwise unrelated existing legal categories. Notably, it also covers expressions that are currently unregulated and protected by the right to freedom of expression. Thirdly, the discussion on disinformation clearly shows how the problem and possible harm associated with disinformation is localized in the large scale and socio-technological spread of information. Finally, as the concept is so broad, involves many different actors, depends to a large extent individual behaviour (sharing, liking etc.) and the fact that the societal impact is not at every point clear, empirical research as to the spread and prevalence of disinformation in the Netherlands is necessary to properly assess the merits of possible policy options.

3. Legal status of relevant internet services (tech companies)

- Legal qualifications of Internet services that are relevant to disinformation are:
  - Information society services
  - Electronic communication services
  - Audiovisual media services
- Different company forms: (i) storage and dissemination services, (ii) networking, collaborative production and interconnection services, and (iii) selection, search and referral services.
- Distinction in enforcement modality according to:
  - The design of the specific service;
  - The policy of the service itself
  - Actual enforcement by the service.

The problem of disinformation arises in relation to a wide range of different Internet services. For example, disinformation may be spread via social media of a public or semi-public nature, but also via new communication services of a private nature, such as WhatsApp. Search engines also play an important role in the distribution and relative accessibility of information via the Internet, partly through sponsored results. In addition, there are online media platforms, such as YouTube, gamer-oriented media services such as Twitch, the recently popular TikTok mobile app, and discussion platforms such as Reddit and 4chan, which can play an important role in popularizing information and spreading disinformation. In the case of a specific focus on advertisements, advertising services are also important, in particular services that play a role in linking the supply of advertising space on websites and advertisers (advertising networks).

For the purpose of this study, given their lack of, or very limited, relevance to the issue of tackling disinformation, a number of Internet services are excluded. For example, it does not consider infrastructural services (such as cloud computing), domain name services, services for optimising the effective delivery of online content, cyber security services, operating system or browser software providers, or the producers of software and hardware relevant to the Internet.

A. Definition of relevant Internet services

From a legal point of view, the relevant internet services for the policy problems of disinformation are not easy to position. From the perspective of tackling disinformation and regulating political advertising, the relevant legal definitions of various internet services can be found at the European level. The following definitions are relevant:

- information society services. This includes services providers via the Internet, for example via a website or mobile application;
- electronic communication services;
- audiovisual media services.

All these services may also qualify as internet intermediaries, in particular as internet *hosting* or a *more conduit* service. Although there is relevant implementing legislation in the Netherlands, there are no relevant additional or different Dutch provisions with respect to these definitions. In addition to these legal definitions, policy frameworks for online platforms are being developed at European level. This is

a relatively elastic concept that does not yet have a clear legal framework but, depending on the specific definition that is used, it does include most of the internet services relevant to disinformation.

The e-Commerce Directive provides the leading legal framework for information society services.[111] This framework contains rules on the transparency of commercial communications, as well as the rules on the limitation of liability of internet intermediaries.[112] The latter is particularly important in view of the fact that many of the relevant internet services, due to the lack of editorial control, will be able (or at least want to) rely on the limitation of liability for internet hosting services. In addition, there are services, such as instant messaging services, which will be regarded as electronic communications services and as such are legally framed at European level in the telecommunications regulatory framework. Finally, the legal framework for audiovisual services also applies to certain disinformation-related Internet services such as YouTube.

B. Company forms and earning models

The core activity of Internet services that play a central role in the spread of disinformation is often that they offer third parties the opportunity to communicate. This quickly creates a company form that touches on the issue of liability and responsibility for illegal and harmful content and communication. In line with a recent study for the European Commission on this subject, the following services can be distinguished in this context, in three broad categories.[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.
4. **IaaS/PaaS:** Infrastructure as a Service and Platform as a Service cloud computing services.

111 Directive 2000/31/EC.
112 See sections 5.A and 6.A below.
113 See https://www.ivir.nl/publicaties/download/hosting_intermediary_services.pdf.

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 addition to this, as indicated above, communication services are relevant. Over-the-top services (OTTs) offered via the Internet in particular play an important role.

The revenue models of the above-mentioned Internet services vary and can best be classified by looking at these services from the perspective of multi-sided platform markets. A distinction can then be made between supply and demand side revenues, as well as possible revenues from advertisers. The generation of revenue through the provision of sponsored communication opportunities, whether or not through dedicated channels, is an important form of revenue for many of these services. There are also many internet services where there is no advertising at all, as is the case, for example, with most electronic communication services. On the other hand, there are other sources of income, such as income from payments by end-users.

C. Enforcement 'modalities' of Internet services

The actual ability of Internet services to deal with disinformation varies from one service to another. In general, it can be said that there will often be a lack of effective prior control and editing of the content. This is particularly the case with regard to the question of whether the information and communication disseminated by third parties through the service complies with the regulations and restrictions imposed by the service or applicable law. A similar lack of supervision can occur in the design and subsequent use of usage profiles (accounts). It should be noted that, in general, there is no mandatory use of identifying data when using Internet services. For this reason, it is fairly easy to create a whole range of accounts and to communicate and interact with content shared by others.

The lack of ex ante control does not, of course, mean that there are no opportunities for control and enforcement. A distinction can be made here between three different modalities of control. Firstly, the way in which the relevant service is designed, including any specific possibilities for distributing sponsored (political) communication, is important. When designing the service, one should certainly also consider the relevant user interfaces through which end users and advertisers can make use of the service. In the case of communication services, for example, the question arises as to how easy it is to further share infor-

mation, or how many people can be sent a message at the same time. In addition, a service can be set up in such a way that, for example, statements from users are enforced when using a particular service, which can promote the effective enforcement of certain rules (so-called 'regulation through design'). With regard to sponsored communication, there is nowadays a multitude of different possibilities (data and other analytical instruments) to target advertisements at specific groups of people. These possibilities are offered partly by the relevant Internet services themselves and partly by other service providers.

Secondly, the policy of the service itself is relevant, which will be imposed on users through guidelines and conditions of use. Such conditions generally impose a multitude of restrictions and conditions in relation to the content of communications, as well as on the use of the service. The influence of social responsibility, regulatory pressure and legal developments also lead to regular adjustments to the terms of use. The accessibility of the service for, and the conditions regarding the ability to display, political advertisements are currently mainly standardized in the Netherlands in this way.

It should be noted here that there are clear restrictions on the possibilities of distributing political advertisements via Internet services. Many relevant services, such as ad networking services, do not allow political advertising. Microsoft and, more recently, Twitter, for example, no longer allows paid political advertisements on their Internet services.[114] LinkedIn prohibits political advertising, including advertising that promotes a particular candidate or political standpoint in an election, or otherwise seeks to influence the outcome of an election. Reddit Inc. also does not allow paid political advertisements outside the United States.[115] The incentives that exist in the market to keep political communication advertising channels open are apparently relatively limited, given the sensitivities of such communication and the relatively limited market. For the time being, Facebook continues to maintain broad accessibility for political advertisements, while also opting not to apply fact checking to political advertisements.[116]

Without effective control and enforcement, the third form of control, there may, of course, be only a limited impact of this policy. It is possible that this control is carried out by the service itself. In the event that it concerns a legal restriction (in part), there may be supervision by third parties or the government. A great deal of use is made of *notice and action* processes, more informally via special buttons for users, and more formally in the case of legal procedures set up for this purpose (such as Notice and Takedown codes and in the case of the German NetzDG legislation).

Finally, with regard to possible unlawfulness or irregular use in relation to information and communication, the following forms of action can be distinguished. In addition to allowing or removing content, de-prioritisation via relevant ranking and recommendation mechanisms is of particular importance. These forms of control over information flows are becoming increasingly important in controlling the quality of information. In addition, most Internet services make use of the possibilities to impose access restrictions on specific users. Finally, a number of services involve the integration of and/or cooperation with so-called fact-checkers. With regard to the latter, it is important to consider the question of the effectiveness of these methods of monitoring disinformation. Social science research shows that because fact-checkers often come from ideologically and socially opposing groups, there can be a serious lack of trust on the

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 politcal 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.

part of the actual target group. This can cause the use of these to be ineffective or even counterproductive.[117]

D. Summary

A large number of different internet services are relevant to the possible regulation of political advertising. These different services can be considered on the basis of their legal qualification, company forms and business models or on the basis of the enforcement modalities available to a specific service. From a legal perspective, the following types of services are relevant: information society services, electronic communications services and audiovisual media services. The concept of *hosting service provider* in the E-Commerce Directive is also important in view of the fact that many of the relevant services are able to invoke this limitation of liability.

As regards the different forms of services, it is useful to distinguish between (i) storage and dissemination services, (ii) networking, collaborative production and interconnection services, and (iii) selection, search and referral services. The revenue models can be divided into services that generate income from the demand or supply side, via advertisers or payments by end users.

Finally, in order to ensure enforcement, the following three types of control should be considered for the Internet service: firstly, the design of the specific service; secondly, the (alleged) policy of the service itself; and thirdly, to what extent and how the service (effectively) maintains its final policy, for example with regard to restrictions on the content, the way in which it is used and the political advertisements.

117 See Harambam, J., *"De/Politicizing the Truth"*. Sociology, 2017/13(1), p. 73-92.

4. Freedom of expression

- Freedom of expression includes a positive obligation on the State to guarantee a pluralistic environment for public debate
- Regulation of disinformation merely on the basis that information is false or misleading, without additional requirements, is difficult to square with freedom of expression standards
- Paid political advertising is considered political speech under Article 10 ECHR
- Transparency is essential for the promotion and protection of human rights, including freedom of expression
- Regulatory frameworks for paid political advertising should ensure that the public is aware that the message is a paid political advertisement
- Key points of the chapter: positive obligations, extensive protection political

The right to freedom of expression is an essential component when considering any regulation of disinformation or political advertising, as freedom of political expression is one of the most cherished democratic values. The Dutch government therefore places this fundamental right at the centre of its policy to protect democracy against disinformation. The first principle of this policy is the constitutional values and fundamental rights, including freedom of expression and freedom of the press. The objective of this policy is 'to protect the stability and quality of our democratic legal order and our open society, including freedom of expression and of the press' ('*de stabiliteit en kwaliteit van onze democratische rechtsorde en onze open samenleving te beschermen, met inbegrip van de vrijheid van meningsuiting en pers.*').[118]

Importantly, the right to freedom of expression is not limited to just being a negative right exercised against government interferences with free expression. It also encompasses certain positive obligations (i.e. duties) on the State to guarantee the type of pluralistic environment needed for individuals to effectively exercise their freedom of expression.[119] In this section, the human-rights framework applicable to freedom of expression relevant for the discussion of the regulation of disinformation and political advertising is discussed. Specifically, relevant doctrine related to Article 10 ECHR and Article 11 of the EU Charter of Fundamental Rights are discussed in section 4(a) below. Section 4(b) discusses Article 7 of the Dutch Constitution.

A. Article 10 ECHR and Article 11 EU Charter

The right to freedom of expression is guaranteed under Article 10 of the European Convention on Human Rights ("**ECHR**"), and it is the ECtHR which is tasked with interpreting Article 10. The ECtHR has delivered a number of judgments concerning freedom of expression, false information, political advertising, online platforms, and information of foreign origin. These judgments can provide guidance on the applicable principles under Article 10 ECHR which would apply to any prospective regulation of disinformation or political advertising carried/facilitated by internet services.

Freedom of expression is also guaranteed under Article 11 of the EU Charter of Fundamental Rights (EU Charter), which is interpreted by the EU Court of Justice ("**CJEU**"). The EU Charter provides that the 'meaning and scope' of certain rights, including freedom of expression, 'shall be the same as those

118 Tweede Kamer, 2019-202, 30 821, nr. 91 Kamerbrief 'beleidsinzet bescherming democratie tegen desinformatie'.
119 See McGonagle, T., *'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.

laiddown' by the ECHR. However, the CJEU has not to date considered the issue of freedom of expression, false information or political advertising, and as such, the discussion below mainly concerns ECtHR case law.

i. State's positive obligations to guarantee pluralism

Under Article 10 ECHR, the ECtHR has emphasised that States have a positive obligation to 'create a favourable environment for participation in public debate by all the persons concerned'.[120] As McGonagle has noted, this obligation requires States to guarantee pluralism in the media ecosystem,[121] with the ECtHR emphasising that States even have an obligation to put in place an appropriate legislative and administrative framework to guarantee effective pluralism.[122] This is because there can be 'no democracy without pluralism', and States 'must be the ultimate guarantor of pluralism'.[123]

When disinformation becomes pervasive and widespread, this clearly undercuts the functioning of media in our democracies. In addition, it may harm fair representation in the public debate of certain voices and sources of reliable information. With respect to the regulation of political advertising, the need for positive measures is most clearly triggered by two aspects thereof. First, it may be necessary to regulate political advertising to prevent money from having undue and distorting effects on democratic debate and participation. The ECtHR has stressed the importance of ensuring that there is a plurality of voices in public debate on matters of societal interest and that everyone, including individuals and small campaign groups, can participate effectively in public debate.[124] Deep pockets should therefore not be allowed to dominate or distort public debate. Second, it may be possible that voluntary measures to restrict certain forms of political advertising, in particular when taken by dominant internet services, unduly restrict the ability of certain groups to communicate effectively, thereby also harming pluralism.[125] In the past, the ECtHR has found that a lack of procedural fairness and equality can give rise to a breach of Article 10 ECHR.[126]

Indeed, in its latest judgment on political advertising, discussed below, the ECtHR connected the issues of pluralism and political advertising regulation. The ECtHR accepted that where powerful financial groups obtain 'competitive advantages in the area of paid advertising', this may 'curtail a free and pluralist debate', and the State may have a positive obligation to intervene to guarantee effective pluralism.[127] Further, Member States of the Council of Europe have an additional duty under Protocol No. 1 ECHR to hold elections 'under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature',[128] including a duty on the State to adopt positive measures to 'secure pluralism of views' during elections.[129] It must be born in mind that the possibility of political advertising creates clear possibilities for distorting effects for the public debate. In the absence of editorial control, however, such effects also exist through the use of non-sponsored communications channels and associated optimization techniques.

120 Huseynova v. Azerbaijan (Application no. 10653/10) 13 April 2017, par. 120; and Dink v. Turkey (Application no. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09) 14 September 2010, par. 137.
121 McGonagle, T., *'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, paragraph 134.
123 Manole and Others v. Moldova (Application no. 13936/02) 19 September 2009, par. 95-99.
124 Steel and Morris v. the United Kingdom (Application no. 668416/01) 15 February 2005, par. 89. See also Dink v. Turkey, cited above.
125 See further: 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., par. 95.
127 Animal Defenders International v. the United Kingdom (Application no. 48876/08) 22 April 2013, par. 112.
128 Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, Article 3 ("The High Contracting Parties undertake to hold, at reasonable intervals, free and secret elections under conditions which ensure the free expression of the people when electing the legislature.").
129 Communist Party of Russia and Others v. Russia, no. 29400/05, 19 June 2012, par. 126.

ii. Freedom of expression and false or misleading information

At the outset, it should be noted that specific regulation of disinformation merely on the basis that information is false or misleading, without additional requirements, such as causing damage to someone's reputation or another person's rights, is difficult to square with freedom of expression. Under international freedom of expression standards it is clear that "[g]eneral prohibitions" on dissemination of "false news," or "non-objective information," are "incompatible with international standards for restrictions on freedom of expression," and "should be abolished."[130] This is also the unanimous view of all four special international mandates for protecting freedom of expression: the UN Special Rapporteur on Freedom of Opinion and Expression; the Organization for Security and Co-operation in Europe Representative on Freedom of the Media; the Organization of American States Special Rapporteur on Freedom of Expression; and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information.

Similarly, the U.N. Human Rights Committee has stated in no uncertain terms that prosecution "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] Regional human rights courts take the same position: the Inter-American Court of Human Rights has held that a "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," and "violates the right to information that this same society has."[132] The European Court of Human Rights has unanimously held a prosecution for "dissemination of false information" violated the right to freedom of expression, holding that "Article 10 of the Convention as such does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful."[133]

And yet, countries still maintain laws on false information, and laws which have been historically known as 'false news laws'. For example, in France, there is a prohibition on publication of "*nouvelles fausses*" ("false news") under its Freedom of the Press Law 1881.[134] As a result supreme courts and constitutional courts throughout the world have considered laws on false or misleading information, and have found various violations of freedom of expression, including the Supreme Court of Canada, Supreme Court of Zimbabwe, and Supreme Court of Uganda. The specific provisions at issue in the countries, as discussed below, bear a striking resemblance to current concepts of disinformation which are being put forward.

One of the leading judgments is that of the Supreme Court of Canada, which considered section 181 of the Criminal Code ("spreading false news"), which criminalised "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] The Court found that the law violated the right to freedom of expression, holding that the purpose of freedom of expression "extends to the protection of minority beliefs which the majority regard as wrong or false," and a law "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] Further, "[e]xaggeration - even clear falsification - may arguably serve useful social purposes linked to the values underlying freedom of expression."[137] Similarly, the Supreme Court of Zimbabwe has also unanimously

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 Concluding Observations of the Human Rights Committee: Cameroon, 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&Lang=en.
132 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.
133 Salov v. Ukraine (App. no. 65518/01), 6 September 2005.
134 Law of 29 July 1881 on freedom of the press, article 27, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722
135 R. v. Zundel, 27 August 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.

found that Zimbabwe's false information provision violated the right to freedom of expression.[138] The law criminalised "any false statement, rumour or report which is likely to cause fear, alarm or despondency among the public or any section of the publicś or is likely to disturb the public peace." The Court found that the law "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] Similarly, the Supreme Court of Uganda has considered section 50 of Uganda's Penal Code (publication of false news), which criminalised "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." The Court found that the law violated freedom of expression, finding that it "imposes an unacceptable chilling effect on the freedom of the press."[140] And in 2018, the Court of Justice of the Economic Community of West African States considered convictions under Gambia's false news law which made it a criminal offence for a person to publish a "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] The Court found that the provision "amounts to censorship on publication."[142]

The leading case on false expression from the US Supreme Court is *United States v. Alvarez*, where the Court found that a federal law which criminalised "falsely claim[ing] receipt of military decorations or medals" violated the right to freedom of speech.[143] The Court held that it "rejects the notion that false speech should be in a general category that is presumptively unprotected."[144] Further, "[p]ermitting the government to decree this speech to be a criminal offense" would "endorse government authority to compile a list of subjects about which false statements are punishable," and "[o]ur constitutional tradition stands against the idea that we need Oceania's Ministry of Truth."[145] The Court concluded that "[t]he remedy for speech that is false is speech that is true. This is the ordinary course in a free society."[146]

iii. Article 10 ECHR and broad definitions of disinformation

Under Article 10 ECHR, laws that interfere with freedom of expression must be formulated with 'sufficient precision', so that individuals can generally foresee the consequences of their actions.[147] Where legislation contains provisions that are too wide or vague, the ECtHR has found violations of Article 10 ECHR, as they may represent a continuing threat to freedom of expression. As such, when considering the possible regulation of disinformation, it may be helpful to explore the definition provided by the European Commission, in light of Article 10 ECHR. Of course, the European Commission's definition may not have been intended as a model definition for legislation, but examining its elements under freedom of expression standards may highlight any potential pitfalls in relation to possible regulation.

When considering the European Commission's definition of disinformation in the light of international freedom of expression standards mentioned above, there is an important observation that must be made. Remarkably, the definition bears a striking resemblance to the 'false news' laws mentioned above that have been considered by an array of supreme courts throughout the world. Four examples are included

138 Chavunduka and others v Minister of Home Affairs and another, 20 May 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 and Anor v Attorney General ((Constitutional Appeal No.2 of 2002)) [2004] UGSC 1 (10 February 2004), p. 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), b.r. 722.
145 United States v. Alvarez, 567 U.S. 709 (2012), b.r. 723.
146 United States v. Alvarez, 567 U.S. 709 (2012), b.r. 727.
147 Altuğ Taner Akçam v. Turkey (Application no. 27520/07) 25 October 2011, paragraph 87.

below from criminal codes where national supreme courts have found violations of freedom of expression, alongside the Commission's definition:

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).

Indeed, some of these definitions have stricter requirements that the European Commission's definition, such as requiring a "*likely*" disturbing of the peace, while the Commission's only requires that false information "*may*" cause public harm. And yet, these definitions of false information have been found to violate freedom of expression. As such, given the clear international freedom of expression standards mentioned above, and the similarity of the European Commission's definition of disinformation with false information laws held to violate freedom of expression, it is clear that any attempt to legislate for the prohibition of disinformation in the form of false or misleading information, would raise serious freedom of expression concerns.

At the time of its ruling, the Supreme Court of Canada remarked that when the Canadian government sought to justify the law on spreading false information, the government could point to "no other free and democratic country with criminal legislation of this type."[148] This has changed. Since 2016, countries such as Cameroon, Russa, Malaysia, Singapore, have been enacting new false and fake news laws with ominous titles like Malaysia's Anti-Fake News Act 2018, or Singapore's Protection from Online Falsehoods and Manipulation Act 2019; and have been criticised under international freedom of expression standards.[149] And many countries still criminalise publication of false information, such as Bahrain's Penal Code or the United Arab Emirates' Federal Law.[150]

In sum, broad, vague or catch-all terms should not be used as a basis for restricting freedom of expression. Reliance on such terms in the context of the regulation of expression runs the risk of overbroad or arbitrary interpretation and implementation of relevant regulation, which in turn has a chilling effect on freedom of expression and leads to self-censorship. Broad and vague terms which cover a range of different types of expression must be assessed in the light of the scope of the right to freedom of expression, as guaranteed by international human rights law and the limitations it permits and the prohibitions it prescribes.[151]

148 R. v. Zundel, 27 August 1992, 2 S.C.R. 731, www.canlii.org/en/ca/scc/doc/1992/1992canlii75/1992canlii75.html
149 See Article 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 Article 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 See Bahrain Penal Code, 1976, article 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, par. 46.

iv. Article 10 ECHR and public harm

Under Article 10(2) ECHR, since freedom of expression 'carries with it duties and responsibilities', it may be restricted, but only on the basis of a number of specially enumerated grounds, such as to protect a person's reputation or privacy, or 'prevention of disorder or crime', etc.[152] Thus, legislation like defamation laws restrict false information which may harm a person's reputation; or incitement to violence laws which are designed for the prevention of disorder.

However, in the European Commission's definition of disinformation, it includes false information which "may cause *public harm*," including "threats to democratic political and policymaking processes."[153] The question thus arises whether there would be a legitimate ground under Article 10 ECHR to regulate false information on the basis that it may cause *public harm*, as opposed to false information that may cause harm to reputation or may cause disorder.

Importantly, in *Perinçek v. Switzerland*, the ECtHR rejected the view that Article 10 ECHR included an exception for protecting a notion of "public order," such as where it is "taken to refer to the body of political, economic and moral principles essential to the maintenance of the social structure."[154] The Court held that the term "prevention of disorder" under Article 10 meant preventing "forms of public disturbance."[155] Indeed, in a 2019 judgment involving Russian government blocking of a social media post to protect "public order," the ECtHR found a violation of Article 10 ECHR, and said quite definitively that "neither Article 10 nor Article 11 allows for restrictions aimed at maintenance, or protection, of public order."[156]

Thus, under Article 10 ECHR, it would be quite problematic to prohibit false information merely on the basis that it may cause what is termed "public harm", and any regulation of disinformation would need to only be targeted at information on the basis of protecting other people's rights (e.g., reputation, privacy, dignity), or a legitimate government interest, such as prevention of disorder (e.g., public disturbance). A nebulous interest such as public harm would not seem to be covered under Article 10 ECHR. Rather than seeking to define new content-focused regulation of disinformation based on new and disputed forms of government interests, such as public harm, a more appropriate basis for tackling disinformation, and one grounded in human rights standards, would be the guaranteeing of media pluralism and an enabling environment for freedom of expression online.

v. Commercial expression

A particular feature of the European Commission's definition of disinformation is that it may consist merely of false or misleading information "disseminated for economic gain," and nothing more. This raises the question whether regulation could be framed targeting false information specifically disseminated for profit reasons, rather than say, public-interest reasons (although most European media organisations like publishers, newspapers, news websites, and broadcasters are for-profit companies). Importantly, the ECtHR has specifically held that Article 10 ECHR applies where the aim pursued is "profit-making," stating that the explicit wording of Article 10 guarantees freedom of expression to "everyone," and "[n]o distinction is made in it according to whether the aim pursued is profit-making or not".[157] Thus, engaging

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 European Commission, *'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), paragraph 146.

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

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

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

in freedom of expression for exclusively commercial or economic gain is protected under Article 10 ECHR. Thus, attempting to regulate false or misleading information on the basis that it is being disseminated for economic gain would be problematic under Article 10 ECHR, and legislating on this basis would be very difficult, given that most online news organisations are pursuing a profit-making aim. As such, attempting to narrow the definition of false or misleading information by focusing on a for-profit element would not cure all the problems described in the previous section, that regulation of false or misleading information, without more (like harm to reputation or causing disorder), are not compatible with international freedom of expression standards.

Of course, by focusing on the dissemination of false information for economic gain, the Commission is attempting to target the supposed problem of what are described as click-bait articles that peddle deliberate falsehoods, composed merely to maximise advertising revenue. Such articles may be problematic for public debate, but it would be quite difficult under Article 10 ECHR to formulate a sufficiently clear and narrowly-tailored law that would also not risk application to perfectly legitimate political expression. A more appropriate way may be to try to formulate laws that would try to target the distribution channels' ability to profit from spreading disinformation.

It may be argued that false or misleading information disseminated for economic gain could be construed as something akin to false or misleading commercial expression. Helpfully, the ECtHR has set out what it considers to be commercial expression: it is 'inciting the public to purchase a particular product',[158] or 'product marketing',[159] and commercial advertising is a 'means of discovering the characteristics of services and goods offered'.[160] In one of its latest judgment on commercial expression, the ECtHR reiterated that member states have a 'broad margin of appreciation in the regulation of speech in commercial matters or advertising'.[161] However, while advertising may sometimes be restricted, especially to prevent 'untruthful or misleading advertising', such restrictions must be 'closely scrutinised by the Court, which must weigh the requirements of those particular features against the advertising in question'.[162] Thus, attempting to regulate disinformation as akin misleading commercial expression would be difficult, as there would need to be product or service marketing involved; and even where speech is classified as commercial expression, the government can only restrict such expression on the basis of the framework under Article 10 ECHR, i.e. prescribed by law, pursue a legitimate aim, and necessary in a democratic society. While the government has a margin of appreciation to regulate commercial expression, it does not have free reign.

vi. Hate speech

In some of the literature on disinformation, the issue of hate speech is included as a distinct feature of disinformation campaigns, and research has noted that calculated amplification of hate speech is one of many tactics deployed in disinformation campaigns.[163] Indeed, EU officials have spoken in the same breath about how the twin problems of hate speech and disinformation are a major challenge for the EU.[164] It is therefore quite important to clearly set out the ECHR standards concerning hate speech, and it can also help inform our discussion of the importance of including specific *intent* and *harm* requirements where legislation seeks to target false information that may harm specific minority groups.

158 VgT Verein gegen Tierfabriken v. Switzerland (Application no. 24699/94) 28 June 2001, paragraph 57.
159 TV Vest As & Rogaland Pensjonistparti v. Norway (Application no. 21132/05) 11 December 2008, par. 64.
160 Casado Coca v. Spain (Application no. 15450/89) 24 February 1994, par. 51.
161 Sekmadienis Ltd. v. Lithuania (Application no. 69317/14) 30 January 2018, par. 73.
162 Casado Coca v. Spain (Application no. 15450/89) 24 February 1994, par. 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.

The ECtHR's development of its case law on hate speech has been at times somewhat unclear, and has raised issues of consistency.[165] However, the ECtHR has helpfully considered the issue of hate speech on social media recently.[166] Notably, the ECtHR unanimously confirmed that it adopts the approach under international freedom of expression standards that "essential" elements when determining whether an expression constitutes (illegal) incitement to hatred: (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. Thus, when the ECtHR reviewed a blogger's prosecution for inciting hatred, the Court unanimously concluded that there had been a violation of Article 10 ECHR, as there was no evidence that the comments were likely to provoke imminent unlawful actions, or "posed a clear and imminent danger". Notably, the ECtHR specifically warned that it is vitally important that criminal law provisions targeting hate speech "clearly and precisely define[s] the scope of relevant offences," and that the provisions be "strictly construed in order to avoid a situation where the State's discretion to prosecute for such offences becomes too broad and potentially subject to abuse through selective enforcement."[167]

Of course, the ECtHR is acutely aware that vulnerable minorities and groups that have a history of oppression or inequality, or face deep-rooted prejudices, hostility and discrimination, may, in principle, need a heightened protection from attacks committed by insult, holding up to ridicule or slander.[168] But any content-focused regulation seeking to target false information that stirs up, promotes or justifies violence, hatred or intolerance, must include the essential elements under Article 10 ECHR, including speaker's *intent* to incite discrimination, hostility or violence. Indeed, the ECtHR in another recent judgment "stresse[d]" that it is "vitally important" governments adopt a "cautious approach" when determining the scope of "hate speech" crimes and strictly construe the relevant legal provisions in order to avoid excessive interference under the guise of action taken against "hate speech".[169] Of course, a properly framed content-neutral regulation, which for example, required the provision of a reporting mechanism for users to report harmful (but not illegal) hate speech intersecting with disinformation, would pose less Article 10 concerns.

vii. Political advertising as a form of political speech

When considering political advertising and freedom of expression, the ECtHR has helpfully set out what it considers political advertising to be, although it has not laid down a specific definition. The ECtHR considers that paid-for political advertising is political speech under Article 10 ECHR. So, for example, a political party's television advertisement which urged viewers to vote for the party was speech 'indisputably of a political nature', and this was '[i]rrespective of the fact that it was presented as a paid advertisement'. Thus, the 'political nature of the advertisements' called for 'strict scrutiny' on the part of the Court, as there is 'little scope' for restrictions on 'political speech' under Article 10. Similarly, the ECtHR has considered that an animal rights association's television advertisement which urged viewers to eat less meat was a political advertisement, because it contained 'controversial opinions pertaining to modern society in general and also lying at the heart of various political debates', and 'fell outside the regular commercial context inciting the public to purchase a particular product'. The ECtHR held that the advertisement was 'political speech by the applicant association'. Finally, the ECtHR has stated that political advertising includes advertising on 'matters of broader public interest', where the political advertisement at issue was an animal rights association's television advertisement encouraging viewers to help stop the abuse of primates.

165 See: 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.
167 Ibid., par. 85.
168 Savva Terentyev v. Russia (Application no. 10692/09) 28 August 2018, par. 76.
169 Stomakhin v. Russia (Application no. 52273/07) 9 May 2018, par. 117.

Accordingly, the ECtHR takes a broad view of what constitutes political advertising, which not only includes advertisements from political parties seeking votes, but also advertisements on matters of public interest from campaign groups, also called issue ads in policy discussions. These political advertisements are considered political speech under Article 10, even though they are in the form of paid-for advertisements.

Notably, the ECtHR has found a violation of Article 10 ECHR where political advertising rules are used to restrict political expression where there is *no* paid-for element. This occurred in a 2017 judgment involving the fining of a Russian newspaper, where the Russian government argued that a partisan newspaper article during an election was in effect a political advertisement, and subject to campaigning rules. The ECtHR emphasised the lack of a 'paid-for' element as crucial, when it wholly rejected that the article was a political advertisement; and instead classed the article as 'ordinary journalistic work' during an election. Thus, focusing on the paid-for element of political advertising can also act as a bulwark against overzealous application of political advertising rules to political expression under Article 10 ECHR.

In sum, the ECtHR considers that paid-for political advertisements are political expression under Article 10 ECHR, and in contrast, commercial advertisements necessarily involve marketing goods and services, and can be subject to wider restrictions.

viii. The permissibility of prohibitions on political advertising

While the ECtHR treats political advertising as a form of political expression, it does not follow that restrictions may not be imposed on political advertising, where it is a content-neutral *general measure*, designed to protect effective pluralism and the democratic process. Indeed, the ECtHR has delivered contrasting judgments where it has found that bans on political advertising on television in Switzerland and Norway violated Article 10 ECHR, while in its latest judgment concerning a ban in the United Kingdom, the ECtHR found no violation of Article 10 ECHR.

The first case was *VgT v. Switzerland,*[170] where an animal rights association wanted to broadcast an advertisement showing a video clip of the life pigs are subjected to in factory farms. However, the Swiss Federal Radio and Television Act bans 'political advertising', and having failed in the Swiss courts to have the advertisement broadcast, the association asked the ECtHR to review whether there had been a violation of Article 10 ECHR.

The ECtHR reviewed the rationales put forward by the Swiss government for maintaining a political advertising ban, namely (a) preventing financially powerful groups distorting public debate, and (b) because the broadcast media is such an influential media, it may be subject to greater government regulation. However, the ECtHR concluded that while these rationales were relevant, 'general reasons' were not sufficient to justify application of the ban to a small animal rights group, which posed no threat of distorting public debate. The ECtHR therefore held that there had been a violation of Article 10 ECHR. Notably, the ECtHR did add that it 'cannot exclude' that a prohibition of '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]

The *VgT* judgment was not surprising, given the protection usually afforded to political expression under Article 10. A similar judgment was delivered in *TV Vest v. Norway*, where a Norwegian political party argued that a ban on political advertising on television, during the run-up to elections, violated its right to freedom of expression. The ECtHR found a violation of Article 10. The ECtHR recognised that there could be relevant reasons for a ban on political advertising, such as preventing the 'financially powerful' from

170 VgT Verein gegen Tierfabriken v. Switzerland (Application no. 24699/94) 28 June 2001.
171 Idem, par. 75.

obtaining an 'undesirable advantage' in public debates, and 'ensuring a level playing field in elections'. However, the ECtHR held that the political party at issue, a small pensioners' party, was 'hardly mentioned' in election television coverage, and paid advertising on television became 'the only way' for it to put its message to the public. Moreover, the party did not fall within the category of a party that the ban was designed to target, namely financially strong parties which might gain an 'unfair advantage'. Thus, the Court held that the general 'objectives' of the ban could not justify its application to the political party, and thereby violated its right to freedom of expression under Article 10.

However, in 2013, the ECtHR, sitting in a 17-judge Grand Chamber (due to the importance of the case), held in *Animal Defenders International v. UK* that a ban on paid political advertising on television in the UK did not violate Article 10 ECHR. For the first time under Article 10 ECHR, the ECtHR held that a certain type of regulation, which the Court called 'general measures', can be imposed 'consistently with the Convention', even where they 'result in individual hard cases' affecting freedom of expression. The Court laid down a new three-step test for determining whether a 'general measure' is consistent with Article 10: the Court must assess 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.

The Court then applied its general-measures test to the ban on political advertising on television in the UK: first, the Court examined the 'legislative choices' underlying the ban, and accepted that it was necessary to prevent the 'risk of distortion' of public debate by wealthy groups having unequal access to political advertising; and due to 'the immediate and powerful effect of the broadcast media'. Second, with regard to the quality of parliamentary review, the Court attached 'considerable weight' to the 'extensive pre-legislative consultation', referencing a number of parliamentary bodies which had examined the ban. Third, as regards the risks from relaxing a general measure, the Court held that it was 'reasonable' for the government to fear that a relaxed ban (such as financial caps on political advertising expenditure) was not feasible, given the 'risk of abuse' in the form of wealthy bodies 'with agendas' being 'fronted' by social advocacy groups, leading to uncertainty and litigation. Therefore, the Court held that the total ban on political TV advertising was consistent with Article 10.

It is not quite clear how the ECtHR would view the regulation of online political advertising from the differing conclusions in *VgT*, *TV Vest* and *Animal Defenders.* In particular, the ECtHR did draw a distinction in *Animal Defenders* between broadcasting and the internet. According to the ECtHR – in 2013 – the internet and social media did not have the same 'synchronicity or impact' as broadcasting, which had an 'immediate and powerful effect', including within the 'intimacy of the home'.[172] The ECtHR at the time said there was 'no evidence of a sufficiently serious shift' in the influences of new media to undermine the need for a political advertising ban in broadcasting.[173]

However, if *Animal Defenders* is treated as the leading judgment by the ECtHR in the future, regulation of online political advertising could be imposed, if four criteria are satisfied:

a. First, if it can be shown that regulation of online political advertising is necessary to prevent the *risk of distortion of public debate*, such as financially powerful groups having unequal access to online political advertising;
b. Second, if there is evidence of online political advertising having a sufficiently *immediate and powerful effect*;
c. Third, if there is *extensive pre-legislative consultation* on the regulation of online political advertising; and

172 Idem, par. 119. See also: Plaizier, C., '*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.
173 Idem.

d. Fourth, if there exists a *risk of abuse or arbitrariness* without the regulation, such as a risk of wealthy bodies with agendas being fronted by social advocacy groups created for that precise purpose; and the risk of financial caps on advertising being circumvented by those wealthy bodies creating a large number of similar interest groups.

Of course, the type of regulation at issue in the above cases was a *total prohibition* of paid political advertising. There are regulatory options less restrictive than total prohibitions, such as transparency rules, spending restrictions, or restrictions limited to election-time.

ix. Service providers and freedom of expression

Any regulation imposed on internet services in relation to third party communications and political advertising would need to be consistent with Article 10 ECHR. In this regard, the ECtHR has delivered judgments holding that service providers that operate online platforms and social media platforms have a right to freedom of expression. For example, the ECtHR confirmed in 2017 that Google Inc. itself enjoys a 'right to freedom of expression' under Article 10 ECHR,[174] which was distinct from its users' rights, given its 'role as the provider of a platform for the free exchange of information and ideas'.[175] Indeed, the ECtHR has highlighted how important online platforms are for freedom of expression, holding that YouTube was a 'unique platform' and an 'important means' for free expression, where 'political content ignored by the traditional media is often shared via YouTube'.[176] Similarly, other services operated by Google which "facilitate the creation and sharing of websites within a group" are also a "means of exercising freedom of expression".[177] Further, when discussing Instagram posts, the ECtHR reiterated the important role the Internet plays in "enhancing the public's access to news and facilitating the dissemination of information in general".[178]

As such, where technology companies provide a platform for the exchange of information and ideas, for others to impart and receive information, or the creation and sharing of information within a group, these companies enjoy a right to freedom of expression under Article 10. This is all premised on the notion that Article 10 guarantees freedom of expression to "everyone", and "[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] Indeed, the Court first established the principle nearly three decades ago, when it rejected the view that a for-profit corporation did not enjoy the protection of Article 10: it applies to 'everyone' and is 'applicable to profit-making corporate bodies'.[180]

x. Restricting the scale, extent and quantity of publication

One of the issues associated with internet services is the amplification of content, and its rapid dissemination. A possible regulatory intervention to target amplification could be rules that aim to restrict the scale, extent and quantity of dissemination. In this regard, the ECtHR has considered the question of whether the scale and quantity of publication of *lawful* information may be restricted. The leading case is the judgment in *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*,[181] where a newspaper published the names and income of over one million Finnish taxpayers, in alphabetical lists, organised by municipality and income bracket. The newspaper collected the information from the Finnish tax authorities, as it was publicly accessible under Finland's public disclosure law. In 2009, after six years of litigation, Finland's Data

174 Tamiz v. the United Kingdom (Application no. 3877/14) 19 September 2017 (dec.), par. 87 and 90.
175 Cengiz and Others v. Turkey (Application nos. 48226/10 and 14027/11) 1 December 2015, par. 52.
176 Ahmet Yıldırım v. Turkey (Application no. 3111/10) 18 December 2012, par. 49.
177 Einarsson v. Iceland (Application no. 24703/15) 7 November 2017, par. 46.
178 Einarsson v. Iceland (Application no. 24703/15) 7 November 2017, par. 46.
179 Kablis v. Russia (Application nos. 48310/16 and 59663/17) 30 April 2019, par. 80.
180 Autronic AG v. Switzerland (Application no. 12726/87) 22 May 1990, par. 47.
181 Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland (App. no. 931/13) 27 June 2017 (Grand Chamber).

Protection Board issued a decision, finding that while publishing taxation data was "not prohibited," the newspaper was prohibited from publishing the data "in the manner and to the extent" it did.[182]

When the case reached the ECtHR, it held that there had been no violation of the freedom of expression, even though the information at issue was "publicly accessible."[183] Crucially, the Court held that the publication was not disclosure of "information, opinions and ideas," but rather "disseminating *en masse* raw data in unaltered form." Because of its "layout," "form, content and the extent of the data disclosed," it did not "contribute to a debate of public interest," and was not "political speech." The Court noted that the publisher was "not prohibited from publishing taxation data," and although the limitations imposed on the "quantity of the information" to be published may have rendered their "business activities less profitable," this was "not, as such, a sanction within the meaning of the case-law of the Court."

It must be pointed out the dissemination at issue was not expression on a matter of public interest, and it is not clear how the ECtHR might approach a rule which imposed a restriction on the scale, extent and quantity of disinformation generally and political advertising specifically. But *Satakunnan* does suggest that it can be consistent with Article 10 to restrict the scale, extent and quantity of dissemination, even where the underlying content itself is lawful. This is an important starting point for regulating the spread of disinformation through internet services.

Further, the ECtHR has also considered the amplification of content by certain internet services. In the recent judgment of *M.L. and W.W. v. Germany*, the ECtHR held that search engines can have an 'amplifying effect on the dissemination of information', and because of the 'nature of the activity underlying the publication of information' on an individual, the '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] Thus, the ECtHR recognises how internet services, such as search engines, facilitate amplification, and due to the nature of their activity, their obligations may differ.

Importantly, in relation to requests for deletion of information from search results, the ECtHR empathised that the '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 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] Thus, the ECtHR does recognise a distinction between an internet service, such as a search engine, and the original publisher of information, whose activity it considers to be at the heart of freedom of expression.

xi. Transparency

Current discussions concerning disinformation and political advertising in particular, emphasize the need for 'transparency'. Importantly, The Council of Europe's Committee of Ministers has underscored the importance of media pluralism and diversity of media content as counterfoils against disinformation in its Recommendation CM/Rec(2018)1 to Member States on media pluralism and transparency of media ownership.[186] The Recommendation calls on States to "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:

182 Idem, par. 13.
183 Idem, par. 120.
184 M.L. and W.W. v. Germany (App. nos. 60798/10 and 65599/10) 28 June 2018, par. 97.
185 Idem.
186 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).

- 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]

The Recommendation also takes a clear stance on the importance of transparency regarding media content throughout the multi-media ecosystem:

"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]

The Recommendation goes on to develop a range of detailed transparency requirements for media ownership, organisation and financing. It also explores the synergies between transparency and media education and literacy.

In relation to political advertising in particular, it is important to note that there is a broad range of transparency rules under discussion, which may include rules on the recognizability of paid political advertisements as political advertisements, information on the person or group behind a paid political advertisement, information on expenditure on paid political advertisements, information on targeting criteria used in the dissemination of paid political advertisements, and requiring public repositories of paid political advertisements.[189]

The question arises whether and which type of transparency rules for paid political advertising would be consistent with freedom of expression. Transparency is essential for the promotion and protection of human rights, including freedom of expression,[190] and the ECtHR has long emphasised the 'right of the public to be properly informed'.[191] While the ECtHR has not directly ruled upon transparency rules for paid political advertising, the Council of Europe's Committee of Minsters has stressed the importance of transparency in paid political advertising, in various Recommendations to member states; which have been cited by the ECtHR.[192] For example, the 1999 Recommendation on media coverage of election campaigns recommended that regulatory frameworks for paid political advertising should ensure that the 'public is aware that the message is a paid political advertisement';[193] while the 2007 Recommendation states that

187 *Ibid*., par. 2.5.
188 *Ibid*., par. 2.7.
189 See: European Commission, '*Tackling online disinformation: a European Approach'*, COM(2018) 236 final, par. 3.1.1; 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.
190 See: UN Human Rights Committee, General comment No. 34, CCPR/C/GC/34, 12 September 2011, par. 1; Cannataci, A. e.a., '*Privacy, free expression and transparency*' UNESCO, 2016, https://unesdoc.unesco.org/ark:/48223/pf0000246610; and ; Voorhoof, D. *'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 Andreotti, O. (ed), '*Journalism at Risk: Threats, Challenges and Perspectives*', Council of Europe Publishing, 2015, p. 106.
191 See: The Sunday Times v. the United Kingdom (Application no. 6538/74) 26 April 1979, par. 66.
192 Animal Defenders International v. the United Kingdom (Application no. 48876/08) 22 April 2013, par. 73-75; Orlovskaya Iskra v. Russia (Application no. 42911/08) 21 February 2017, par. 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.

regulatory frameworks should ensure that paid political advertising is 'readily recognisable as such'.[194] In a similar vein, the Council of Europe's Venice Commission has recommended that regulation should require that paid political advertising 'be clearly labelled'.[195] The Venice Commission also recently adopted an important Report on digital technologies and elections, emphasizing the importance of '[a]ccountability of internet intermediaries in terms of transparency and access to data enhancing transparency of spending, specifically for political advertising'.[196] Also in the US, the Supreme Court has held that rules on the recognisability of paid political advertisements - called disclaimers - are consistent with freedom of speech. They "may burden the ability to speak, but they do not prevent anyone from speaking",[197] and instead "ensure that the voters are fully informed about the person or group who is speaking".[198]

Not only are transparency rules consistent with freedom of expression, there may actually be a duty on the government to enact transparency rules for paid political advertising in the narrow sense (election ads) in order to properly guarantee freedom of expression. Support for this can be found in international human rights standards, where the UN Special Rapporteur on the right to freedom of opinion and expression has stated, for instance, that States, in the electoral context, have an *obligation* to put in place measures to ensure that '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] This is because an 'informed political debate requires transparency, with respect to the conduct of political organizations, the financing and promotion of political campaigns',[200] and any regulatory framework for electoral processes 'must have as a key objective the achievement of transparency in all facets of political life and discourse'.[201]

Notably, these principles concern paid political advertising promoting political candidates or groups (election ads). Whether these principles should be applied to issue-based ads during and outside of election-time is an open question.[202] Clearly, transparency rules are not an easy catch-all formula to cure all the possible ills associated with paid political advertising. And moreover, there are difficult policy questions associated with each type of rule. For instance, requiring public repositories of paid political advertisements, sometimes called ad libraries, has raised a range of issues,[203] such as whether to place an obligation on those buying the ads to submit/flag ads for archiving, or instead an obligation on internet services to register all paid political advertisements.[204] This has even sometimes led to major internet services simply ending paid political advertising altogether in order to avoid the complexity of implementing ad libraries.[205]

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, par. I.6.

195 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.

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, 2019, p. 39, 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 v. 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'*, Human Rights Council, 2014, par. 82, https://undocs.org/A/HRC/26/30.

200 Idem, par. 5.

201 Idem, par. 61.

202 The imposition of transparency rules for *issue-based ads* outside election time also raises the question of whether it is possible to make anonymous statements, especially in small campaign groups. See for example 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 See: Leerssen, P. Ausloos, J., Zarouali, B., Helberger N. & de Vreese, C. '*Platform Ad Archives: Promises and Pitfalls',* 2019, https://ssrn.com/abstract=3380409.

204 It should be noted that the Directive on electronic commerce, discussed in section 5(a), prohibits Member States from imposing on certain service providers either a general obligation to monitor the information they transmit or store, or a general obligation to actively seek facts or circumstances indicating illegal activities.

205 See the country studies below, Part 1.

It follows from the above standards on freedom of expression that transparency rules for political advertising that are narrowly targeted and framed in a sufficiently clear manner, and are proportionate (i.e. 'prescribed by law' and 'necessary in a democratic society') are consistent with Article 10 ECHR. As mentioned above, well-intentioned proposals must be 'meticulously crafted', or otherwise, they may 'enable censorship and silence less powerful communities, threaten online anonymity, and result in the takedown of lawful' expression.[206]

xii. Foreign influence

In the current discussion on disinformation and political advertising, a particular issue has been disinformation from 'foreign governments',[207] and 'foreign actors'.[208] Indeed, the French government argued that the new French law on Manipulation of Information was needed due to the 'widespread and extremely rapid dissemination of fake news' through 'dissemination channels offered by social networks and media outlets influenced by foreign states'.[209] As such, an important consideration in this discussion is the compatibility of targeting information disseminated by foreign actors,[210] and Article 10 ECHR.

The right to freedom of expression exists, crucially and explicitly, *regardless of frontiers*. States may only restrict free, cross-border flows of information and expression in accordance with the strict limitations and prohibitions provided for by international and European human rights law. In its case-law on transfrontier broadcasting, the ECtHR has applied its standard test to ascertain whether bans on foreign broadcasts have amounted to violations of the right to freedom of expression, while also taking considerations of media pluralism into account, as relevant.[211]

International human rights law's traditional insistence on the importance of the cross-border dimension of freedom of expression takes on added importance in today's globalized communications environment. Nevertheless, fear of foreign influence in national politics has always animated discussions about the scope of freedom of expression. Such discussions tend to focus on how journalism, media and more recently social media, can contribute to such influence. The drafting of the European Convention on Human Rights, the International Covenant on Civil and Political Rights and the OSCE Commitments on freedom of expression and media freedom were clearly informed by fears of foreign influence and interference.[212]

For instance, during the drafting of the ICCPR, it was proposed to recognise that freedom of expression could be limited with regard to: "The systematic diffusion of deliberately false or distorted reports which undermine friendly relations between peoples and States".[213] While this proposed wording was ultimately not incorporated into the final text of Article 19, ICCPR, it indicates that concern about disinformation was very palpable. This concern was compounded by Cold War divisions and distrust and a political preoccupation with the dangers of propaganda for war and political ideologies.[214]

206 See Williams, J., *'Cavalier Bot Regulation and the First Amendment's Threat Model'*, Knight First Amendment Institute, 21 August 2019.
207 HLEG, *'A multi-dimensional approach to disinformation'*, p. 11.
208 European Commission, *Tackling online disinformation: a European Approach*, COM(2018) 236 final, par. 3.5.
209 Government Information Service,'Combating the manipulation of information', https://www.gouvernement.fr/en/combating-the-manipulation-of-information
210 See Wong S., Shepherd C., & Liu, Q., '*Old messages, new memes: Beijing's propaganda playbook on the Hong Kong protests'*, Financial Times, 2019.
211 See, for example, *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 For details, see: 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), pp. 1-51, at p. 16.
214 *Ibid*., pp. 12 *et seq*.

Under the ECHR, Article 10 guarantees the right to "receive and impart information and ideas without interference by public authority and *regardless of frontiers*". In this regard, the ECtHR has held that the right to freedom to receive information basically prohibits a Government from restricting a person from receiving information that others wish or may be willing to impart to him or her.[215] Thus, imposing a restriction on information from abroad is an interference with freedom of expression, such as the issue in *Association Akin v. France*, where the ECtHR considered a French law which permitted the banning of publications of 'foreign origin'.[216] The ECtHR found a ban imposed on a book's publication under the provision violated Article 10, and held that '[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]

However, this does not mean that restrictions may not be imposed on information from abroad, in particular information that does not make a legitimate contribution to the debate about matters of public concern and is meant to distort the democratic process; as long as the restriction satisfies the requirements under Article 10(2) ECHR that it is prescribed by law and necessary in a democratic society. In this regard, the Council of Europe's Committee of Ministers' Recommendation to member states on the free, transboundary flow of information on the Internet,[218] is particularly helpful. The Recommendation clarifies that member states are obliged to ensure that the blocking of content or services deemed illegal is in compliance with Article 10 ECHR; and measures adopted in order to combat illegal content or activities on the Internet should not result in an unnecessary and disproportionate impact beyond that State's borders. Further, States should strive to develop measures which are the least intrusive and least disruptive and implement them following a transparent and accountable process.[219]

Further, another policy option might be to impose spending restrictions on the dissemination of certain information, or purchasing of political advertising, especially from individuals or groups from aboard. The ECtHR has considered the issue of election spending restrictions in *Bowman v. the United Kingdom*.[220] The case concerned an activist who had distributed 25,000 leaflets in the run-up to an election, and had been prosecuted under a provision in election law which limited expenditure on publications 'promoting or procuring the election of a candidate' to only £5 for unauthorised persons i.e. non-candidates or parties.

The ECtHR first held that while the expenditure limit 'does not directly restrain freedom of expression', it nonetheless 'amounted to a restriction on freedom of expression'.[221] The ECtHR found the limit was a disproportionate restriction on freedom of expression, in violation of Article 10 ECHR. This was because the expenditure limit was 'set as low as £5', and the provision 'operated, for all practical purposes, as a total barrier to [the applicant] publishing information with a view to influencing the voters'.[222] The ECtHR was 'not satisfied' that it was necessary to limit expenditure to £5 in order to achieve the legitimate aim of securing equality between candidates.

The *Bowman* judgment thus confirms that restrictions on spending are an interference with freedom of expression, and must not operate as a complete barrier to publishing information during elections. Importantly, the ECtHR did state, as a matter of principle, that during election periods, it may be considered necessary to place certain restrictions, 'of a type which would not usually be acceptable', on freedom of

215 Khurshid Mustafa and Tarzibachi v. Sweden (Application no. 23883/06) 16 December 2008, par. 41.
216 Association Ekin v. France (App. no. 39288/98) 17 July 2001, par. 26.
217 Idem, par. 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, 2015, https://search.coe.int/cm/Pages/result_details.aspx? ObjectID=09000016805c3f20.
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, par. 33.
222 Idem, par. 47.

expression, in order to secure the 'free expression of the opinion of the people in the choice of the legislature'.[223] Thus, certain restrictions can be placed on freedom of expression under Article 10 ECHR during election time, which might not be appropriate outside of election time.

xiii. Election-time restrictions on false information

As discussed in the country studies, France has enacted a law which targets false information during election-time. The 2018 Law on Manipulation of Information provides that during the three months prior to an election, a court can order an online platform to remove '*des allégations ou imputations inexactes ou trompeuses d'un fait*' ('inaccurate or misleading allegations or imputations of fact"), which may "alter the sincerity of an upcoming vote', and are 'disseminated deliberately, artificially or automatedly', and on a massive scale.[224] Upon request for such an order, the court is required to deliver a decision within 48 hours of an application for removal being filed. It could be argued that such a provision is more narrowly-tailored than general prohibitions on false information, as the interest sought to be protected is the integrity of elections.

However, it is notable that the ECtHR has delivered three unanimous judgments concerning a provision under Polish election legislation, which allows election candidates to apply to a regional court for an order restraining publication of campaign material or statements containing 'untrue data or information', with the court required to examine the application 'within 24 hours'.[225] Notably, the ECtHR has found in all three judgments, including in a 2019 judgment, that various proceedings under this provision violated Article 10 ECHR.[226] For instance, in *Brzeziński v. Poland,* the Court unanimously found a violation of Article 10, as domestic courts had 'immediately classified as lies' statements made by a local politician during an election, and '[b]y following such an approach the domestic courts effectively deprived [the politician] of the protection afforded by Article 10'.[227] Further, in *Kwiecień v. Poland*, the Court found serious deficiencies under proceedings for 'untrue information' during an election, and even held that the 'fairness of the proceedings may be called into question'.[228] Similarly, in *Kita v. Poland*, the Court unanimously found a violation of Article 10 over 'untrue information' proceedings, holding that the courts 'unreservedly qualified all of [the statements] as statements which lacked any factual basis', and the 'standards applied' by the courts were 'not compatible with the principles embodied in Article 10'.[229] Therefore, in general it can be concluded from this that there are serious questions about the compatibility with Article of legislation which seeks to target untrue information, but which does not allow for examination of whether there has been harm to reputation, or candidates' personality rights.

B. The Dutch Constitution

In addition to the ECHR, the protection of freedom of expression is also laid down in Article 7 of the Dutch Constitution ("**GW**"). This Article does not protect the freedom of expression or reception as such, but it provides a specific protection against prior restraint (censorship) by public authorities. The provision makes a distinction between the protection it offers according to the medium in which the expression is made public. Article 7 GW protects 'thoughts and feelings' ('*gedachten en gevoelens*') expressed through: the printing press (paragraph 1), radio and television (paragraph 2) and all other media such as theatre, speech or dance (paragraph 3). Paragraph 4 completely excludes commercial advertising from protection.

223 Idem, par. 43.
224 Article 1 Act No. 2018-1202 of 22 December 2018 on combating the manipulation of information,, 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 http://merlin.obs.coe.int/iris/2019/2/article11.en.html
225 See Brzeziński v. Poland (Application no. 47542/07) 25 July 2019, par. 28.
226 See 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, par. 58.
228 Kwiecień v. Poland (Application no. 51744/99) 9 January 2007, par. 55.
229 Kita v. Poland (Application no. 57659/00) 8 July 2008, par. 51.

In the current Dutch case law, European case law based on the ECHR is mainly followed, and the Constitution often lacks application. What is still interesting for the regulation of disinformation and an understanding of the changed context in which governments find themselves with regard to new means of dissemination on the Internet, is the 'doctrine of dissemination' ('*verspreidingsleer'*). On the basis of this doctrine, the distribution of writings in the public domain can be regulated at a decentralized level. It has been fully developed in case law, with the explicit aim of making this standard possible at the municipal level.[230] Local regulation is considered necessary to maintain public order.[231]

In its core, the doctrine of dissemination comes down to the following. In order to make decentralised regulation constitutionally possible, a fundamental distinction is made in the doctrine between the freedom of disclosure, on the one hand, and the freedom to disseminate, on the other. Whereas the freedom of the press in Article 7 paragraph 1 of the GW explicitly protects the freedom of disclosure, the freedom of distribution as a connected right is read in with the freedom of disclosure. Bearing in mind the aim is to find the difference between the 'main right' of the freedom of disclosure and the 'derived right' of distribution logically in the restriction possibilities: revelation itself can only be limited by formal law, but also by material law.

The wording "in accordance with the law" of the right of disclosure in the first paragraph of Article 7 means that the right of disclosure can only be limited by a formal law. On the other hand, the related right of distribution can be restricted by a law in the material sense, since it is separate from the right of disclosure and thus from the wording of Article 7 of the Judicial Code. The time, place and method of distribution can therefore be standardised in lower regulations.[232] It is relevant to emphasise on this point that, unlike Article 10 of the ECHR, this freedom of disclosure under Article 7 of the Civil Code can be limited unlimited as long as it takes place in a formal sense by means of the law.

The *APV Tilburg*[233] judgment of 1950 provides the criteria, which are still valid as standard, on the basis of which this connection right of distribution may be restricted at the local level: (i) the restrictions must not relate to the content of the advertisement; (ii) a means of dissemination with independent meaning must not be generally prohibited; and (iii) the restriction must leave a use of some significance.

This first requirement ensures the separation between the right of dissemination and the right of disclosure by separating restrictions on the right of dissemination from the right of disclosure. The local authority can set a standard for the "time, place or mode" of distribution, as long as this does not affect or is done on the basis of substantive considerations. The second criterion prevents certain methods of disseminating information in the public domain from being completely prohibited. This was further specified in the *Eindhoven I* judgment,[234] where a ban on leaflets was declared ineffective because it is a means of distribution that "has independent significance and can meet a certain need with a view to such distribution". Other examples are posters, the distribution of bibles and the placing of letters on a building.[235]

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. and others, "*Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief*, Amsterdam: Cramwinckel 2000 p. 112; R.E. de Winter, De heersende leer: honderd jaar verspreidingsjurisprudentie: 1892-1992, The Hague: SDU 1993 p. 18.

232 See the standard judgment HR 28 November 1950, NJ 1951, 137 (APV Tilburg); J.M. De Meij and others, 'Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief', Amsterdam: Cramwinckel 2000 p. 113; De Winter, R.E., De heersende leer: honderd jaar verspreidingsjurisprudentie: 1892-1992, The Hague: 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 February 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. et al., 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, pp. 136-139.

The third criterion ensures that each means of dissemination is actually used in a meaningful way. In the *Nuth*[236] judgment, this additional criterion was developed to prevent the guarantees from being circumvented by not completely prohibiting an independent spreading agent, but by making it effectively unusable. These last two criteria are now replaced by the proportionality and subsidiarity tests of Article 10(2) of the ECHR.[237]

The doctrine of dissemination applies without question to political advertisements in the physical public space. The distribution of political posters, posters and flyers is regularly regulated at municipal level. However, it is uncertain whether the dissemination of political advertisements and misinformation by Internet services can also be limited by the doctrine of dissemination.

In the past, the doctrine was only applied in the *physical* public space and it is unclear to what extent it also applies in an *online* context. Questions such as what should be seen as an 'online' independent means of dissemination, how to explain restrictions on 'time and place', and whether in a digital environment the distinction between disclosure and dissemination as such can be made, remain unanswered. The easiest way to propose time restrictions is to fit in with the existence of temporary measures, while restrictions in the sense of different parts of the day are more difficult to propose. The delineation of measures by location then raises even more questions, since case law explicitly assumes a physical location. Perhaps instead of defining a 'place' on the internet, the underlying legal entities or the specific service that are offered for the delineation of a measure will be looked at.

Subsequently, the application of distribution theory in an online environment also raises questions regarding the use of municipal powers. How, for example, can a municipality on the Internet remain within its territorial jurisdiction and when there is a threat to public order in a digital context, concrete enough to take action? Regardless of the tension this would create with Article 10 of the ECHR and European law on Internet services, it is, of course, possible to abandon regulation at local level and to formally regulate the online distribution of disinformation at national level by law in the formal sense. When a law is used in a formal sense, Article 7 GW does not restrict the content or scope of the restriction and the doctrine of dissemination does not formally apply. The standards developed in the case law of this Dutch doctrine can of course serve as a guideline for the development of such legislation, also in the context of the subsidiarity and proportionality requirements of Article 10 of the ECHR. Although the legal doctrine with regard to Article 7 of the GW therefore offers a number of relevant insights, it ultimately provides few answers with regard to the problems at hand.

C. Summary/conclusion

This chapter has discussed relevant aspects of the freedom of expression framework for the regulation of disinformation and political advertising. A number of key points can be summarised here. The right to freedom of expression is not simply a right exercised against the government; it also involves positive obligations on the government to guarantee a pluralistic environment for public debate by all elements of democratic society. These obligations include that the government has a duty to ensure that pluralistic democratic debate is not distorted; and that financially-powerful groups do not obtain competitive advantages (such as through paid political advertising), which may curtail a free and pluralist political debate.

The chapter then considered various aspects of disinformation, and suggested that specific regulation of disinformation merely on the basis that information is false or misleading, without additional

236 HR 17 March 1953, *NJ* 1953, 389 (*Nuth).*
237 Dommering, E.J., *'De nieuwe Nederlandse Constitutie en de informatietechnologie',* Computerrecht, 2000, nr. 4, pp. 182 - 183.

requirements, such as causing damage to someone's reputation or another person's rights, is difficult to square with freedom of expression standards. Further, it would be quite problematic to prohibit false information merely on the basis that it may cause what is term public harm; and attempting to regulate false or misleading information on the basis that it is being disseminated for economic gain would also be problematic under Article 10 ECHR. Any content-focused regulation of disinformation would need to only be targeted at information on the basis of protecting other people's rights (e.g., reputation, privacy, dignity), or a legitimate government interest, such as prevention of disorder (e.g., public disturbance).

Crucially, paid political advertising in particular, is considered political speech under Article 10 ECHR. In addition, the ECtHR takes a broad view of what constitutes political advertising. It not only includes advertisements from political parties seeking votes (election ads), but also advertisements on matters of public interest (issue ads). While political advertising is a form of protect political expression, regulation of political advertising may be compatible with Article 10 in certain limited situations; but the reasons must be relevant and sufficient in respect of the particular interference with the rights under Article 10. The ECtHR will carefully scrutinise national legislative frameworks to ensure that political advertising laws are not used excessively to stifle journalistic coverage of a political debate, or a campaign group's right to engage in political expression. Further, it is also clear that service providers themselves enjoy a distinct right to freedom of expression. This is based on their crucial role as platforms for the free exchange of information and ideas, enhancing the public's access to news, and facilitating the dissemination of information in general. The ECtHR is cognisant of how internet services facilitate amplification of content, and due to the nature of their activity, their obligations may differ.

The chapter also laid out the importance attached to the principle of transparency, as essential for the promotion and protection of freedom of expression. Transparency rules for political advertising are consistent with Article 10 ECHR, where they are narrowly targeted (i.e. least restrictive), framed in a sufficiently clear manner, and proportionate. Indeed, in the particular context of election-time, there may be a duty on the government to implement transparency measures on paid political advertising during elections. However, any such measures must be narrowly-tailored to avoid the risk of (self-)censorship, prevent negative impacts on participation and representation of minority groups, undue restrictions on online anonymity, or result in removal of lawful political expression. Finally, the freedom of expression framework applicable to restriction on foreign influence was explored, including the limited-scope for imposing restrictions on information from abroad; and restrictions on spending affecting freedom of expression during elections.

It can be suggested that in order to tackle disinformation consistent with freedom of expression, it is necessary to begin from the premise that the State has a positive obligation to guarantee pluralism and the democratic process. An appropriate mechanism for intervention in this regard would be what the ECtHR calls general measures, which apply to pre-defined situations, and as such, as not content-focused, nor a prior restraint imposed on an individual act of expression.

5. European regulatory framework

- The EU framework includes the ECD, the AVMSD, Direct Marketing regulation, Commercial Regulation, the GDPR, and self-regulation;
- The actual regulation applicable depends on the type of internet service, content of the disinformation and the context in which it is spread (e.g. commercial, political, private);
- It is a very dynamic field of law. Many elements of the relevant European regulatory framework are either of a recent date (GDPR and AVMSD) or currently under revision (e-Privacy Regualtion and the ECD).
- Internet services themselves are also actively creating policies to address disinformation.

This chapter and the next discuss the relevant regulatory framework for disinformation in the Netherlands. This chapter focusses specifically on the relevant European Union law while the next, Chapter 6, will focus on law and regulations at the national level.

It is important to note that the internet services under consideration offer different and distinct services, from the perspective of EU law. For example, as discussed below, YouTube, as a video-sharing platform, may be subject to EU audiovisual media services rules; WhatsApp, as an electronic communication service, may be subject to the EU telecommunications rules or direct marketing rules; while Google Search, as a search engine,[238] may be subject to EU e-Commerce rules for information society services. As such, this section runs through a number of relevant EU instruments, and how they relate to the distinct services offered.

A. E-Commerce Directive

The tackling of disinformation and the regulation of internet services concerning political advertising has to be consistent with the E-Commerce Directive (“**ECD**”), which includes rules on the imposition of monitoring obligations, and liability exemptions for certain service providers.[239] First, the ECD contains conditional liability exemptions, or ‘safe harbours’, for three types of intermediary service activities: mere conduit (Article 12), caching (Article 13), and hosting (Article 14). Importantly, Article 15 ECD provides that EU member states are prohibited from imposing a general obligation on service providers that qualify under Article 12-14 to monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity.

A first question that would thus arise is whether the particular service, including its advertising service, would be able to invoke the protections offered by one of these provisions. In this regard, the services under consideration in this Report tentatively map to Article 14 (online media platforms, social media, and search engines) and Article 12 (communications services). It should be noted at the outset here that the scope of the safe harbour provisions has been the subject of litigation in the Member States and at the European level and is heavily debated.[240] The European Commission is currently preparing proposals

238 See also the recently adopted Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of on-line intermediation services, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:3201 9R1150&from=EN#d1e563-57-1, which sets out new transparency rules for search engines on the main parameters determining ranking.

239 See Van Hoboken, J. 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’,* 2018, https://www.ivir.nl/publicaties/download/hosting_intermediary_services.pdf. See also, Joris van Hoboken and Daphne 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.

240 For a discussion of the scope of Article 14 of the EC Treaty, see idem.

to amend these provisions of the ECD through a proposal for a Digital Services Act and the need for clarification on the scope of the safe harbour framework is an important aspect of this important revision.[241] Within a Dutch context, these articles 12 to 14 ECD are codified, without any important deviations from the directive, in article 6:196 of the Dutch Civil Code. The government judged that article 15 ECD was not in need of a codification of Dutch law as it consists of a duty of care directed at the Dutch state to which it is already bound by means of the directive itself.[242]

Currently, in terms of application to disinformation carried by or facilitated by internet services, the safe harbour framework of the ECD is relevant in two respects. First, in terms of the liability of service providers for illegal or unlawful content or activity. Second, on the types of obligations that can placed on service providers to monitor their service activity that qualifies for protection under Article 14 and 15 ECD. Addressing lack of clarity on the scope of these provision has been placed on the legislative agenda of the new European Commission.

Under Article 14 ECD on hosting, where an 'information society service' consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service. Importantly, this exemption only applies where the service provider does not have actual knowledge of illegal activity or information, or upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

The case law of the CJEU has further specified that in order to invoke Article 14 ECD, a service's activity needs to be 'neutral' and 'passive' and it should not have 'played an active role of such a kind as to give it knowledge of, or control over, the data stored'.[243] Notably, in relation to search engines, the CJEU has not excluded search engines from the scope of Article 14 ECD, and has concluded that advertising features of a search engine can be covered (Google Search).[244] In conclusion, depending on the particularities of the service, paid advertising service activity of relevant service providers may be covered by Article 14 and 15 ECD in view of the possibility of allegedly illegal and harmful content distributed through their services by advertisers.

This means that, in such cases, any obligations under Dutch law that would amount to a de facto general obligation to monitor, would be violating European law. On the other hand, Article 14 ECD does not affect the possibility for a court of requiring the service provider to terminate or prevent an unlawful communication, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

A new approach that has started to emerge in new measures and proposals with respect to the liability and responsibility of internet services, is to require service providers to make disclosures with respect to their efforts to address illegal and harmful content on their services and the risks that their service activity has in view of the possibility of illegal and/or harmful information and ideas. Such disclosures can be combined with oversight, thereby opening up new space for effective rule-making in relation to internet services, in the otherwise heavily contested issue of third-party liability for illegal content online.[245]

Another perspective on the liability framework concerns the much-heard criticism that the framework incentivises hosting providers to overly focusses on the removal of unlawful or illegal user generated

241 Bjarke Smith-Meyer, Lili Bayer and Jakob Hanke, 'EU officials float €100B boost for European companies', Politico 25 august 20109, full document: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/08/clean_definite2.pdf, p. 24

242 Lower House of Parliament, session year 2001-2002, 28 197, no. 3, p. 27.

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

244 Idem, p. 12.

245 The German NetzDG, the British White Paper and a recent report by the French government contain elements in this direction.

content, neglecting the protection of legal speech. The fact that hosting providers can escape liability and enjoy protection by the safe harbour when they "expeditiously"[246] remove content after they gained knowledge of the (alleged) unlawful or illegal nature of the content, means it is rewarding for hosting providers to remove content without much scrutiny. It follows that the safe harbour framework incentivises hosting providers to remove lawful content as soon as there are any doubts as to its legality or lawfulness. The criticism is that this system insufficiently protects the freedom of speech of the users whose content is removed, and threatens controversial or fringe speech.[247]

In addition to the liability framework for internet intermediaries,[248] the E-Commerce Directive also provides for a number of important rules specific to advertising. Of particular importance are the information requirements from Article 6 of the Directive, which was implemented almost immediately in Article 3:15e of the Civil Code.[249] Although the Directive imposes a number of general information requirements on service providers, Article 6 specifically covers "commercial communications", which should also include advertising. The obligation applies only to commercial advertising when it forms part of an 'information society service', which by definition is provided only by electronic means such as the Internet or radio.[250]

The provision stipulates that commercial advertising on the Internet must be recognisable as such. The advertiser must be clearly identifiable and the conditions for any offers must be clear. Spam via 'electronic mail' should also be recognisable as such as soon as it is received, and therefore before the e-mail is opened.[251] It appears from Dutch case law that the information necessary for identification does not have to be included in the advertisement itself. It is sufficient that 'clear and recognisable' reference is made to where the data can be found.[252]

The active enforcement of these and other transparency provisions prescribed by the Directive is carried out on the basis of Article 3:15f(3) of the Civil Code by the auditors of the FIOD (Fiscale Inlichtingen- en Opsporingsdienst – Economische Controle dienst).[253] These auditors have the authority to initiate a collective action on the basis of 3:305a BW. This was considered necessary because damage is difficult to detect in an individual case, and a collective context is more suitable for this purpose.[254] In addition, the transparency obligations have also been identified as a violation of Section 2(4) of the Economic Offences Act (*Wet op de economische delicten*), and the provisions can also be enforced by virtue of this Act. The effective monitoring of this provision is underdeveloped and in the corridors it is considered to be a somewhat forgotten provision.

B. General Data Protection Regulation

The use of personal data has seen a significant increase in the communications landscape. As mentioned in Chapter 2, in connection with disinformation, political advertising carried or facilitated by service providers may involve the collection and use of personal data in order to steer the distribution of relevant sponsored messaging. Relevant internet services, such as Facebook or Google's advertising properties,

246 Article 14(1) Directive 2000/31/EC.
247 Keller, D. (2018), "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; Angelopoulos, C., Brody, A., e.a. (2015) '*Study of fundamental rights limitations for online enforcement through selfregulation*', Institute for Information Law. available at: https://www.ivir.nl/publicaties/download/1796.
248 Section 5.A, implemented in Section 6:196c of the Netherlands Civil Code.
249 Where the text of the directive has not been reproduced verbatim, the wording does appear in the explanatory memorandum. The article will in any case have to be interpreted in accordance with the directive. See Schaub, M.Y., *Groene Serie Vermogrecht,* article 3:15e Civil Code, note 4.3.
250 Article 3:15d(3) of the Civil Code; Article 1(a) of Directive (EU) 2015/1535.
251 Parliamentary Papers II 2001-2002, 28 197, no. 3, p. 19-20 and 43.
252 Rb Rotterdam, 25 February 2010, ECLI:NL:RBROT:2010:BL6368 with reference to *Parliamentary Papers II* 2001-2002, 28 197, no. 3, p. 42.
253 See Section 15f, paragraph 3, Book 3 of the Civil Code in conjunction with Section 1, subsection 4 of the Economic Offences Act.
254 House of Representatives, session year 2001-2002, 28 197, no. 3, p. 8-9.

construct highly granular and data-driven possibilities for targeted communications with internet audiences. This implies that the General Data Protection Regulation ("**GDPR**") is highly relevant in this context as it applies to the processing of personal data and requires that any such processing is fair, lawful, and transparent, respects data subject rights and is made subject to independent oversight. Independent data protection authorities have started to take note of the practices in the field and played a leading role in investigating problematic practices with respect to political advertising, such as in the case of Cambridge Analytica and Facebook.

The European Data Protection Board ("**EDPB**") has adopted guidance on the use of personal data in the course of political campaigns, as have a number of national data protection authorities (Belgium, France, Ireland, Poland, and UK).[255] In relation to online political microtargeting, the European Data Protection Board has stated that "adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it and how they can exercise their rights as data subjects".[256] The Dutch data protection agency, the "Autoriteit Persoonsgegevens", has in February 2019 started a research into the use of personal data in the context of political campaigns.[257] The research focusses especially on the use of third parties that assist the political parties with their election campaigns.

The GDPR's broad applicability, its wide aims to protect the fundamental rights and freedoms of individuals in the context of the processing of personal data and its relatively open provisions that have to be interpreted and applied to different contexts, allow it to play a significant role in protecting the rights and freedoms of internet users. In relation to disinformation campaigns, the GDPR could be an important general safeguard in protecting against disproportionate processing of personal data. Whereas under U.S. law, platforms are free to leverage the information they have on their audiences, combined with information of data brokers and other third parties, to construct opportunities to influence people, European law requires the use of personal data for such operations to be lawful, fair and transparent. For instance, whereas the publication of factually false information may not be unlawful itself, the probing of audiences with targeted false messaging would lack a lawful basis under the GDPR. It is important to note, in this regard, that the personal data related practices of relevant services are the subject of litigation and investigations. Questions about compliance can also certainly be raised about the broad variety of practices related to the collection of audience metrics, insights and their application in different types of communications campaigns.

The GDPR contains a special more restrictive regime for the processing of sensitive categories of personal data that is relevant for targeted political advertising. Under Article 9 GDPR, personal data revealing political opinions is a special category of data under the GDPR. As a general principle, the processing of such data is prohibited and is subject to a number of narrowly-interpreted exceptions, such as the explicit, specific, fully informed, and freely given consent of the individuals. Notably, the GDPR also contains a further exception for political parties:

255 See 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. See also Annex 1 of the DPA guidance: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections-annexi_en.pdf.

256 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.

257 Personal Data Authority *'Exploratory research into the use of personal data in election campaigns',* 2019, https://autoriteitpersoonsgegevens.nl/nl/nieuws/verkennend-onderzoek-naar-gebruik-persoonsgegevens-verkiezingscampagnes

> '[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' (emphasis added).

Thus, political parties may process personal data revealing political opinions, but only relating solely to their members or former members, or people who have regular contact with the party. But this processing must have appropriate safeguards, and as Recital 56 GDPR provides, "[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".[258]

Notably, France, as discussed below, has imposed specific obligations on certain service providers (during election-time) to provide information to users on the use of personal data in the context of the promotion of content 'related to a debate of general interest'.[259] Thus, promoted and sponsored content on a debate of general interest must include clear and transparent information on the use of personal data for that content.

In sum, due to the fact that online communications and (political) advertising tend to involve the processing of personal data, the European data protection framework provides for relevant provisions that can empower internet users, offer minimum levels of transparency with respect to the data-driven aspects of the distribution of political advertisements, and create an avenue for enforcement and oversight by independent regulatory authorities in the Member States. Currently, the data protection framework is in the process of being more fully enforced with respect to relevant internet services. Such effective enforcement would constitute an important safeguard to protect people against manipulative practices that involve the processing of personal data.

Finally, the European Data Protection Supervisor (EDPS) has also published an *Opinion on online manipulation and personal data*.[260] It was prompted by how the digital information ecosystem is impacting the political economy, and how "deliberate disinformation ('fake news') has been propagated via this system", including through online manipulation. In this regard, the EDPS considers online manipulation to involve a three-stage cycle from data collection through profiling to microtargeting or personalisation as a form of manipulation which can vary in degree from trivial to seriously harmful.[261] The first stage, data collection, is where personal data are collected from a variety of sources using different dataset merging techniques, and most data is observed or recorded automatically, ('digital breadcrumbs') and deposited unwittingly as a result of individuals' online and offline activities.[262] Second, profiling, which occurs where the collected data is examined to segment people according to precise profiles. And third, microtargeting and manipulation. Microtargeting is where decisions, based on profiling, personalise an individual's informational environment with a high degree of personalisation. These microtargeting activities lead to a "culture of manipulation" in the online environment, where manipulation takes the form of microtargeted, managed content display which is presented as being most 'relevant' for the individual

258 General Data Protection Regulation (EU) 2016/679 [2016] OJ L 119/1.
259 Article 1 Act No. 2018-1202 of 22 December 2018 on combating the manipulation of information, https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte
260 European Data Protection Supervisor, *'EDPS Opinion on online manipulation and personal data, Opinion 3/2018'*, 19 March 2018, p. 7, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.
261 European Data Protection Supervisor, *'EDPS Opinion on online manipulation and personal data, Opinion 3/2018'*, 19 March 2018, p. 7, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.
262 Idem. p. 7.

but which is determined in order to maximise revenue for the platform. The EDPS links manipulation with the intention behind the design of devices and software has been to "induce addictive behaviour", with features such as auto-play, endless newsfeeds, notifications and 'streaks', which are "deliberate attempts to maximise attention" through microtargeting towards users, (similar to techniques used by the gambling industry).[263]

The EDPS has a number of recommendations on tackling on online manipulation, although it is recognised that no single regulatory approach will be sufficient on its own. These include (a) rigorously enforcing current data protection law - reinforce protection of special categories of data, the principles of transparency, purpose limitation and data minimization, and safeguards against unlawful profiling; (b) regulators should aim for a collective diagnosis of the problem, such what extent political movements engage in profiling and targeting of individuals, what sources of personal data they rely on and what tools they employ to profile and target them; (c) regulators should cooperate across sectors, as responses to 'fake news' need to be supported through more interagency cooperation e.g. cooperation between data protection and consumer protection regulators could potentially investigate the underlying ecosystem which facilitates political microtargeting; and cooperation with electoral regulations has become essential; and (d) self-regulation and codes of conduct should be encouraged.

C. Regulation of Direct Marketing in Electronic Communications Services

EU telecommunications law contains rules on direct marketing, in the current ePrivacy Directive, that are relevant for the regulation of disinformation. These rules are only applicable to direct marketing via a limited number of communication technologies. The ePrivacy Directive is mainly implemented in the Dutch "Telecommunicatiewet" that regulates 'public electronic communication networks' such as telephone, television, internet and fax.[264] The rationale behind these specific norms is that spam should be regulated as communication services such as telephone and email facilitate direct and targeted contact. As such, people should retain a measure of control over such channels to prevent nuisance or over-usage.

When implementing the e-Privacy Directive in the Telecommunications Act, the Dutch legislator opted for a broad interpretation of the ban on spam, which also includes political communication. Specifically, Section 11.7 of the Telecommunications Act primarily prohibits unsolicited communications via "automatic call and communication systems without human intervention, faxes and electronic messages" if the recipient has not given permission to do so. Automated advertising by telephone, fax or the Internet is therefore prohibited. This prohibition also applies to political advertisements as it includes "transmitting unsolicited communications for commercial, ideological or charitable purposes".[265] This provision implements Article 13 of the e-Privacy Directive,[266] with the important difference, as stated above, that where the Directive leaves open the question of whether political advertising also falls within the definition of direct marketing, the Telecommunications Act clearly indicates that this is the case.

The Netherlands is not the only European country that already chose to interpret these rules on direct marketing broadly, and that consider them to be applicable to political communication through internet-based communications services like WhatsApp and Facebook Messenger. For example the UK regulator takes this position, stating that direct marketing 'includes the promotion of the aims and ideals of any organisation including political campaigns', and would include 'appeals for funds or support for a campaign, encouraging individuals to take some form of direct action or vote for a particular political

263 Idem., p. 9.
264 Article 1.1 of the Telecommunications Act '*public electronic communications network'*.
265 Article 11.7 paragraph 1 Telecommunications Act.
266 Directive 2002/58/EC.

party or candidate'.[267] This would apply to any means of electronic communication, including email, but also social media and messaging applications.

There is a second limitation in the Telecommunications Act, this time of national origin, relating to the do-not-call register for telephone advertising . Once a person has registered in this register, they may not be contacted by unsolicited telephone calls for political advertising.[268] With the introduction of the e-Privacy Regulation, this regime is expected to be adapted from an opt-out to an opt-in system. Advertising is only allowed when permission has been given. This prohibition, unless consent is given, will apply to any form of unsolicited electronic communication.[269] Supervision of these rules is carried out jointly by the Data Protection Authority (AP) and the Consumer and Market Authority (ACM). The AP is competent for the processing of personal data, and the ACM for the regulation of unsolicited electronic communications itself.[270]

Furthermore, it is important to note that both these frameworks are currently under revision. Firstly, the EU's Communications Code (**"EECC"**),[271] which replaces the set of existing Directives on public electronic communications networks and services, extends its scope to so-called 'over the top services', e.g. internet-based communications services like WhatsApp and Skype. The EECC must be implemented in national law by December 2020, and the European Council stated that the purpose of the ECCC is to ensure that consumer rules will now extend to services provided over the internet, such as messaging apps; and that Member States will also have to establish rules for compensation in case of misconduct by providers of electronic communications networks or services. Secondly, proposals to replace the existing ePrivacy Directive with an ePrivacy Regulation are under discussion in the Council of Ministers.[272]

This proposals for a new ePrivacy Regulation contain rules on direct marketing that may be applicable to the type of political communication described above, where a political party sends a political message directly to an individual through a messaging service such as WhatsApp or Facebook Messenger. The proposed ePrivacy Regulation may also be a tool to address the use of fake accounts to spread political messages directly on WhatsApp. In the recent Indian elections, WhatsApp emerged as a central method of disseminating political communication.[273] In response to its rising importance for political communications during elections, WhatsApp has introduced user controls to protect the integrity of elections, including a forwarding label, a forwarding limit, and a ban on automated messaging to combat viral misinformation during elections.[274]

Indeed, the Regulation explicitly mentions that the concept of direct marketing includes 'messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties', and 'messages sent by other non-profit organisations to support the purposes of the organisation'. Not only that, but the Regulation also speaks about it being 'necessary to prohibit the masking of the identity and the use of false identities' while sending unsolicited commercial communications for direct marketing purposes.

267 Information Commissioner's Office, '*Guidance on political campaigning'*, 2018, p. 6.
268 Article 11.7 paragraph 5 to the Telecommunications Act.
269 Article 16(1) proposed e-Privacy Regulation, COM/2017/010 final - 2017/03 (COD), see further chapter 5.
270 Article 17 Protocol of Cooperation between the Consumer and Market Authority and the Authority for Personal Data, ACM, Netherlands Government Gazette 2016 No 58078.
271 Richtlijn (EU) 2018/1972 establishing the European Electronic Communications Code, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN.
272 Proposal for a Regulation of the European Parliament and of the Council on the respect for privacy and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications), COM(2017) 10 final, 10 January 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010
273 See Murgia, M., Findlay, S. & Schipani, A. '*India: The WhatsApp Election',* Financial Times, 5 May 2019.
274 WhatsApp, *'Contributing to the security of elections in India'*, https://faq.whatsapp.com/en/26000233/https://faq.whatsapp.com/en/26000233/.

The relevant rules on direct marketing in the proposals are contained in Article 16, which provides that any person using electronic communications services to transmit direct marketing communications must inform end-users of (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. The ePrivacy Regulation proposal also provides that fines of up to 10 million euro may be imposed for infringements of Article 16.

In sum, the European Union legal frameworks for electronic communications services already provide for rules on direct marketing communications and relevant amendments in this area will further increase the relevance of EU electronic communications law for the regulation of political advertising through electronic communications services.

D. Audiovisual Media Services Directive

The Audiovisual Media Services Directive (**"AVMSD"**)[275] seeks to ensure a minimum level of harmonisation across the EU of national legislation governing audiovisual media services, with a view to removing obstacles to the free movement of such services within the EU's single market. In pursuance of these aims, the Directive coordinates a number of areas: general principles; jurisdiction; incitement to hatred; accessibility for persons with disabilities; major events; the promotion and distribution of European works; commercial communications and protection of minors. The directive is mainly implemented in the Dutch Mediawet, that also contains a large number of national provisions on the programme offer and advertisement possibilities.[276] Oversight and enforcement of media regulation within the Dutch context is delegated to the Commissariaat voor de Media (CvdM).[277]

The AVMSD has evolved from the former 'Television without Frontiers' Directive, and covers traditional television broadcasting as well as on-demand audiovisual media services. Following the revision of the Directive in 2018,[278] the providers of video-sharing platform services now also fall under the scope of the Directive, insofar as they are covered by the definition of such services. The definition is rather convoluted:

> "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.[279]

The thinking behind this shift is that privately-owned internet intermediaries exert organisational control over third-party content; they determine the modalities of how that content is made available, its level of prominence, and so on. If they *de facto* control what their users see and how they see it, they should also be held responsible or liable for the content – even though they do not have editorial control over

275 Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0013rom=EN

276 See chapter 6.

277 Chapter 7 of the Media Act.

278 Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0013rom=EN

279 Idem, Article 1(1)(aa).

it. Recital 47 of the Directive spells out this thinking in relation to video-sharing platforms in the context of the Directive:

> "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."

This thinking has been criticized for resulting in "considerable political and social pressure [being] exerted on these platforms to resolve the problems 'themselves'".[280] This, in turn, "leads to a 'spiral of privatised regulation'".[281]

The applicability of the Directive to the providers of video-sharing platform services does not concern all provisions of the Directive. The focus is very much on harmful content that is damaging for minors, as well as certain types of illegal content, in particular incitement to violence or hatred, and public provocation to commit a terrorist offence, offences concerning child pornography and offences concerning racism and xenophobia.[282] Without prejudice to Articles 12 to 15 of the E-Commerce Directive, Member States shall ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect minors and the general public from programmes, user-generated videos and audiovisual commercial communications entailing the aforementioned types of content.

The AVMSD contains rules on "audiovisual commercial communications", which are defined as "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".[283] "Audiovisual commercial communication" is a wide term that covers television advertising, sponsorship, teleshopping and product placement. Under Article 9(1)(a) of the Directive, audiovisual commercial communication must be "readily recognisable as such" and surreptitious audiovisual commercial communication is prohibited. Also, under Article 9(1), subliminal techniques shall not be used; audiovisual commercial communications shall not prejudice respect for human dignity or include or promote discrimination. Member States must ensure that video-sharing platform providers comply with these and the other requirements of Article 9(1) "with respect to audiovisual commercial communications that are marketed, sold or arranged by those video-sharing platform providers".[284]

The first issue is whether political advertising is covered by the AVMSD's rules on advertising. As the definitions are primarily about the promotion of goods, services or image in pursuit of an economic activity, paid political advertising is not, as such, covered by the AVMSD's advertising rules.

280 Wagner, B., *'Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech'*, in: Moore, M. & Tambini, D. (eds.) (2018) '*Digital Dominance: the Power of Google, Amazon, Facebook, and Apple*' (Oxford, Oxford University Press, 2018), p. 219-240, p. 223.
281 Ditto
282 Directive (EU) 2018/1808, Article 28b.
283 Idem, Article 1 paragraph 1 sub h.
284 Idem, Article 28b(2).

The second issue is whether the rules imposed on video-sharing platforms under the AVMSD are applicable to political advertising distributed on, for example, YouTube. Article 28b, summarized above, sets out that any protective measures taken by Member States must not lead to any ex-ante control measures or upload-filtering of content which do not comply with the e-Commerce Directive.

Article 28b(3) provides that the measures "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. Article 28b(6) provides that Member States may impose on video-sharing platform providers measures that are more detailed or stricter than the measures referred to, so long as they are consistent with EU law, including the e-Commerce Directive.

As such, the new AVMSD requires member states to ensure video-sharing platforms in certain circumstances, put certain measures in place concerning user-generated videos and audiovisual commercial communications. As mentioned, paid political advertising is not covered by the definition of audiovisual commercial communications. However, the definition of user-generated 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"[285]) may apply to campaign videos and videos containing political communication uploaded by a political party or group. Again, it is an open question whether the concept of political advertising should include a political party or group publishing a campaign video, and uploading it to YouTube. But this type of organic content would still be covered by the rules under Article 28b AVMSD.

It also seems that a member state could possibly extend the definition of "audiovisual commercial communications" to include political advertising, and then impose the measures under Article 28b(3)(1) of the AVMSD on video-sharing platforms such as YouTube. This would ensure uploaded videos carry a notice that it contains sponsored content, and allow users to flag objectionable content.

It may also be helpful to refer to its rules on freedom of reception, which can inform the present report's discussion of foreign influence. Under Article 3 AVMSD, Member States must ensure "freedom of reception" and must not "restrict retransmissions on their territory of audiovisual media services from other Member States for reasons which fall within the fields coordinated by this Directive". Thus, Member States are generally prohibited from restricting retransmissions of audiovisual media services from other Member states. However, there are exceptions to this rule, where content may contain incitement to violence or hatred, public provocation to commit a terrorist offence, content that seriously impair minors.

Finally, it should be noted that in the European Commission's 2018 Recommendation on disinformation and elections, it suggests that member states can 'draw inspiration' from the AVMSD's rules on the recognisability of audio-visual commercial communications when considering how to ensure transparency in paid online political advertisements.[286]

285 Idem, Article 1 paragraph 1 sub ba.

286 European Commission, *'Recommendation on election cooperation networks, online transparency, protection against cyber security incidents and combating disinformation campaigns in the framework of the elections to the European Parliament'*, C(2018) 5949 final, 12 September 2018, p. 4.

E. Disinformation & commercial regulation

Per the definition, some forms of disinformation are explicitly linked to economic profit, bringing EU commercial regulation into scope. The European Commission emphasizes that the creation and dissemination of disinformation are often economically profitable, although the precise relationship is not elaborated on.[287] Delving deeper, the economic gain can be achieved, on the one hand, by means of the content of the disinformation for parties that profit from the spread of that particular false and harmful information.[288] On the other hand, there are also parties that spread disinformation on a large scale commercially. These so called 'trolls' do not necessarily profit from the content of the disinformation and rather simply get paid for spreading it.[289] Given this for-profit aspect to disinformation, two important connections can be made between commercial regulation and disinformation. Firstly, in the regulation of commercial speech and actions, specifically of importance are the prohibition of misleading advertisements, unfair trade practices and unfounded health claims. Secondly, the large number of transparency obligations with regard to commercial advertisements can be linked to or serve as an example for the possible regulations pertaining to disinformation. It follows from this existing regulatory landscape that the commercially motivated disinformation that distorts economic relations or, for example, contains harmful medical claims directed at consumers, is already extensively regulated.

With regard to the regulation of commercial speech and actions that can be linked to disinformation two directives are of specific importance. This is firstly, and most importantly, the directive on Unfair Commercial Practices[290] (**"UCP Directive"**), that is implemented in section 3A, articles 193a through 193j of book 6 of the Dutch Civil Code (**"DCC"**).[291] This directive made substantial steps in harmonizing commercial regulation in the EU.[292] The substantive norms of the directive are in the Netherlands implemented as a part of tort law, allowing civil enforcement in addition to enforcement by the relevant regulatory authorities.[293] The UCP Directive aims to protect consumer interests and does so by means of maximum harmonisation.[294] The directive is explicitly aimed at the commercial practices of business directed at consumers, excluding any business to business practice.[295] These latter relations are covered by the directive on misleading advertisement discussed below, and do fall under the general category of a wrongful act.

The notion of 'commercial practices' in the context of the UCP-directive covers a wide range of activities, encompassing "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".[296] The substantive norms can be divided into three categories: (i) a general prohibition on unfair commercial practices,[297] (ii) specific norms regarding misleading or aggressive

287 European Commission, *'Tackling online disinformation: a European Approach, COM(2018) 236 final'*, https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-236-F1-EN-MAIN-PART-1.PDF.
288 Wardle, C., & Derakhshan, H. '*Information Disorder. Toward an interdisciplinary framework of research and policymaking*', z.p., 2017 p. 27.
289 Idem, p. 31; 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. 32, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.
290 Directive 2005/29/EC.
291 House of Representatives, 2006-2007, 30 928, no. 3.
292 Stuyck, J.,Terryn, E. &Van Dyck, T., *'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, p. 381.
293 Duivenvoorde, B.B., *'Unfair commercial practices'*, TcVH 2016-1, pp. 16-23.
294 House of Representatives, 2006-2007, 30 928, no. 3 p. 1.
295 Directive 2005/29/EC, Article 3, Recitals 6 & 8; De Vrey, R.W., '*Commercial Practices and Advertising', in*: Hondius, E.H. & Rijken, G.J.., *Handbook Consumer Law*, 2015 Zutphen: publisher Paris, p. 383; House of Representatives, 2006-2007, 30 928, no. 3, p. 1; See also for the Dutch context: Hof Arnhem-Leeuwarden 15 May 2014, ECLI:NL:GHARL:2014:3884 (*Het Gilde Utrecht/Telefoonboek).*
296 Article 2(d) Directive 2005/29/EC.
297 Article 5 of Directive 2005/29/EC; Article 6:193a of the Netherlands Civil Code.

commercial practices,[298] and (iii) the commercial practices which in all circumstances are considered unfair.[299] These norms overlap with disinformation substantially.

The general prohibition of unfair commercial practices, in article 5 of the directive or article 193b sub 2 book 6 DCC, states that a commercial practice is unfair if it both is "contrary to the requirements of professional diligence" *and* "materially distorts or is likely to materially distort the economic behaviour" of the "average consumer" who is " who is reasonably well-informed and reasonably observant and circumspect."[300] This general prohibition would also apply to any type of disinformation that goes against general commercial standards (professional diligence) and successfully manipulates consumers' economic behaviour. However, the specific set of unfair commercial practices that fall within the category of 'misleading commercial practices' are most closely related to disinformation. This category, codified in article 6-7 of the Directive and the articles 193c to 193f book 6 DCC, considers a practice to be unfair when it firstly "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" and secondly this causes the consumer "to take a transactional decision that he would not have taken otherwise".[301] The false or misleading information has to pertain to one of a large, albeit limitative, list of aspects such as the main characteristics of the product or the identity of the trader. The provision also covers misleading comparative advertisement.[302] Additionally, omissions can also be considered a misleading practice, for example when an information requirement is not met.[303] With the focus on false or misleading information, this category of 'misleading commercial practices' definitely falls within the scope of disinformation. On the other hand, the specific category of aggressive commercial practices is less related to disinformation, as it mainly deals with consumer harassment or coercion rather than deception or manipulation. Finally, there is a long list of commercial practices that are considered unfair in any circumstance, contained in annex I of the directive and implemented in Article 193g (misleading practices) and Article 193i (aggressive practices) Book 6 DCC. Therein are many examples of false or misleading information that would also qualify as disinformation.

Enforcement of these norms is both possible via civil proceedings, brought by consumers or by competitors,[304] or via the relevant supervisory authorities that can administer fines and issue orders.[305] The Dutch regulatory authorities the Autoriteit Consument en Markt ("**ACM**") and, with regard to financial products, the Autoriteit Financiële Markten ("**AFM**") are competent for the enforcement of these norms in the UCP Directive.[306] Self-regulatory instruments such as the Nationale Reclame Code (National Advertising Code) also play a significant role in the norm-enforcement pertaining specifically to advertisements.[307]

The second relevant directive for the relation between disinformation and commercial regulation is the directive Misleading and Comparative Advertising[308] ("**MCA Directive**"), and its precursor the directive on Misleading Advertisement.[309] Misleading and comparative advertisements within a Dutch context is

298 Misleading commercial practices in Sections 6 and 7 of Directive 2005/29/EC and Sections 6:193c-193f of the Netherlands Civil Code; aggressive commercial practices in Sections 8 & 9 of Directive 2005/29/EC and Section 6:193h of the Netherlands Civil Code.
299 Annex II Directive 2005/29/EC and Section 6:193g in conjunction with 6:193i of the Netherlands Civil Code.
300 CJEU, 16 July 1998, C-210/96 (*Gut Springenheide/Steinfurt; '6-Korn - 10 frische Eieren')* par. 37. There are still specific rules for vulnerable consumers, see recital 18 and Article 5(3) of Directive 2005/29/EC.
301 Article 6 of Directive 2006/114/EC as implemented in Sections 6:193c of the Netherlands Civil Code.
302 Article 6(2) Directive 2006/114/EC as implemented in Sections 6:193c(2) of the Netherlands Civil Code.
303 Article 7 of Directive 2005/29/EC implemented in Section 6:193d of the Netherlands Civil Code. This information obligation is particularly important in the case of an invitation to purchase, see Article 7(4) of Directive 2005/29/EC. See also 6:193e BW and annex II Directive 2005/29/EC.
304 De Vrey, R.W., *'Handelspraktijken en reclame',* in: Hondius, E.H. & Rijken, G.J., 'Handbook of *Consumer Law',* 2015 Zutphen: publisher Paris, p. 405.
305 Article 2.9 Consumer Protection Enforcement Act.
306 Article 8.8 in conjunction with 8.11 and annex a of the Consumer Protection Enforcement Act.
307 De Vrey, R.W., *'Commercial Practices and Advertising'*, in: Hondius, E.H. & Rijken, G.J., Handbook on *Consumer Law,* 2015 Zutphen: publishing house Paris, p. 405.
308 Directive 2006/114/EC.
309 Directive 84/450/EEC.

codified in title 3.4, in the articles 194 to 196 of book 6 DCC. In this section the different directives are implemented, although some of these provisions predate the European harmonisation efforts.[310] The MCA Directive is closely related to the UCP-directive with some exceptions. A first notable difference is that it offers minimum harmonization, creating more space for national implementation,[311] secondly the MCA-directive has a fundamentally different scope as it is only concerned with business to business communication.[312] This more narrow scope is clear from the purpose stated in article 1: "to protect traders against misleading advertising and the unfair consequences thereof and to lay down the conditions under which comparative advertising is permitted." The focus on business to business communication makes these provisions less relevant for spread of disinformation, as follows from the focus on public harm and the implied wide societal spread of the information contained in the discussion on disinformation. Nevertheless, the two central provisions, article 194 and 194a book 6 DCC do merit brief consideration.

Article 194 book 6 DCC states that an advertisement directed at another business is unlawful when it is misleading, and the misleading information pertains to a limited list of aspects contained in the article, such as the nature, price or origin of the product. An omission can also be considered misleading when it pertains to information necessary to make an informed purchase.[313] Advertisement is defined as making a public announcement about goods or services on offer irrespective of medium, explicitly excluding advertisements of a political nature.[314] Subsequently, article 194a book 6 DCC was created for the 2002 directive on comparative advertisement.[315] The provision, as a general rule, allows for comparative advertisement under specific cumulative conditions contained in the provision. CJEU has in its case-law elaborated extensively on how the different conditions for lawful comparative advertisement have to be interpreted.[316] Enforcement via civil proceedings is made easier by the provisions in article 195 book 6 DCC that relieve the burden of proof. Administrative oversight and enforcement are, as with the UCP Directive, carried out by the ACM and the AFM.[317] Additionally, the self-regulatory instrument of the *Nationale Reclame Code* plays a substantial role in enforcing the MCA Directive and the broader Dutch rules on misleading and comparative business-to-business advertisements.[318]

Furthermore, a related sector specific legal framework regulating the content of commercial communication exists for the regulation of health claims in a commercial context. These provisions are especially relevant for any discussion about disinformation given the potential harm health-related disinformation could inflict. An example of such a connection is the widespread harmful information on the purported damaging effects of vaccines that is suspected to have contributed to lowered vaccination rates.[319] A myriad of EU provisions exists that regulate the content of commercial communication regarding food and medication safety. There is for example the Regulation on nutrition and health claims made on foods, that sets out in minute detail the conditions under which such claims can be made in the labelling, presentation and advertising of foods and misleading or false claims are forbidden.[320] With regard

310 House of Representatives, 1975-1976, 13 611, no. 1-4.
311 Article 8 Directive 2006/114/EC.
312 De Vrey, R.W., *'Commercial Practices and Advertising'*, in: Hondius, E.H. & Rijken, G.J., Handbook on *Consumer Law,* 2015 Zutphen: publishing house Paris, p. 398.
313 article 194 sub 2-4 book 5 DCC.
314 Second Chamber, 1975-1976, 13 611, no. 3, p. 9; Asser/Hartkamp & Sieburgh, 6IV 2015/315 "Openbaar (doen) maken misleidende kennisgeving.
315 Directive 97/55/EC.
316 CJEU 18 November 2019, C-159/09 (*Lidl SNC/Verizon Distribution SA)*.
317 Annex a Consumer Protection Enforcement Act.
318 De Vrey, R.W., *'Commercial Practices and Advertising'*, in: Hondius, E.H. & Rijken, G.J., Handbook on *Consumer Law,* 2015 Zutphen: publishing house Paris, p. 411.
319 For the Dutch context, see: External Advisory Committee on Vaccination Readiness to Vaccinate, *'In gesprek over vaccineren'*, Rijksvaccinationprogramma Nederland 2018' RIVM; Volkskrant, *'Vaccination Rejectors: Why Anti-vaccineers Cause So much Resistance'* 2019, https://www.volkskrant.nl/nieuws-achtergrond/vaccinatieweigeraars-waarom-anti-vaxxers-zo-veel-weerstand-oproepen~baad1ac0/. For a discussion on possible mandatory vaccination see: Pierik, R.H.M. (2019). Does an obligation to vaccinate fit within the ECHR regime? *Tijdschrift voor Gezondheidsrecht*, *43*(4), 8-25. https://doi.org/10.5553/TvGR/016508742019043004002 and Pierik, R. (2018). Mandatory Vaccination: an Unqualified Defence. *Journal of Applied Philosophy*, *35*(2), 381-398. https://doi.org/10.1111/japp.12215.
320 Article 3 Regulation (EC) No 1924/2006.

to medicine, the directive on the Community code relating to medicinal products for human use, takes centre stage regulating almost all aspects regarding the sale, production, distribution and advertising of medical products for human use.[321] Title VIII of the directive is concerned especially with advertising and is implemented in chapter 9 of the Dutch *Geneesmiddelenwet* (Medicines Act). As a general rule, misleading advertisement is prohibited and notably, advertisement directed at the general public of medical products only available on a medical prescription or containing narcotic substances, is completely prohibited.[322] The directive furthermore sets out several information requirements on the medical advertisements that are allowed. These requirements are part of annex II of the UCP Directive, which means that any such omissions are also considered to be a misleading commercial practices under the UCP Directive.[323] Consequently, in a commercial context misleading health-claims or the omission of vital information regarding, among others, the medical product or the producer is thoroughly regulated. In the Netherlands, the *Nederlandse Voedsel- en Warenautoriteit* (Netherlands Food and Consumer Product Safety Authority) is responsible for oversight and enforcement of these norms.[324]

Closely related to the aforementioned limitations on commercial communication and equally relevant in the discussion of disinformation are the many different transparency obligations regarding commercial communication or more specifically commercial advertisements. The transparency obligations contained in the UCP Directive and ECD have already been discussed, but there are several other norms that regulate the disclosure of relevant information within a large number of different commercial contexts. The general aim of these provisions is to ensure that advertising is recognisable as such and that sufficient information is provided to enable economic actors to make reasoned decisions. For example, the AVMSD requires advertising on television to be recognisable as such[325] and the ePrivacy Directive requires the sender of direct marketing messages via electronic mail to be identifiable.[326] The Commission has indicated that member states could draw inspiration from the information requirements in the ECD and the AVMSD for any possible transparency measures regarding political advertising.[327]

From this overview of the EU commercial regulation relevant to disinformation follows firstly that, within a commercial context, false and misleading information in many cases will already be prohibited, and secondly that a large number of information requirements exists aimed at properly informing consumers and other relevant economic actors. Consequently, a large part of the for-profit disinformation is already regulated; as soon as economic interests are involved and people's economic behaviour is manipulated, this large body of regulations comes into play. Because of the often-meagre incentives for consumers or other individuals to seek judicial redress to non-compliance to these norms, oversight and enforcement by regulators such as the ACM are especially of importance. Notably, the European Commission is currently discussing a proposed directive aimed at improving the consumer rights enforcement which will expand the possibilities of representative injunctive and compensatory redress.[328]

321 Directive 2001/83/EC.
322 Article 88 of Directive 2001/83/EC, implemented in Article 85 of the Medicines Act.
323 See Annex II in conjunction with Article 7(4) of Directive 2005/29/EC.
324 Article 100 of the Medicines Act.
325 Article 19 Directive 2010/13/EU.
326 Article 13(4) Directive 2002/58/EC.
327 European Commission, 'Code of Practice on Disinformation, preamble. *'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, p. 4.
328 COM/2018/0184 final - 2018/089 (COD).

F. Current state of self- and co-regulation

In 2018, the European Commission facilitated the creation of a new self-regulatory instrument for disinformation and political advertising: The EU Code of Practice on Disinformation.[329] This code was established in line with the objectives set out in European Commission 2018 Communication on Tackling online disinformation: a European Approach,[330] and formed a part of the Action Plan against Disinformation.[331] Signatories include advertisers and major tech companies such as Google, Facebook, Mozilla and Twitter, with Microsoft joining in May 2019.

The Code includes a number of actions that tech companies can put in pace in order to address the challenges of disinformation. These include putting in place (a) safeguards against disinformation; (b) intensify and demonstrate the effectiveness of efforts to close fake accounts[332] and establish clear marking systems and rules for bots to ensure their activities cannot be confused with human interactions; (c) intensify and communicate on the effectiveness of efforts to ensure the integrity of services with regards to accounts whose purpose and intent is to spread disinformation; (d) invest in technological means to prioritize relevant, authentic, and accurate and authoritative information where appropriate in search, feeds, or other automatically ranked distribution channels; (e) dilute the visibility of disinformation by improving the findability of trustworthy content; and (f) consider empowering users with tools enabling a customized and interactive online experience so as to facilitate content discovery and access to different news sources representing alternative viewpoints, also providing them with easily-accessible tools to report disinformation.

Further, the Code has a specific section on the integrity of services, and the companies committed to (a) put in place clear policies regarding identity and the misuse of automated bots on their services and to enforce these policies within the EU; and (b) put in place policies on what constitutes impermissible use of automated systems and to make this policy publicly available on the platform and accessible to EU users.

Of particular relevance with regard to the regulation of political advertising is the requirement for the signatories to perform: "Scrutiny of ad placements" targeting "purveyors of disinformation" (Section II.A.) and Transparency in political and issue-based advertising – including public disclosures and user-facing disclaimers (Section II.B.). Further, the code requires the signatories to produce yearly compliance reports. These offer detailed information on their political advertising practices, such as monitoring and verification procedures and takedown statistics. (Section III).[333]

The Code also includes an annex with best practices of the different signatories,[334] and the signatories created roadmaps for the implementation of the code in their respective organisations.[335] Facebook, Google and Twitter were asked by the Commission to report on a monthly basis on the progress of the implementation of the code. The reports of the months January to May 2019 are published together with the Commission's own assessments.[336] The Commission is in general satisfied with the code's implementation but has urged Facebook, Google and Twitter to develop tools to "increase the transparency and

329 Europese Commissie, *'EU praktijkcode tegen desinformatie'*, preambule, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. See Peter H. Chase, The EU Code of Practice on Disinformation: The Difficulty of Regulating a Nebulous Problem, Transatlantic Working Group on Content Moderation Online and Freedom of Expression, 29 August 2019, https://www.ivir.nl/publicaties/download/EU_Code_Practice_Disinformation_Aug_2019.pdf.

330 Europese Commissie, *'Tackling online disinformation: a European Approach,* COM(2018) 236 final', https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-236-F1-EN-MAIN-PART-1.PDF.

331 Action Plan against Disinformation, JOIN(2018) 36 final.

332 See Financial Times, '*Facebook's fake numbers problem – Lex in depth',* 18 November 2019 van https://www.ft.com/content/98454222-fef1-11e9-b7bc-f3fa4e77dd47.

333 See https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

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

335 See: https://ec.europa.eu/digital-single-market/en/news/roadmaps-implement-code-practice-disinformation.

336 See: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

trustworthiness of websites hosting ads for the benefit of advertisers".[337] Before the end of 2019 the Commission will evaluate the effectiveness of the Code in its first year.

Concretely, Facebook, Twitter and Google have all created ad repositories,[338] and political ad transparency tools.[339] Google for example requires advertisers to verify both their eligibility to run political ads and their identity.[340] Facebook also requires advertisers to identify themselves, and imposes the additional requirement that advertisers have to be a resident of the country they plan to campaign in.[341] The creation of these policies and specific requirements for political advertising by internet services raises the logical question about their effective enforcement. Additionally, these and other policy changes have been initiated by these platforms specifically to prepare for large elections such as the 2020 US presidential election.[342] Further, Twitter has banned 'state-controlled news media' from advertising on its platform.[343] Finally, on 20 November 2019, Google published its new, most recent policy on political advertising.[344] The news item accompanying this new Google policy explicitly states that *granular microtargeting* for election advertisements is not permitted. For election advertisements, targeting is only permitted on the basis of age, gender and postal code. *Contextual targeting is* also permitted. In the case of *contextual targeting* for election advertisements, it is possible to use an advertisement on the basis of subjects and keywords used. At the moment it is still possible to target more specifically, as it will take until the end of 2019 before this change enters into force throughout Europe. In the rest of the world, this will take even longer. Google will start implementing the changes as of January 6, 2020. It is not known when the implementation will be completed.

In addition to these organised self-regulatory measures, many social media platforms are finding their own way to address disinformation connected to political advertisements through their platform policies. Facebook for example, announced to stop checking political advertisements on their content, sparking a wide spread debate on the desirability of unchecked political advertisement and generating resistance of Facebook employees themselves.[345] On the other end of the spectrum, Twitter announced it will ban political advertisements completely on its platform, again sparking widespread debate.[346]

G. Recent developments and proposals with respect to disinformation and political advertisements

There are a number of developments and proposals at EU level on political advertising and disinformation, beyond the self-regulatory EU Code of Practice on Disinformation. First, in the European Commission's 2018 Recommendation on elections and disinformation, it recommended that EU member states (a) encourage and facilitate the transparency of paid online political advertisements and communications; and (b) encourage the disclosure of information on campaign expenditure for online activities, including

337 European Commission, *'Code of Practice on Disinformation: Intermediate targeted monitoring – May reports'*. https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation.
338 Leerssen, P. e.a., '*Platform Ad Archives: Promises and Pitfalls*' working paper, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380409).
339 European Commission, *'Code of Practice on Disinformation: Intermediate targeted monitoring – May reports'*. https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation.
340 Google February 2019 report, https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation.
341 Facebook April report p. 7 https://ec.europa.eu/digital-single-market/en/news/fourth-intermediate-results-eu-code-practice-against-disinformation
342 Barrett, P.M., *'Disinformation and the 2020 Election: how the Social Media Industry Sould Prepare',* NYU Stern: september 2019, par. 3.
343 See Wong S., Shepherd C., & Liu, Q., *'Old messages, new memes: Beijing's propaganda playbook on the Hong Kong protests'*, Financial Times, 2019.
344 Google, '*An update on our political ads policy*', 20 November 2019, https://blog.google/technology/ads/update-our-political-ads-policy/
345 Mike Isaac, *'Dissent Erupts at Facebook Over Hands-Off Stance on Politcal Ads',* The New York Times, 28 October 2019, https://www.nytimes.com/2019/10/28/technology/facebook-mark-zuckerberg-political-ads.html?module=inline
346 Kate Conger, *'Twitter will ban all politcal 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

paid online political advertisements and communications.[347] Further, in the European Commission's 2018 Communication on European elections, it stated that transparency of political advertisements should apply similarly in the online world. [348]

More recently, the European Council adopted its Conclusions on Securing Free and Fair European Elections, in which it highlighted the "need, in line with the applicable rules, to foster and facilitate the transparency of paid online political advertisements and communications including on their advertising purpose, the methods by which they are targeted to citizens, and their funding".[349]

Of note, the new European Commission President's Political Guidelines for the next European Commission 2019-2024, states that a European Democracy Action Plan will be put forward, which will include "legislative proposals to ensure greater transparency on paid political advertising and clearer rules on the financing of European political parties".[350] In addition, the Guidelines also include plans for "common standards to tackle issues such as disinformation and online hate messages" on digital platforms.[351]

A leaked Commission Staff Document on e-Commerce reform includes specific rules for "cross border online advertising services, including for rules around political advertising, adequate possibilities for auditing and accountability, as well as with a view of lowering entry barriers for competitors and alternatives".[352] Most recently, in October 2019, the Commission launched its plans to create a European Digital Media Observatory, which will be a digital platform to help fight disinformation in Europe.[353] It will serve as a hub for fact-checkers, academics and researchers to collaborate with each other and actively link with media organisations and media literacy experts, and provide support to policy makers. Thus, there is considerable EU activity on or implicating the regulation of disinformation and political advertising, with possible EU law on the issue entering the EU legislative agenda in different areas.

In addition to facilitating the EU Code of Practice on Disinformation, the European Commission has already started self-regulatory initiatives that touch on disinformation. In 2015, the EU Internet Forum was established as part of the European Agenda on Security in order to combat terrorist and hate-mongering material.[354] The aim of the EU Internet Forum is to achieve a joint, voluntary approach to harmful material through cooperation between public and private parties. Ask.fm, Facebook, Google, Microsoft and Twitter, among others, participate in the EU Internet Forum.[355] During the fifth EU Internet Forum, the EU Crisis Protocol was concluded in October 2019. The Protocol is an EU response to contain the devastation caused by events such as the attack in Christchurch. The Protocol is a form of self-regulation.

---

347 European Commission, *'Recommendation on 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, p. 8, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

348 European Commission, '*Communication on Securing free and fair European elections, COM(2018) 637 final*', https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0637:FIN.

349 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, par. 31, https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf.

350 Von der Leyen, U., '*A Union that strives for more - My agenda for Europe: Political Guidelines for the next European Commission 2019-2024*', p. 21, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

351 Ibid.

352 See Fanta, A. & Rudl, T, *'Leaked document: EU Commission mulls new law to regulate online platforms',* netzpolitik.org, 2019, https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/.

353 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-create-european-digital-media-observatory.

354 European Commission, '*EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online*', 3 December 2015, van https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243; see also: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

355 European Commission, '*EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online*', 3 December 2015, https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243; see also: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

The Protocol has been signed by the European Commission, the Member States of the European Union and private actors such as Facebook, Twitter, Google, Microsoft, Dropbox, JustPaste.it and Snap.[356] The Protocol is not publicly available.

The Protocol contains procedural descriptions for the exchange of critical information. The Protocol is divided into four phases: adoption, notification, information exchange and post-crisis reporting. The Protocol is based on three principles: (a) to reassure the public that the crisis is being managed; (b) to ensure that any tensions are reduced; and (c) to prevent the dissemination of fake news. The Protocol shall apply to exceptional situations where national measures are not sufficient. The Protocol takes care of it: (a) a coordinated and rapid response; (b) a facilitation of cooperation between the public and private sectors; and (c) a facilitation of self-regulation.[357]

H. Overview EU framework

Against the backdrop of the fundamental rights framework developed in chapter 4, this chapter has provided an overview of the relevant EU legal framework for disinformation. The following chapter, discussing the Dutch national legislation, will complete this legal framework.

The overview of relevant EU legislation shows the breath of different legal areas involved: intermediary liability, privacy law, direct marketing, media regulation and commercial regulation as well as self-regulation with respect to disinformation and (political) advertising. Important to note is that the exact applicable legal framework differs along the following dimensions: (i) type of service (hosting provider, video platform service) (ii) type of communication (commercial, health-related) (iii) type of medium (direct messaging, telecommunication service). The diversity of relevant regulation also means several different regulators are involved. For the Dutch context these include the Autoriteit Persoonsgegevens (AP), ACM, AFM and the Commissariaat voor de Media (CvdM).

Another important observation is that this is a very dynamic field of law. Much of the legislation is of a recent date (e.g. the AVMSD and the GDPR), and other legislation is currently under revision (e.g. the e-Privacy Regulation and the ECD). In addition to these legislative activities, several social media platforms are actively addressing disinformation in connection to political advertising by means of their own policies. Further, the commission has given out several Recommendations and supported important self- and co-regulatory developments. As follows, these fast-moving changes mean that the legal framework governing political advertisement is developing quickly on an EU-level.

356 European Commission, *'Fighting Terrorism Online: EU Internet Forum committed to an EU-wide Crisis Protocol'*, October 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6009.

357 European Commission, *'A Europe that protects - EU Crisis Protocol: responding to terrorist content online'*, October 2019, 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. National legal framework

- The relevant national legal framework for disinformation intersects with private law, administrative law and criminal law and includes, among other things, the following
  - Private law: unlawful act (unlawful press publication) and intellectual property law;
  - Criminal law: offences in relation to expression, election crimes, computer crime and offences in relation to distribution;
  - Administrative law: advertising regulation, financing of political parties, national security and critical infrastructure.
- With regard to self-regulation, the National Advertising Code and the Council for Journalism are particularly important.
- There are also a large number of (self-)regulatory initiatives at national level in the area of disinformation.

Now that the constitutional legal framework for freedom of expression and the applicable European legislation have been discussed, it is possible to look at the relevant national law. Below is an overview of the various national regulations that are relevant to the problem of disinformation. In the discussion of the various relevant standards, the classification of private law, criminal law and administrative law is followed for structuring. This was chosen because these three areas of law have their own enforcement instruments and normative frameworks. When discussing criminal law standards, the focus is specifically on the scope of the offence 'election manipulation' and the question of whether it can be extended to make 'online election manipulation' punishable. In this discussion, standards of criminal law relevant to disinformation in the context of computer crime are also discussed. This in the context of the Asscher/Van Der Molen motion,[358] and the fifth research question in this report. In the discussion of the administrative law standards, the emphasis is on regulations that are relevant to the regulation of online political advertisements, because of the specific focus in the interim report.

After discussion of the relevant legal standards, the various self-regulatory instruments at national level will be discussed, especially with regard to advertising and journalism. This is followed by an overview of the relevant national regulatory developments in the field of disinformation.

A. Private law standards

As private law encompasses the general standards of liability, contract and procedural law, it inevitably touches on the problem of disinformation in a very large number of areas. Since it would be impractical to discuss all of these, the focus can be placed on the national private law standards that affect freedom of expression, and are thus directly relate to disinformation.[359] Specifically, the legal structure of tort and intellectual property law (**"IP law")** are important. In many cases, for example, unlawful statements can be regarded as disinformation, but a parody or satire are emphatically not.

Within civil law, the unlawful act in Section 6:162 of the Dutch Civil Code constitutes the broadest possibility of restricting freedom of expression. Detailed standards have been developed in case law for when an expression can be regarded as unlawful and can lead to, inter alia, damages, a ban or, for example, a

358 House of Representatives, 2018/2019 30 821, no. 68.
359 For a discussion of the Dutch approach to unlawful content online see: Letter from the Minister for Legal Protection, 17 July 2019, 2644949 '*Burgerinitiatief "Internetpesters aangepakt'*.

rectification.[360] There are many interfaces between tort on the one hand and disinformation on the other. On the one hand, an unlawful statement can in many cases be classified as disinformation, as it is often incorrect and harmful information. An important difference, however, is that the offender's intention is not relevant to the unlawfulness, while it is relevant to disinformation as established. On the other hand, if there is legally demonstrable damage and a clearly injured person, disinformation can often be qualified as an unlawful expression. In the context of the online distribution of disinformation via internet services, it will often specifically concern the doctrine of the unlawful publication in which the violation of someone's honour and reputation are central. Especially when it comes to disinformation in connection with news, from a legal point of view this is often an unlawful press publication.

This doctrine, which has been developed in case law, requires the judge to make a comprehensive weighing of interest, balancing the interests of the wrongdoer, the injured party and the broader social interest. In essence, the balancing of interests amounts to, on the one hand, freedom of expression of the allegedly wrongdoer, the right to receive information of the wider public, and the protection of the privacy of the allegedly injured party.[361] It is therefore a balancing of two fundamental rights, on the one hand Article 10, and on the other Article 8 of the ECHR. The ECtHR agrees that these fundamental rights are in principle of equal importance.[362] The Supreme Court follows the ECtHR in this respect and ruled in the *Hemelrijk* judgment that there is no separate assessment of the two fundamental rights, but that a consideration must be made of certain factors,[363] which are largely derived from the *municipal council* judgment of 1983.[364] The factors on the basis of which a balancing of interests is made include whether it is a matter of public interest, whether it is a public person, the truthfulness of the publication, the tone used and the working method of the person who has published the information.[365] It follows that the doctrine requires an extensive and complicated legal assessment and motivation. This means that it is also constantly evolving with regularly new judgments.[366]

In addition, there are the more specific standards of IP law, which prohibits, for example, the use of material protected by copyright or trademark law for the purpose of disinformation. On the one hand, IP law thus regulates specific types of disinformation where, for example, for commercial gain, the public is misled by false use of a certain trademark or where an attempt is made to disrupt elections by attributing certain texts to the wrong person. For this type of disinformation, IP law offers tools for regulation and enforcement. On the other hand, IP law also protects freedom of expression by making parody and satire explicitly possible.[367] These are also explicitly excluded from the concept of disinformation in the literature.[368] However, it is not easy to determine when a parody is involved and there is detailed case law at both the Dutch and European level.[369]

Any liability based on tort or copyright infringement is also closely related to the liability framework for internet intermediaries under the E-Commerce Directive with regard to disinformation disseminated via

360 Section 10, title 1, book 6 BW.
361 Alberdingk Thijm, C., *Kiezen uit twee hoogwaardige belangen*, in: C. Eradus, C. Brouwer, H. & Veraart, M. (ed.) 'Bodem *kort geding',* Amsterdam, 2013.
362 Couderc and Hachette Filipacchi Associés v. France (Application No 40454/07) 10 November 2015 [GC], § 91
363 HR 18 January 2008, *NJ* 2008/274 (*van Gasteren/Hemelrijk).*
364 HR 24 June 1983, *NJ* 1984/801.
365 Conclusion, Supreme Court (Advocate General), 07-09-2007 ECLI:NL:PHR:2008:BB3210, ro. 6.
366 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.
367 Article 5(3)k Directive 2001/29/EC, implemented in Article 18b of the Copyright Act.
368 See for example EAVI, July 2017 "Beyond 'fake news' 10 types of misleading news", available at: https://eavi.eu/wp-content/uploads/2017/07/beyond-fake-news_COLOUR_WEB.pdf;
McGonagle, T. et al., '*Inventory of methods to combat "fake news"'*, Institute for Information Law, 2018; Wardle, C., & Derakhshan, H. '*Information Disorder. Toward an interdisciplinary framework of research and policymaking*', September 7, 2017 p. 17.
369 See, for example: Hof Amsterdam 13-09-2011, ECLI:NL:GHAMS:2011:BS7825, *IER* 2012/15 with annotation by Mr. Herman M.H. Speyart; ECJ 03-09-2014, C-201/13 (*Deckmyn).*

internet services.[370] If an internet intermediary falls outside the so-called *safe harbour* and does not adequately address an unlawful statement, it runs the risk of itself being subject to legal proceedings under civil law. The *safe harbour* is therefore of great importance to the injured party as it determines which actors may be held liable. If disinformation via an internet service constitutes a unlawful act and this internet service can invoke the *safe harbour*, the injured person can only appeal to the distributor of the disinformation. In order to maintain a successful reliance on the hosting *safe harbour*, the Internet service must take action as soon as it becomes aware of the unlawful content (notice and action). As the ECD provides for a horizontal limitation of liability, the same applies to the criminal law standards discussed below.

This is directly related to the fact that the filing of a claim often depends on the personal data provided by the internet services of the person who made the statement. These personal data are often only provided by court order due to the complex interplay of data protection standards and different liability grounds, including the E-Privacy Directive, the Enforcement Directive and the ECD discussed earlier.[371] For when such a court order is requested, case law has been developed in which the *Lycos/Pessers* judgment applies as the standard.[372] The court examines whether (i) it is sufficiently plausible that the information is unlawful and harmful towards the third party, (ii) whether the third party has a real interest in obtaining the personal data, (iii) whether there is no less drastic way to obtain the data and (iv) whether a weighing of the interests of the third party, the internet service, and the person whose personal data are involved is in favour of the third party.[373] This doctrine therefore once again requires an extensive and nuanced judicial assessment, which means that it is in continuous development.[374]

Although this is only a selection of the private law standards that could possibly apply to the problem of disinformation, liability law, specifically the tort of unlawful acts and intellectual property law, are the most relevant private law standards and a number of clear conclusions can be drawn from this brief explanation. The above doctrines clearly show how complex and context-specific the explanation and concrete application of these standards are. The boundary between a lawful and an unlawful publication is very difficult to draw, which has led to a very nuanced and balanced jurisprudence. The same applies when an expression has to be considered as a protected satire and when not. This considerably complicates the possible regulation of disinformation, as it means that in such cases the legal qualification is difficult to make.

B. Criminal law standards

A large number of the types of statements that fall under the heading of disinformation are (partially) criminalised at national level. First of all, there are the general rules of criminal law, which are purely based on the content of a specific expression and, as such, place limits on freedom of expression. These are penal provisions such as libel (261 Sr), slander (262 Sr), hate speech (137d Sr) and, for example, group defamation (137c Sr). The criminal law norms that specifically relate to the democratic process are of particular importance for the problem of disinformation, as the disruption of the democratic process is one of the main feared effects of disinformation. These will be discussed below.

As in the case of private law standards, the enforcement of criminal law standards to disinformation is linked to the liability framework for internet intermediaries in the E-Commerce Directive.[375] As long as an internet intermediary falls within the *safe harbour,* it cannot be prosecuted for any disinformation. In

370 See par. 5.A.
371 Directive 2002/58/EC; Directive 2004/48/EC; Directive 2000/31/EC; see Kingma, S.H., '*De botsing tussen IE- en privacyrechten. Het einde van het Lycos/Pessers-tijdperk'*, *P&I* 2012/4 p. 171-177.
372 HR 25-11-2005, ECLI:NL:HR:2005:AU4019.
373 Idem, par. 4.10.
374 Kingma, S.H. *" De botsing tussen IE- en privacyrechten. Het einde van het Lycos/Pessers-tijdperk '*, *P&I* 2012/4 p. 171-177; ECJ no. C-275/06 (Productores de musica de espana (Promusicae)/Telefonica de Espana SAU).
375 See paragraph 5.A.

addition, an improvement in the availability of evidence through Internet services in criminal investigations is currently being pursued through the proposals for an e-Evidence regulation at European level.

Three categories of criminal provisions are relevant for further elaboration in the context of disinformation, specifically in relation to the democratic electoral process. These are the criminal standards that relate to influencing the election process, standards that relate to cybercrime and a number of so-called 'distribution offences' ('*verspreidingsdelicten*').

i. Online manipulation of elections

The Asscher/Van der Molen Motion calls on the government to investigate "whether current descriptions of offences in election manipulation can be extended, so that deliberate online manipulation can also be dealt with under criminal law".[376] Before investigating the existing criminal law possibilities, it is important to consider the concept of 'online manipulation'. As the analysis of the concept of disinformation in chapter 2 showed, online manipulation must be understood as the surreptitious influencing of a person's decision-making by technological means. This includes a wide variety of practices and the Council of Europe's Committee of Ministers has indicated that the problematic and unacceptable version of online manipulation consists of influencing "[that is] subliminal, exploits existing vulnerabilities or cognitive biases, and/or encroaches on the independence and authenticity of individual decision-making".[377] In the context of the democratic election process, it is important that voters independently form an opinion on how they wish to exercise their right to vote, and online manipulation techniques can pose a threat to this.

There are a number of different penal provisions related to this conceptualisation of 'online manipulation', and the dissemination of disinformation via internet services in the context of the improper influencing of elections. This concerns in the first place Title IV of the Criminal Code ("**Criminal Code**") entitled "*Misdrijven betreffende de uitoefening van staatsplichten en staatsrechten*" ("Offences relating to the exercise of state duties and rights"), including five provisions directly related to the prevention of the exercise of the right to vote. There are also a number of provisions in Section VI of the Elections Act (*Kieswet*) that make certain acts in connection with the election process punishable as criminal offences.

The first provision, which relates to the election process, makes it a punishable offence to prevent the free and unhindered exercise of the right to vote by means of violence or the threat of violence.

ARTICLE 125 SR

A person who, on the occasion of an election organised pursuant to a statutory provision **by force or threat of violence, intentionally prevents a person from** exercising his or her right to vote freely and unhindered, or from doing so in any other way, shall be liable to a term of imprisonment not exceeding one year or to a fine of the third category.

This concerns the exercise of the right to vote in elections formally called by law. A causal link must be established between the violence or threat of violence and the prevention of the right to vote. The intent must be to prevent the free exercise of the right to vote, this includes all degrees of intent. For the

376 House of Representatives, 2018/2019 30 821, no. 68.
377 Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, Decl(13/02/2019)1, section 9.

interpretation of "violence" one must refer to Article 81 of the Criminal Code and for the interpretation of "threat of violence" one can look at the same wording from Articles 95, 242 and 284 of the Criminal Code. The Supreme Court has clarified that in the event of a threat of violence it is necessary "that the threat is of such a nature and under such conditions as to give rise to a reasonable fear on the part of the threatened person that violence would be used against him".[378] At the time of introduction, there was a discussion as to whether a broader threat than just the threat of violence should not be included in the description of the offence. At the time it was explicitly decided that only the threat of violence would be punishable as a criminal offence "precisely because this offence involves political views and convictions, it is desirable to describe the offence as narrowly as possible" ('*juist omdat bij dit misdrijf de politieke inzigten en hartstogten in het spel zijn, is het wenschelijk, het strafbaar feit zoo naauwkeurig mogelijk te omschrijven*').[379] This means that scaremongering via the media, or scaremongering in general, is insufficient. There must actually be a concrete threat, as a result of which someone can reasonably fear that violence against him will be used.

There must then be a causal link between this violence or threat of violence and the exercise of the right to vote. This violence or threat must in fact have prevented or psychologically forced the voter, so that there was no longer any question of the "free and unhindered" exercise of the right to vote.[380] This last element, the "free and unhindered" exercise of the right to vote, must be interpreted broadly and does not merely involve the casting of the vote. The secret ballot and the self-selection of the time of casting the vote are also included.[381] As a result, this description of the offence is broader than the description in the following section 126 of the Criminal Code. The fact that the violence or threat must be directly related to the casting of the vote also means that actions prior to the election period must be disregarded.[382]

ARTICLE 126 SR

1. A person who, on the occasion of a statutory election by gift or promise, bribes a person to exercise his or another's right to vote, whether not or in a particular way, shall be liable to a term of imprisonment not exceeding six months or to a third category fine.
2. The same penalty shall apply to the voter or the proxy voter who has been bribed by a gift or promise.

This article prohibits the bribing of a voter or his proxy, and has a slightly narrower scope of protection than article 125 of the Criminal Code: compare 'free and unhindered' ('*vrij en onbelemmerd*') with 'either not or in some way' ('*hetzij niet, hetzij op bepaalde wijze*'). It must concern the content of the vote or the way in which, for example, by means of a proxy. Bribery to just cast a vote regardless of the content is not punishable.[383]

Bribery does not refer to any civil-law legal form of the purchase, but to a certain reciprocity between the actions of the briber and the person entitled to vote.[384] The requirement of intent is embedded in this concept. No causal link is required between the bribery and the actual exercise of the voting right; an accepted offer for bribery as such is sufficient.[385] In a recent case, the Supreme Court ruled that if a voter accepts a gift and/or promise and, in view of the specific circumstances of the case, raises a reasonable

378 HR 3 February 2015, *NJ* 2015/245 see further HR 7 June 2005, *NJ* 2005/448
379 Smidt (1881) p. 60-61.
380 T&C Criminal Law, comments on article 125 of the Criminal Code.
381 Noyon/Langemeijer/Remmelink Criminal Law, section 125 of the Criminal Code, aant. 7.
382 *Idem.* , aant. 6.
383 *Ibidem.*
384 Smidt (1881) p. 62; J.S. Nan, Commentaar op Wetboek van Strafrecht art. 126 (Strafrecht) (article text valid from 01-05-1984).
385 M.A.H. van der Woude, T&C Strafrecht, commentaar op artikel 126 Sr.

expectation that he or she will exercise his or her right to vote in a particular manner, bribery is complete. This does not have to be explicitly promised or made known.[386]

This article is very closely linked to Article Z 4 of the Elections Act, which makes it a punishable offence for someone to "bribe a voter by gift or promise in order to give a proxy to cast his vote". This means the same act could fall under both provisions (art. 55(2) of the Criminal Code).[387]

ARTICLE 128 SR
A person who deliberately takes **part in an election** organised pursuant to a statutory provision on **impersonating another person shall be liable** to a term of imprisonment not exceeding one year or to a fine of the third category.

This penal provision speaks for itself. It's about casting a vote when someone pretends to be someone else, thus frustrating the second person's right to vote. The official registration of the polling station committee states that this second person has already voted, whereas this is not the case.

ARTICLE 129 SR
A person who, on the occasion of an election called for by virtue of a statutory provision, deliberately **obstructs a vote that was last held or commits any fraudulent act as a result of which the result of the vote is different from the result that would have been obtained by the votes lawfully cast**, shall be punished by a term of imprisonment of a maximum of one year and six months or a fine in the fourth category.

Contrary to the previous articles, this provision relates to the outcome of the elections; the other articles were about the free and unhindered casting of the vote itself.[388] This is a fairly broad penal provision, covering all acts that invalidate a previous vote. All acts prior to the conclusion of the vote fall outside the scope of this penal provision and are rather subject to Article 127 of the Criminal Code. Acts falling under Article 129 of the Criminal Code include, for example, the opening of the ballot box or the misappropriation of ballot papers.[389] The second part of the penal provision may, however, relate to acts close to the vote. It is necessary that the results of the elections have changed as a result of the action (as in the absolute number of votes), not that the winner or the distribution of seats would have been different.[390]

ARTICLE 127 SR
A person who, on the occasion of an election which has been called for by virtue of the law, commits any **fraudulent act** that causes a **vote to be void** or **that another than the candidate chosen is selected**, shall be punished by a term of imprisonment not exceeding six months or a fine of the third category.

386 HR 7 June 2019, ECLI:NL:HR:2019:843, *NJ* 2019/242, ro. 7.7.
387 J.S. Nan, Commentaar op Wetboek van Strafrecht art. 126 (Strafrecht) (article text valid from 01-05-1984).
388 Smiths II p. 65.
389 T&C Strafrecht, commentary, comments on Article 129 of the Criminal Code
390 Noyon/Langemeijer/Remmelink Criminal Law, Article 129 of the Criminal Code, aant. 2

Of all these different provisions, Article 127 of Title IV of the Criminal Code seems to be the most appropriate to cover 'deliberate online manipulation', which is why this provision is given the most extensive consideration. The purpose of this article is to protect "unsuspecting and unaware voters" ('*argelooze en onwetende kiezers*') from being misled.[391] This Article deals mainly with fraud in relation to the ballot paper itself, for example by deliberately offering voters invalid ballot papers. The relevant elements are (i) a **causal link**, (ii) an **fraudulent act** and (iii) the consequence of the act of deception, namely (iii-a) the **vote becomes void** or (iii-b) the **error in persona**.

First of all, we must consider the causal connection, since this is by far the most problematic component and determines the extent of both the possible cause (deceptive action) and the possible consequences (invalid vote or error in persona). To put it simply, this specific deceptive act must result in the vote being void or in the wrong candidate being selected.[392] It is therefore necessary to establish a causal link between the two acts. Where it becomes problematic is that parliamentary history gives the impression that a so-called *'causa proxima*' is required in which the fraudster makes the ballot directly the object of his action. This impression is created because the examples in parliamentary history all directly relate to the ballot paper.[393] However, Fokkens argues that such a strict interpretation must be abandoned: even if the voter himself still acts on the ballot paper *after* the fraudulent act, the description of the offence can still be fulfilled.[394] Crucial to this interpretation is that the spreading of misleading information would also be included in the description of the offence. This argument is supported by Nan and van der Woude.[395] In this report the more extensive reading of Fokkens is followed, as the requirement of a causa proxima would limit the description of the crime too much. For example, it would be desirable to include the following in the offence definition: the situation in which voters at polling stations are fooled into believing that the voting procedure has been changed, which results in their votes becoming invalid.

Then, the second element to be discussed concerns the possible consequences of the fraudulent act covered by the description of the offence: (i) the vote becomes invalid or (i) the error in persona. With regard to the first possible consequence, i.e. the loss of the value of the vote, this is determined by the polling station committee on the basis of the objective criteria laid down in the electoral rules.[396] This means that the polling station committee concerned must declare a vote cast invalid. This is a fairly strict and objective criterion. The second possible consequence, the error in persona, must also be narrowly interpreted. Whether or not 'another than the candidate chosen is selected' must be interpreted narrowly: this concerns the situation in which the voter is lead to believe that he has voted for one candidate X while in reality he has voted for another candidate Y.[397] Situations in which a voter is confused about who a specific candidate is (was candidate X the one who was also elected to the Lower House?) or what the exact political convictions of a candidate are (Is candidate X for tax reduction or not?) are explicitly excluded from this. A recent judgment of the Court of Appeal of Den Bosch (2008) dealt with this error in persona and clarified how narrowly this criterion should be interpreted. This concerned fraud in relation to the voting computer in which the defendant as operator of the voting machine, did not at different times did not properly operate the voting computer when a voter wanted/was going to cast his or her vote. He then told those voters, contrary to the truth, that they had voted and/or allowed those voters to leave without informing them that they had not cast a legally valid vote. Afterwards he would he released the voting computer and cast those people's votes himself.[398]

391 Smiths II p. 62.
392 HR June 10, 1924, W 11227.
393 Smiths II p. 62.
394 Fokkens, Noyon/Langemeijer/Remmelink Criminal Law, section 127 of the Criminal Code, aant. 2.
395 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.
396 *Ibid.*
397 *Ibid.* Note 4.
398 Hof Den Bosch, 18 January 2008, ECLI:NL:GHSHE:2008:BC2171.

The last element to be worked out is the element 'fraudulent act' ('*bedrieglijke handeling*'). It is important that the requirement for intent is included in this element and includes all degrees of intent.[399] Then the possible actions that may fall under this element: this is determined on the one hand by the extent of the causal link and on the other hand by the consequences that fall under the description of the offence. In general, parliamentary history defines 'fraudulent acts' as 'tricks' ('*kunstgrepen*') that are intended to make voters vote differently than they intended, for example by means of fake ballot papers.[400] The more extensive interpretation of the causality requirement elaborated above completes this general description by also including *misleading statements* under 'fraudulent acts' within the meaning of the description of the offence. Next, there are a number of examples from the literature and case law that further fill in the concept. Nan gives the example of distributing misleading information "such as passing on the wrong electoral list".[401] Fokkens then gives an example of a party lying about its list number, which creates confusion. A similar case from the end of the 19th century led to a conviction in Utrecht. Two elections took place at the same time and the ballot papers were of a different colour to distinguish them. On the eve of the elections, one of the parties misinformed voters about these colours, and it turned out that people had voted for a different candidate than they wanted.[402] Returning to the causality requirement, this Utrecht case also supports the extensive interpretation of the required causal relationship and thus the broader interpretation of fraudulent acts. Although there is broad support and good arguments for this interpretation, it is not possible to say with absolute certainty, without a final court ruling, whether, in addition to physical acts, the spreading of misleading or inaccurate information should also be included in the description of the offence.

What can be said with complete certainty is that it goes too far to include the dissemination of false information about a candidate's *political beliefs* in 'fraudulent acts'. Parliamentary history shows that this choice was made for because "as much as possible, the judge should remain outside politics; as far as possible it should be prevented by a strict definition of the crime, that politics influences the judge's verdict, even if he were to be influenced by it" ('*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*').[403] The fact that disseminating incorrect information about political convictions does not fall within the scope of the offence description also follows from the fact that such incorrect information cannot have the causal effect of making a vote invalid or making an error in persona.

The analysis of the three central elements gives a fairly clear picture of which situations are, and are not, punishable by Article 127 of the Criminal Code. The following is particularly important in this context: deception about a candidate's political convictions and deception resulting in a person not going to vote are both *not* deceptive acts and are therefore *not* punishable under Article 127 of the Criminal Code. In both cases, it is not possible for a vote cast to become invalid or for an error in persona to occur.

It is clear from the above that Article 127 of the Criminal Code has common ground with the distribution of misinformation via Internet services, since both relate to the distribution of incorrect or misleading information and public harm, particularly to the election process. Since the current wording of the article is technology-neutral, it is already not limited to fraudulent acts in the physical space or through a specific medium. The examples given by Fokkens and Nan are by no means medium-bound and could also occur through modern forms of communication. For example, this reading of Article 127 of the Criminal Code prohibits the deliberate dissemination of misleading information via a social media service about,

399 Van der Woude, T&C Criminal Law, comments on article 127 of the Criminal Code.
400 Smiths II p. 63.
401 J.S. Nan, Commentary on the Penal Code art. 127 (Criminal Law) (article text valid from 01-05-1984).
402 HR 10 November 1890, W 5966.
403 Smidt II p. 62; Fokkens, Noyon/Langemeijer/Remmelink Criminal Law, section 127 of the Criminal Code, aant. 3.

for example, the voting method required, which actually leads to an invalid vote. Also the 'hacking' of a voting computer whereby clicking on candidate X is always counted as a vote for candidate Y, is prohibited by this article. The table below shows the type of situations already covered by Article 127 of the Criminal Code in the above interpretation of the article.

Situation	Criminalized under Article 127 Sr?		Disinformation?
Deliberately misinforming people online about the required voting method (pen instead of red pencil).	Yes	If the causal link can be established, this misleading information leads to an invalid vote.	Yes
Manipulating a voting computer so that if candidate X is chosen, it is registered as a vote for candidate Y.	Yes	This 'fraudulent act' results in an error in persona.	No.
Voters give fraudulent ballots at the polling station.	Yes	This 'fraudulent act' has the effect of invalidating a vote.	No.
To swap a vote cast with a ballot paper where another candidate has been voted for.	Yes	This fraudulent act' results in an error in persona.	No.
The deliberate dissemination on social media of inaccurate information about an election programme.	No.	This erroneous information cannot cause a vote to become invalid or an error in persona.	Yes
Deliberately spread online the wrong date of a vote.	No.	This erroneous information cannot cause a vote to become invalid or an error in persona.	Yes

Figure 2

In view of all these connections that are related to disinformation problems, the question is to what extent the provision should be adapted at all to include the desired 'online manipulation'. Three elements are important here: (i) the lack of clarity of the concept of 'online manipulation', (ii) the possible impact on freedom of expression, and (iii) the fact that the above extensive interpretation of the causal link has not been legally confirmed in Article 127 of the Criminal Code.

If 'online manipulation' is interpreted fairly narrowly as 'deliberately misleading expression via an Internet service that is directly causal to *or* the invalidation of a vote *or* the belief of a voter that one person has been voted for while another has actually been voted for, then this falls within the scope of the description of the offence in Article 127 of the Criminal Code. The table above shows the type of acts that are already punishable. This is, of course, a very specific reading of 'online manipulation' and this concept can also be interpreted in a much broader way. But if the description of the offence in Article 127 of the Criminal Code were to be extended, problems would arise with freedom of expression. The misleading statements that the provision makes punishable are related to the political process in which the freedom of expression under Article 10 ECHR has the most extensive protection.[404] Next, as a general rule, the dissemination of incorrect information falls under the protection of Article 10 ECHR and cannot be prohibited without further qualification.[405] Further expansion of the description of the offence would constitute a far-reaching restriction of freedom of expression.

404 ECtHR Lingens v. Austria, 8 July 1986 (No 9815/82).
405 ECHR Salov v. Ukraine, 6 September 2005. (No 65518/01).

This interpretation also depends on the more extensive reading of the causal relationship, which does not require a '*causa proxima*'. Although this reading is supported by literature, it is important to test such an extensive interpretation against freedom of expression. After all, the criminal provision is closely linked to the democratic election process and, in this extensive reading, makes expression related to this process punishable as criminal offences. As the goal is to ensure fair and free elections, one must tread carefully when restricting freedom of expression so as not to overshoot the mark. It follows from the above that 'deliberate online manipulation' to a large extent already falls under Article 127 of the Criminal Code. In summary, whether this is actually the case depends on the following points:

- **Definition of 'deliberate online manipulation':** if it is understood as a deliberate fraudulent act via an Internet service that makes a vote invalid or a voter has actually voted for a different candidate than he or she is lead to believe, then it falls under Article 127 of the Criminal Code. Any broader concept of 'online manipulation' is not covered by Article 127 of the Criminal Code and cannot, from a fundamental rights perspective, simply be included in the description of the offence.

- **Explanation of the scope of Article 127** of **the Criminal Code** In all probability, the explanation of the causal link without the causa proxima is unproblematic, but the legislator, or judiciary, have not given a definitive answer to this question.

- **Impact on freedom of expression**: an extensive interpretation of the causal link required by Article 127 of the Criminal Code is, in principle, compatible with freedom of expression, although the scope for interpretation also means that the fundamental rights boundaries must be kept in mind on an ongoing basis.

ii. Disinformation & computer intrusion

Another criminal law provision that is interesting for the problem of disinformation is computer intrusion ('*computervredebreuk*'), or the 'hacking ban'. Computer intrusion is punishable under Article 138ab of the Criminal Code. The article has been amended several times as a result of the Council of Europe's Cybercrime Convention,[406] and EU Directive 2013/40/EU, among other things. At its core, cyber-intrusion consists of the deliberate and unlawful intrusion of all, or parts of, an automated system. This 'intrusion' is an open concept that is not determined exhaustively in the first paragraph of article 138ab of the Criminal Code. At the minimum it includes (a) a breach of security, (b) a technical intervention, (c) false signals or a false key or, (d) assuming a false identity. The judiciary has been given room to adapt this concept of intrusion to the rapidly changing reality. [407] For example, the Supreme Court recently ruled that "The mere circumstance that the defendant (...) has investigated the claimant's website for vulnerabilities by means of a scan programme" is insufficient to speak of intrusion.[408]

The term 'automated system' ('*geautomatiseerd werk*') must be interpreted broadly and includes, in addition to computers, systems such as networks, telephone and fax, and social media accounts. A system qualifies as long as it is able to (i) store, (ii) process and (iii) transfer data.[409] It has been established in case law that the intrusion of part of an automated system constitutes a computer intrusion.[410] Examples include a situation in which a person is authorized to access certain data but allows himself to access or modify other data,[411] or the intrusion of a router as part of a network.[412]

406 Convention on Cybercrime, Budapest, 23-11-2001.
407 Parliamentary Papers II 2004/05, 26 671, no. 7, p. 33.
408 HR 9 April 2019, ECLI:NL:HR:2019:560.
409 Rb. Midden-Nederland 23 August 2016, ECLI:NL:RBMNE:2016:4673; Parliamentary Papers II, 2004-2005, 26 671, no. 10, p. 31; HR 26 March 2013, ECLI:NL:HR:2013:BY9718.
410 HR 26 March 2013, ECLI:NL:HR:2013:BY9718.
411 Parliamentary Papers II, 1990-1991, 21 551, no. 6, p. 30-32 (MoA)
412 HR 26 March 2013, ECLI:NL:HR:2013:BY9718.

The second paragraph of Article 138ab of the Criminal Code protects the integrity of data processing in an automated system.[413] The article reads as follows: "A term of imprisonment not exceeding four years or a fine of the fourth category shall be imposed for a computer breach if the offender copies, intercepts or records for himself or for another person data which have been stored, processed or transferred by means of the automated process in which he gained unlawful access". It is essential that the data is recorded in a sustainable manner.[414] When data are destroyed, and not only copied, Article 350a of the Criminal Code shall apply.[415] Finally, the third paragraph provides for an increase in penalties for the situation where the offender, via a public telecommunications network, makes use of the processing capacity of an automated system, or gains access to an automated system of a third party.[416]

There are a number of interfaces between the doctrine of computer intrusion and the problem of disinformation or 'online manipulation'. First of all, one could think of the scenario in which an automated system, and mainly an electronic communication service, is attacked and then disinformation is disseminated on a large scale via that system. An example of this is the KPN hack from 2012, which provided access to customer data such as name and address details, telephone numbers and bank account numbers. It is conceivable that such a hack not only provides access to customer data, but that disinformation can also be spread over these networks. A related example is the DigiNotar hack from 2011 in which more than 500 fake SSL certificates were issued and the websites of the Dutch government were temporarily declared unsafe. These two examples can be qualified as computer-related offences and are punishable as such, including the increase in the sentence under the third paragraph of Article 138ab of the Criminal Code. The distribution of disinformation by means of breaking into a network is therefore already a criminal offence.

Another possible link between the spread of misinformation via Internet services and the doctrine of computer intrusion is the use of 'bots' or fake accounts. This involves automated posting, sharing or 'liking' of messages on social media via fake accounts to help spread certain, often political, information.[417] The question is to what extent this is 'intrusion' of an 'automated system'. Article 138ab(1)d of the Criminal Code explicitly states that 'the taking of a false identity' must be seen as 'intrusion'. On the other hand, it is not immediately clear whether the creation of a false account and the automated distribution of messages should be qualified as the 'intrusion' of an automated system as it is seen more as the use or perhaps abuse of a service. However, in 2013 the Supreme Court confirmed that an account on a social media platform should be seen as an automated system.[418] It is also clear from case law that the unauthorised use of someone else's account is covered by intrusion.[419]

In essence, the problem of fake accounts is related to the 'intentionally and unlawfully' element. The fact is that the mere use of a service does not lead to unlawful intrusion, whereas unauthorised use of the services of a platform can be regarded as unlawful intrusion. In the case of the use of bots and fake accounts, the question of illegality is therefore also directly related to the conditions under which the social media offer their service. These terms of use are all the more important as there is no other form of 'security' on access to the service, and it is the only source known to the user for what constitutes legitimate use of the service.[420] This reading means that a social media service is an 'automated system', and the use of this service in violation of the terms of use constitutes 'unlawful intrusion'.

413 Parliamentary Papers II, 1991-1992, 21 551, no. 11, p. 19.
414 Parliamentary Papers II, 1991-1992, 21 551, no. 12, p. 4.
415 C.M. Gerritsma-Breur & A.G. Nederlof, Commentary on the Penal Code art. 138ab (criminal law) (article text valid from 01-07-2015).
416 C.M. Gerritsma-Breur & A.G. Nederlof, Commentary on Penal Code art. 138ab (criminal law) (article text valid from 01-07-2015).
417 See 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.
418 HR 26 March 2013, ECLI:NL:HR:2013:BY9718
419 Rb Midden-Nederland, 18 February 2019, ECLI:NL:RBMNE:2019:609.
420 Senate, session year 2005-2006, 26 671 and 30 036 (R 1784), D.

The question is to what extent the terms of use of an Internet service should actually be given such importance. This reading of the law would have far-reaching consequences and has not yet been discussed in the case law. The reading would mean that in many cases the boundary of the private law conditions of use would coincide with the criminal law norms for computer intrusion. Since these terms of use are unilaterally imposed by the Internet services and could unilaterally be modified at any time, they form a highly subjective basis for a criminalisation. This, combined with the fact that many of the internet services involved are communication and/or media services on which people depend for the maintenance of their social relations and participation in the democratic debate, argues in favour of using a more objective standard for 'intrusion' than just the terms of use. Perhaps the concept of 'normal use', derived from consumer law, can serve as a basis.[421]

It is possible that lessons can be drawn for further research from the U.S. Computer Fraud and Abuse Act (**"CFAA"),** where both criminal and private law standards have been developed with a similarly broad scope.[422] For example, the 9th Circuit Court of Appeals recently ruled that violating the terms of service by scraping information that is publicly accessible on an internet platform (in this case LinkedIn) does not constitute 'hacking' within the meaning of the CFAA, in spite of an explicit prohibition by LinkedIn.[423] Another case, brought by investigators of algorithmic processes, is still pending.[424]

iii. Disinformation & dissemination offences

A last category of criminal law standards relevant to the dissemination of disinformation via Internet services are the so-called dissemination offences. This is a category of penal provisions that form the 'culpability''*culpoze*' variants of a predicate offence, an expression offence or specifically a press offence, for which guilt is required.[425] This means that this type of penalty is not aimed at the person who intentionally commits the offence (such as, for example, making discriminatory or hate statements, or making images of sexual abuse of minors), but is aimed at the person who further disseminates this information in public and 'could reasonably suspect' that the information is punishable. This person therefore has no intention or fault of his own in relation to the original crime, but is responsible for its further spread. Specifically, within the Criminal Code, this concerns the criminalisation of the following types of expression: *lese-majeste* (Article 113 of the Criminal Code), sedition (Article 119 of the Criminal Code), group defamation, discrimination and incitement to hatred (Article 137e of the Criminal Code), depiction of sexual abuse of minors (Article 240b of the Criminal Code) and defamation, defamation and insulting of special bodies and officials (Article 271 of the Penal Code). Article 134 of the Criminal Code also contains a distribution offence, but differs from the previous articles in that there is no specific primary offence. This is because it makes it a criminal offence to disseminate information "offering to provide intelligence, opportunity or means of committing any criminal offence". Parliamentary history shows that the rationale behind these crimes is that, a printing press offence is completed at the time when it is published or revealed and that further dissemination is therefore a *new* offence.[426]

Article 137e of the Criminal Code, the offence of spreading hatred, discriminatory or group insulting statements, is particularly relevant. In 2017, the Supreme Court ruled in an important judgment that, in that specific instance, the criminal provision should be dis-applied on account violation of Article 10 of the ECHR.[427] The case concerned an antiquarian bookshop that had antique copies of Hitler's 'Mein Kampf' in its inventory. The Supreme Court emphasized that such crimes of distribution must also be tested against

421 See Section 7:23 of the Dutch Civil Code.
422 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/okjolt/vol7/iss1/2
423 United States Court of Appeals for the Ninth Circuit, 9 september 2019, no. 17-16783 (*HIQ Labs vs. LinkedIn).*
424 https://casetext.com/case/sandvig-v-sessions
425 Verkade, Text & Comment Intellectual Property, Crime of Dissemination, in stock; culpoze variant at: Copyright Act, Article 32.
426 Blacksmith II p. 46-47 & p. 401.
427 HR 14 February 2017, ECLI:NL:HR:2017:220

freedom of expression under Article 10 ECHR, and that the context of the actual distribution is very important in this respect: "In assessing this need to intervene in the freedom of expression, the special circumstances of the case are important. In this assessment, consideration may be given to the interaction between the nature of the statement or information and the potential impact of that statement or information and to the context in which such a statement or information was made or provided.[428]

These criminal provisions are very closely related to the problem of disinformation central to this research as the focus is on the distribution of criminal expressions. These criminal law standards could therefore be a starting point for regulating the distribution of illegal statements via Internet services. However, the problem is that the E-Commerce Directive's *safe harbour* offers a horizontal (conditional) exclusion of liability, which means that many Internet services are also exempt from these criminal law standards. This is, of course, only the case in so far as this service falls within the *safe harbour* and has no knowledge of the illegal nature of the information, or "acts promptly to remove the information". However, it is important to note for the further regulatory debate that Dutch criminal law is familiar with these doctrines, in which a primary offence, an expression offence, is complemented by a dissemination offence.

C. Administrative law standards

A large number of administrative law standards are relevant for the dissemination of disinformation through Internet services. The most important of these will be discussed. First, advertising regulation because of the disinformation-related problems of political advertising, and in the context of the commercial interests associated with disinformation. Second, the regulation of the financing of political parties is also discussed in the context of disinformation through political advertisements. Subsequently, the dissemination of disinformation is also related to state security and the protection of critical infrastructure.

i. Advertising regulation

The problem of disinformation is related in various ways to the regulation of advertising. More generally, the business models of many Internet services depend on the revenue generated from advertising,[429] which means that these services are designed to retain the attention of users for as long as possible in order to optimise this advertising revenue. As a result, the service may prefer sensational or 'click-bait' content, and thus use the same logic as disinformation.[430] Disinformation is more specifically also related to advertising via misleading and harmful political advertisements. As indicated in the debate on disinformation, the regulation of political advertising as a possible strategy for tackling the larger problems is currently high on the (international) political agenda.

When discussing legislation on the subject of advertising, a distinction should be made between (i) the provisions specific to political advertising, (ii) the provisions specific to both political and commercial advertising, and (iii) provisions that apply solely to commercial advertising. The latter category, although not applicable, is still discussed as these provisions may serve as an example and context for the possible regulation of political advertising. Commercial advertising is regulated at the European level, as is clearly shown in chapter 5. The e-Commerce Directive, AVMS Directive, the Unfair Commercial Practices Directive, and the Misleading Advertising Directive, all contain standards on commercial advertising, many of them transparency obligations. On the other hand, given the sensitive and national nature of the political process, the regulation of political advertising is left to the national legislators.

428 *ibid.* Ro. 3.5 having regard to ECHR 15 October 2015, ECLI:CE:ECHR:2015:1015JUD002751008 (*Perincek/Switzerland).*
429 See chapter 3.
430 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.

Political advertisements as such are not specifically regulated in the Netherlands.[431] Historically, this can partly be explained by the long-held idea that the government should keep its distance from the political process, as well as the structure and campaigns of political parties.[432] The Media Act is the only legal source that speaks specifically about political advertising. Section 6.1.1. of this Act provides that established political parties (which acquired a seat in a previous election) are allocated free airtime. This airtime is made available by the Commissariaat voor de Media (CvdM) (Dutch Media Authority) on national public service media prior to an election, and is the same for all established parties.[433] In terms of content, this airtime should be devoted to political programmes.[434] Parliamentary history still stresses that it should not be used for commercial advertising.[435] Strictly speaking, this regulation in the Media Act does not concern the regulation of political advertisements, since it does not affect the production, content or further distribution of the political communication in question. On the other hand, the provision of free airtime does increase the visibility of political parties and contributes to a level playing field. However, the introduction of this scheme should not be overestimated as political broadcasts generally have a rather limited coverage.[436]

Further, the Media Act also prohibits the sponsorship[437] of media programmes that consist of "political information".[438] This term is broadly interpreted and includes both programmes and advertisements. As regards public service broadcasting, the rationale was that sponsorship is generally not appropriate in view of the public service remit of the broadcaster.[439] In addition, the underlying idea is, more generally, to prevent the mixing of political and commercial influences and to guarantee transparency. Originally, the ban implemented Article 17(3) of Directive 89/552/EEC,[440] although the Directive did not elaborate on the ban. As far as the supervision is concerned, the CvdM is charged with the enforcement of the sponsorship ban.[441] Apart from the ban on sponsorship, the Media Act does not prevent political parties from buying commercial airtime themselves. But because of the high costs involved, the relatively small budgets and the still limited viewing figures, parties hardly do this.[442]Finally, it should be noted in that although online political advertisements do not fall under a specific statutory regulation, the civil courts have general jurisdiction. The principle of an unlawful act is so broad that it can always be invoked as a legal basis and can standardise the use or content of online political advertisements through the civil courts.[443]

In addition to the specific provisions of the Media Act that have political advertisements as their subject matter, the Media Act also regulates commercial advertisements on broadcasters. Title 2.5 and 3.2 of the Media Act contain extensive regulations that determine how often, for how long and what type of advertising is permitted.[444] Like the e-Commerce Directive, Articles 2.88b and 3.5b of the Media Act provide for transparency and an obligation to provide information for advertisements distributed via broadcasters. The CvdM is responsible for supervision.[445]

---

431 Cappello, M. (ed.), *'Media coverage of elections: the legal framework in Europe*', IRIS Special, European Audiovisual Observatory, Strasbourg, 2017, p. 83; 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: Routlegde, 2017, p. 370.

432 Evaluation and Advisory Committee for the Political Parties (Funding) Act, *'The Public Interest of Political Parties'*, 2018, p. 18-19.

433 Article 6.1 of the Media Act; Lower House of Parliament, session year 2007-2008, 31 356, no. 3, p. 73-74.

434 Article 6.4 of the Media Act.

435 Lower House of Parliament, session year 2007-2008, 31 356, no. 3, p. 73-74. See the definition of advertising in Article 1 paragraph 1 of the Media Act.

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

437 Sponsorship is defined in Article 1 as "the provision of financial or other contributions by an undertaking or a natural person not normally engaged in the provision of media services or media offerings, for the purpose of establishing or acquiring media offerings in order to promote or enable their distribution to the general public or to part of it".

438 Article 2,106 paragraph 3 under a in conjunction with 3.15 paragraph 2 of the Media Act.

439 Lower House of Parliament, 1993-1994 session, 23 752, no. 3, p. 4.

440 Lower House of Parliament, session year 1993-1994, 23 752, no. 3, p. 6. Directive 89/552/EEC has been replaced by Directive 2010/13/EU which does not include this ban on sponsorship of political programmes.

441 Article 7.11 of the Media Act.

442 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: Routlegde, 2017, p. 371-2.

443 See further section 6.

444 See for example 3.8 and 3.11 Media Act for the duration and frequency of the advertising and 3.10 Media Act for the content.

445 Article 7.11 of the Media Act.

Further, the Netherlands has various advertising bans, often included in specific sector legislation, that cover both commercial and political advertisements. These prohibitions apply regardless of the medium used. A good example is the ban on tobacco advertising as included in Section 5 subsection 1 of the Tobacco Act or the ban on advertising of prescription medicines under Section 85 of the Medicines Act. As they are generally prohibited, this type of regulation applies to both commercial and political advertisements.

ii. Financing of political parties

As stated earlier, the Netherlands has traditionally had little regulation aimed at political parties, based on the idea that the government should keep its distance from political parties.[446] The only real exception to this rule is the Political Parties (Funding) Act. This law lays down the criteria for granting subsidies and contains financial transparency obligations. Supervision is carried out by the Ministry of the Interior and Kingdom Relations; the Political Parties' Financial Supervision Commission (*Commissie toezicht financiën politieke partijen*) has an advisory role. Failure to comply with the financial transparency obligation may result in an administrative fine.[447]

This lack of regulation makes the Netherlands quite exceptional in an international context. Influential organisations such as the OSCE,[448] and GRECO,[449] have repeatedly indicated that the regulation of party financing in the Netherlands is inadequate from the point of view of combating corruption. According to these organisations, the main point of improvement concerns the transparency of party financing and expenditure.

The implementation of such transparency obligations can be highly relevant for the regulation of online political advertising. Financial transparency obligations may be used to clarify and influence the way in which political parties conduct their campaigns. The current Dutch regulation is only too general in nature to achieve this goal. It only requires transparency of revenues and debts, and not of expenditure.[450]

The existing financial transparency obligations under the Political Parties (Funding) Act mainly concern the political parties themselves.[451] They are obliged to register all their income and debts, where the data of the donor must be recorded for every gift of more than 1,000 euro. All donations received anonymously in excess of 1,000 euro must be transferred to the Ministry for this added value.[452] The parties are further obliged to submit an annual summary of their administration to the Ministry, which is then published in the Government Gazette (*Staatscourant*).[453] This overview only contains data concerning donations over 4,500 euro and debts of more than 25,000 euro. An overview of the administration must also be submitted to the Ministry between two and three weeks before each election so that the Ministry can publish it before the vote. Similarly, if an individual candidate has received donations totalling more than 4,500 euro for his political activities, this must be made known to the Minister so that he can publish it.[454]

Last year there was a discussion in the Netherlands about banning donations from abroad.[455] In 2016, a

446 Evaluation and Advisory Committee Political Parties Funding Act, *'The Public Interest of Political Parties'* 2018, p. 18-19. Annex to: Lower House of Parliament, session year 2017-2018, 32 752, no. 50.
447 Article 35-37 Financial Supervision of Political Parties Act.
448 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.
449 GRECO, *"Third Evaluation Round. Second Compliance Report on the Netherlands. Transparency of Party Funding"* 2012.
450 Article 20-23 Political Parties Funding Act.
451 The sections of political parties are excluded from the obligation of transparency (Article 24). The obligation has been reduced to apply to ancillary institutions including youth organisations and scientific institutes (Article 30).
452 Article 20-23 Political Parties Funding Act.
453 Article 15 of the Political Parties (Funding) Act.
454 Article 28-29 Political Parties Funding Act.
455 Some countries restrict foreign funding for the organisation of elections. See the country report on Canada below, which restricts certain foreign funding during elections (Elections Modernization Act 2018, section 232.4(1) - Undue influence by foreigners).

motion to this effect was adopted by the House of Representatives by a large majority,[456] and the committee charged with evaluating the Political Parties (Funding) Act also advised on the ban.[457] The government has now clearly indicated its intention to implement the ban on foreign donations, and intends to include it in a new Political Parties Act and in the meanwhile in an amendment to the current Political Parties Funding Act.[458] The idea is that donations from non-EU countries should be banned and donations from other EU countries should be made public.[459]

Although financial transparency obligations for political parties can be seen as an opportunity to get a grip on the use of digital advertisements by political parties, the current regulation does not provide for this. For this purpose, transparency about campaign expenditure is important and this aspect is lacking in Dutch legislation. It is possible that such an obligation of transparency regarding expenditure, together with the ban on foreign donations, will become part of the proposed Political Parties Act.[460] It is also relevant that political parties in the Netherlands have relatively small budgets. This has, for example, often prevented the parties from buying commercial airtime on the broadcasters or from launching online campaigns on a larger scale.[461]

iii. National security

In some cases, disinformation and the problem of improper influence on the Dutch democratic process by means of political advertisements are linked to threats to national security. This is not a new phenomenon, but has always been a factor in the provision of information as such. It involves multiple aspects. This may involve destabilising democracy in general or influencing elections and promoting and inciting terrorism or extremism in particular. Disinformation through foreign interference is central to policy-making. All measures in this area must comply with the requirements of Article 10 ECHR.

Recently, in March 2018, the Minister of the Interior and Kingdom Relations and the Ministry of Transport, Public Works and Water Management reported to the Lower House of Parliament on what is meant by undesirable foreign interference and how this will be dealt with.[462] With reference to the AIVD's (*Algemene Inlichtingen- en Veiligheidsdienst*) (General Intelligence and Security Service) annual report for 2017, an example is the clandestine political influence exerted by Russia, exploiting the vulnerabilities of open and democratic societies. In its 2018 annual report, the AIVD again warns of possible undesirable foreign interference by means of 'clandestine political influence'.[463] The AIVD also considers influence via social media in its work.[464]

Not all undesirable interference - the broader subject of the letter - concerns disinformation. Where disinformation is concerned, the government takes the view that the spread of online disinformation by state actors must be prevented. It is stated that: "The government's efforts in this regard will be focused primarily on three points: 1) improving the understanding of the scale and nature of the threat, 2) raising awareness, and 3) intensifying cooperation between the various parties that can play a role in this regard. The Cabinet further emphasises that in the search for solutions, "journalistic independence is guaranteed and respected (...)".[465] The letter elaborates on how to improve resilience, while also mentioning EU devel-

456 Motion Amhaouch c.s., Lower House, session year 2016-2017, 34 270, no. 22.
457 Evaluation and Advisory Committee for the Political Parties (Funding) Act, *'The Public Interest of Political Parties'* 2018. Annex to: Lower House of Parliament, session year 2017-2018, 32 752, no. 50.
458 Acts II, session year 2018-2019, Appendix to the Acts, no. 875; Lower House, session year 2017-2018, 32 752, no. 50; Coalition Agreement 2017-2021, '*Trust in the Future*', p. 4, Parliamentary Papers 34 700, no. 34; A bill to amend the Political Parties (Funding) Act is currently being presented in internet consultation, see: https://www.internetconsultatie.nl/wijzigingwfpp.
459 Letter from the Minister of the Interior and Kingdom Relations, Lower House, session year 2018-2019, 32 752, no. 54.
460 See also paragraph 6.C.
461 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: Routlegde, 2017, p. 371-2.
462 Parliamentary Papers II, 2018/19, No 30821, No 42.
463 AIVD annual report 2018, p. 9 ff.
464 Idem p. 10.
465 Parliamentary Papers II, 2018/19, No 30821, No 42.

opments in the field of disinformation. It also discusses the use of diplomatic instruments, such as the early identification of undesirable interference via diplomatic channels and making it possible to discuss it, but it also mentions the public accountability of a country. It is the government's preference to get involved in this with other countries.

A letter to the House of Representatives in December 2018 stated that the government considered the threat of misinformation from state actors to be a real one.[466] In addition, six other principles are used, including the primacy of constitutional values and fundamental rights, and - for the time being - trust is expressed with regard to "the own responsibility of tech companies in the form of self-regulation, with due regard for freedom of expression and freedom of the press". The extent to which these other principles relate to disinformation by state actors is not discussed in the letter. However, the threat posed by state actors is further clarified by extending it to 'actors who can be related to state actors'. This probably includes 'troll factories' that are assumed to operate by order of a foreign state actor or to be tolerated by a state actor.[467]

State-related threats are discussed again in a letter from Parliament in April 2019.[468] Again, the dissemination of disinformation is mentioned as one of the tactics in the event of undesirable foreign interference. The approach to tackling state threats is described in more detail and the earlier efforts to raise awareness of disinformation is confirmed. The annex states that a government response is justified in the event of "a threat to economic or political stability or national security posed by the interference of state or associated actors".

The National Security Strategy 2019,[469] drawn up under the auspices of the National Coordinator for Counterterrorism and Security (NCTV) (*Nationaal Coördinator Terrorismebestrijding en Veiligheid*),[470] considers disinformation to be one of the national threats that must be tackled. The dissemination of inaccurate information about elections, including through social media, is cited as an example. In this context, state threats - in line with previous documents - are primarily undesirable foreign interference. Such undesirable interference could also be of a national nature, but does not appear to be such as to give rise to prioritisation within the national security strategy.

The information provided by the government to the House of Representatives does not refer to the inadequacy of instruments or the need for further legislation on disinformation from foreign state actors. It could therefore be assumed that the existing instruments are adequate or that they will be taken into account in other new policies to be developed at national and European level. The Parliamentary documents referred to above seem to indicate the latter, in particular when - see above - reference is made to the early identification and discussion of undesirable interference via diplomatic channels, but also to the public accountability of a country. The policy described indicates that, in view of the threat to the rule of law, disinformation originating from state actors (or parties affiliated with them) represents a higher interest than other forms of disinformation. This is confirmed by the motions adopted in the House of Representatives on manipulation/foreign interference.[471]

The aspect of competences at national level, in relation to the European legal framework, plays an important role in ensuring aspects that affect national security. The European Union has no direct powers in relation to national security, and the question is to what extent other European competences are suffi-

466 Parliamentary Papers II, 2018/19, No 30821, No 51.
467 Details about the operation of the so-called Internet Research Agency in Russia, have become known through Mueller's research in the United States. See for example https://www.justice.gov/file/1035477/download
468 Parliamentary Papers II, 2108/19, No 30821, No 72.
469 Parliamentary Papers II, 2018/19, No 30821, No 81 (Annex).
470 The NCTV plays a central role in analysing and combating state threats. The tasks include the analysis of information, policy-making and the realisation of cooperation between the parties involved, see: https://www.nctv.nl/organisatie/wieisnctv/index.aspx.
471 Parliamentary Papers II, 30821, nos. 61, 63 and 68.

cient to tackle threats from state actors through disinformation without affecting national sovereignty. Finally, it is important that there is sufficient transparency regarding the way in which disinformation through Internet services is dealt with by the services concerned, in view of the possible restrictions that this may impose on freedom of expression and the requirement that restrictions must be provided for by law and be necessary in a democratic society. Relevant competencies of the services in this context are the competencies with regard to sigint (signal intelligence, eavesdropping, tapping, analysis of metadata) and osint (Open-source intelligence, collection of information from public media, via internet, social media), and the exchange of information in an international context. These powers can be found in particular in Sections 3 and 4 of the Intelligence and Security Services Act 2017.

iv. Vital/Critical Infrastructure

Increasing attention is being paid to vital/critical infrastructure and the control over it. Parts of the information infrastructure fall under the scope of the Network and Information Systems (Security) Act.[472] Telecommunications networks and elements of the digital infrastructure are covered by the law. Although the focus in this law is on maintaining basic services and preventing vulnerabilities, there is a connection to disinformation. Failure of the communication infrastructure can have major consequences, as several incidents have shown. Though, these incidents were not linked to the issue of disinformation.

At the moment, the bill 'Wet ongewenste zeggenschap telecommunicatie' (Law on undesired control of telecommunications) is before Parliament.[473] It offers the possibility to limit the control of telecommunications operators as far as the control of undertakings is concerned. The possible acquisition of KPN by a Mexican company was a direct reason for this. Public order and national security may be at stake in such takeovers, as follows from the explanatory memorandum.[474] No explicit reference is made to risks of disinformation, but it is indicated that the continuity and confidentiality of communications may be impaired.

Also not directly related to disinformation is the discussion about the ownership of Dutch newspapers, which to a large extent lies with Belgian parties.[475] The Netherlands has no special rules that restrict or prohibit the ownership of media companies. No distinction is made as to whether or not there is a controlling influence on companies from other EU countries or beyond.

D. Self-regulation

Since disinformation as a policy subject is still relatively new, the Netherlands does not have any self-regulatory instruments at national level that are specifically tailored to the problem. The self-regulatory initiatives that have been developed are mainly at European level. On the other hand, there is strongly developed self-regulation in the Netherlands with regard to advertising via the Dutch Advertising Code (*Nederlandse Reclame Code*) (NRC). Moreover, the media have their own self-regulating body: the Netherlands Press Council (*Raad voor de Journalistiek*), which plays a role with regard to disinformation in the media.

The absence of legal regulation means that, in the Dutch context, self-regulation is the main source of specific standards for political advertising.[476] The various self-regulatory codes are also very important with regard to commercial advertising. These codes generally contain higher standards, and in addition to the law, also standards that relate to the morality or social acceptability of advertisements.[477]

472 Stb 2018, 387/389.
473 Parliamentary Papers II, 35153.
474 Parliamentary Papers II, 35153, no. 3, p.1/2.
475 See for example: Aanhangsel handelingen II, 2016/17, nr. 1250.
476 Cappello, M. (ed.), *'Media coverage of elections: the legal framework in Europe',* IRIS Special, European Audiovisual Observatory, Strasbourg, 2017 p. 83, 87.
477 See, for example, article 3 of the Dutch Advertising Code: "Advertising must not be contrary to the general interest, public order or morality".

The main focus is on the Stichting Reclame Code (Advertising Code Foundation) which, as an independent organisation, is responsible for the NRC.[478] The NRC consists of a general section, applicable to all forms of advertising, and in addition to that 23 different special advertising codes that relate to advertising within a particular sector.[479] The Code is based on a very broad definition of advertising, which also includes political advertising: "any public and/or systematic direct or indirect commendation of goods, services and/or ideas by an advertiser or in whole or in part for their benefit, whether or not with the help of third parties".[480] The NRC does not have a specific definition of "an advertiser" and the text of the code itself does not provide much more than a circular definition. See, for example, Article 19 of the NRC, which refers to an advertiser as "an organisation or institution that advertises".[481]

A large number of interest groups and professional groups are affiliated,[482] and participate in the so-called Platform of Participants (*Platform van Deelnemers*), which has an influence on the adoption of the codes.[483] In addition to the voluntary affiliation of organisations such as the Dutch Advertisers' Association and the Dutch Cosmetics Association, under the Media Act all media organisations that provide advertising are required to adhere to the Code.[484] None of the organisations that fall under the definition of Internet services as discussed in chapter 2 is a member of the NRC. The dominant Internet services, on the other hand, are affiliated with the previously discussed *EU Code of Practice against Disinformation*,[485] which mainly provides for transparency obligations. Given the international nature of the services offered by most Internet companies, the possibility of European coordination and the fact that the Internet companies themselves cannot be regarded as advertisers, it is unlikely that these Internet companies will join the NRC in the context of Dutch self-regulation.

As far as enforcement is concerned, the NRC is not binding and there are no formal legal consequences for non-compliance.[486] The Code does, however, provide that the Dutch Advertising Commission (*Nederlandse Reclame Commissie*), can make decisions ("recommendations") on the basis of complaints about specific cases. Although there is no obligation to do so, the Advertising Code Foundation states that 96% of the recommendations of the Advertising Code Commission are followed.[487] Of particular relevance to this study is that the Advertising Code Commission is not limited in competence in disputes involving a party to the code. The Commission is also empowered to make recommendations in the event of the involvement of an Internet service which is not a member of the Code.[488] However, the standards of the various advertising codes apply in principle only to advertisers and not to the Internet service providers that are relevant to us. Internet companies can therefore only be addressed by the Advertising Code Commission if they act in the capacity of advertiser. This does not alter the fact that 'advertising power' can also be significant on social networks. When important advertisers withdraw or threaten to withdraw, this can have a major impact.

In terms of content, different transparency obligations and a ban on misleading advertising are at the heart of the advertising codes.[489] In addition, there are a large number of general standards relating to the social acceptability of advertising. For example, advertising must comply with 'good taste and

478 Article 2 of the Articles of Association of the Advertising Code Foundation NL01-000131.00001/JS.
479 See https://www.reclamecode.nl/nrc/
480 Article 1 Dutch Advertising Code.
481 See for example also article 2b Advertising Code Social Media & Influencer Marketing: Advertiser is the one who stimulates the Distributor to make and/or publish Advertising via Social Media and/or the one who makes advertising by placing it on social media and/or by editing or having edited statements on social media.
482 See: https://www.reclamecode.nl/over-src/organisatie/
483 Article 6 in conjunction with Article 10 of the Articles of Association of Stichting Reclame Code, NL01-000131.00001/JS.
484 Article 2.92 in conjunction with Article 3.6 of the Media Act.
485 See paragraph 5.F.
486 Second Chamber, 2000-2001 session, 27 619, no. 3, p. 9-10.
487 Annual Report of the Advertising Code Authority 2017 p. 32.
488 Second Chamber, 2000-2001 session, 27 619, no. 3, p. 9-10.
489 Cappello, M. (ed.), *'Media coverage of elections: the legal framework in Europe',* IRIS Special, European Audiovisual Observatory, Strasbourg, 2017 p. 83.

decency',[490] it must not be 'unnecessarily offensive' or contrary to 'good morals'.[491] With regard to political advertisements, the Advertising Code Commission has indicated that, in view of the great importance of freedom of expression in political statements, a cautionary test should be carried out.[492]

In addition to this general code, the special advertising code relating to "Social Media & Influencer Marketing" from 2019 is also relevant. This code is aimed at advertisers as well as 'disseminators', those who advertise for an advertiser via social media in return for payment or other consideration.[493] The disseminators are therefore the influencers, bloggers and vloggers who spread the advertising via social media. In terms of content, the code consists of three aspects, all of which are very relevant to the problem of disinfection: (i) transparency obligations, (ii) prohibition of fake accounts and (iii) a duty of care on the part of the advertiser. The first substantive obligation, in Article 3 of the Code, contains well-known information and transparency obligations, whereby advertising must be recognisable as such. A special feature of this obligation is that the 'relevant relationship' between the distributor and the advertiser must be made clear. This is "the relationship between the Advertiser and the Distributor aimed at distributing Advertising via Social Media (or having it distributed), against payment or any other advantage, that may influence the credibility of advertising via Social Media".[494] There must therefore be both the possibility of an advantage and the possibility of a loss of credibility. The code provides detailed examples of how this relevant relationship can be made clear, for example by means of hashtags ('#adv' or '#spon') or indicating what the distributor has received compensation. The Advertising Code Commission recently issued an interesting recommendation based on this obligation. This was a Facebook video by Jan Roos in which he opposes the introduction of neutral cigarette packets. However, he did not mention that the film was sponsored by the tobacco industry, which in the Commission's view constituted a breach of the information obligation.[495]

The code then contains a ban on manipulation, which, like the obligation of transparency, is closely in line with the European consumer regulation for commercial advertising.[496] Interestingly, Article 4(d) of the Code explicitly prohibits "the systematic creation and/or use of false/non-existent identities in bulk to report on a product and/or service via social media". This implies a ban on the use of fake accounts, trolls and bots and therefore has very clear interfaces with the spread of disinformation, which is often done using these techniques. This prohibition is linked in the explanatory memorandum to the general obligation, also arising from European law, to clearly state the identity of the advertiser. After all, when using bots, people are misled about the identity of the advertiser. Thirdly, the code provides a duty of care for the advertiser to ensure that the distributor complies with the advertising code.[497] The concept of 'relevant relationship' and the duty of care are particularly interesting additions to the existing European law framework for commercial communication from the point of view of the disinformation issue.

In the past year, the Commission has made several pronouncements in response to complaints about political advertisements. It was claimed that advertisements from the Forum for Democracy, the Labour Party, and the Party for the Animals, among others, contained incorrect or misleading information.[498] In all cases, the complaints have been rejected and the Commission has been cautious in its assessment.

490 Article 2 Dutch Advertising Code.
491 Article 3 Dutch Advertising Code.
492 Stichting Reclame Code, 30 October 2012, 2012/00789B. See also, for example, a discussion of various matters relating to political advertising 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.
493 Article 2 Advertising Code Social Media & Influencer Marketing 2019.
494 Article 2 d Advertising Code Social Media & Influencer Marketing 2019.
495 Advertising Code Commission, 16 October 2019, no. 2019/00571, https://www.reclamecode.nl/uitspraken/influencer/tabak-2019-00571/255894/.
496 See Chapter 5.E 'Disinformation and commercial regulation'.
497 Article 6 Advertising Code Social Media & Influencer Marketing 2019.
498 Advertising Code Committee 5 June 2019, 2019/00333; Advertising Code Committee 27 March 2019, 2019/00204; Advertising Code Committee 27 March 2019, 2019/00201/A; Advertising Code Committee 13 March 2019, 2019/00157.

Two statements explicitly stated that t was not up to the Advertising Code Commission to prohibit a political party from referring to points from its election programme and the arguments it puts forward in ideological advertising, even if many are found to be incorrect, as long as the way in which this is done remains within the limits .[499]

Although the Dutch Advertising Code is the main source of substantive standardisation, it appears that this form of self-regulation does not offer many points of departure for this study either. The cautious assessment of the Advertising Code Commission and the fact that the Code is in principle not aimed at internet companies means that in practice the Code lacks a great deal of impact with regard to political advertisements.

In addition to the NRC, there is also the Netherlands Press Council (*Raad voor de Journalistiek*) in the field of self-regulation. The Netherlands Press Council is a self-regulating body for the media. The core task of the Press Council is to shape self-regulation. The Dutch Press Council is able to help victims if the medium itself does not comply with the injured party's requests.[500] The Press Council publishes non-binding conclusions.

The Press Council rules on the basis of the Guidelines of the Press Council 2018 (**"Guidelines")**[501]. The Guidelines were presented in 2007, and have since been revised four times. The Guidelines focus on good journalism. Good journalism has a number of characteristics: it is true, accurate, impartial, fair, verifiable and honest.[502] The responsibility of the journalist is central to the Guidelines. Although the Guidelines are primarily aimed at journalists and journalistic organisations, the Dutch Press Council also encourages other parties involved in journalism to follow the Guidelines. The Guidelines contain a number of provisions that are relevant to disinformation, such as the obligation to state the source and to make a clear distinction between facts, statements and opinions.[503] There is an exception for columnists, cartoonists and reviewers: they are free to exaggerate. Another relevant provision in the context of disinformation is the provision that visual material may not be used to illustrate a different subject or context from that for which the images were created. In addition, image manipulations must not be misleading and interventions that bring about a clear change in the image must be reported to the reader and viewer.[504] In the case of responses submitted which contain serious allegations, the editorial board of a news medium should investigate whether there is a factual basis for the allegation.[505]

On 18 March 2019, the Netherlands Press Council published a conclusion on the complaints against the *Gelderlander* and the *AD* newspapers.[506] The complainant argued that an article conceals disinformation as news facts. It was claimed that the article contains numerous errors of fact. The Dutch Press Council concluded that by publishing the sentence "FIOD conducts research", it was careless, since the article did not provide any insight into the research conducted and the available source material. The journalist had heard from trustee source that an FIOD (*Fiscale Inlichtingen en OpsporingsDienst*) (Fiscal Information and Investigation Service) investigation was taking place, but in the article the existence of the investigation was presented as an established fact. The Dutch Press Council concluded that the information on which

499 Advertising Code Committee 27 March 2019, 2019/00204; Advertising Code Committee 27 March 2019, 2019/00201/A.
500 https://www.rvdj.nl/over-de-raad.
501 Guidelines of the Netherlands Press Council, 2018, available at https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae.
502 Guideline of the Netherlands Press Council, 2018 via https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae, p. 2.
503 Guideline of the Netherlands Press Council, 2018 via https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae, p. 4.
504 Guideline of the Netherlands Press Council, 2018 via https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae, p. 5.
505 Guideline of the Netherlands Press Council, 2018 via https://www.rvdj.nl/uploads/fckconnector/bd261851-faaa-46f9-80ba-00d9d5d761ae, p. 6.
506 Council of Journalism, conclusion number 2019/16 via https://www.rvdj.nl/2019/16

it is based was insufficiently transparent and verifiable for readers, so that the reporting can be qualified as unbalanced. On 19 March 2019, *De Gelderlander* complied with the advice of the Netherlands Press Council and published the conclusion.[507]

On 24 October 2019, the Dutch Press Council published a conclusion on misleading headlines.[508] JOOP, the online opinion page of BNNVARA, had published an article entitled "Dutch psychologist again pulls Nazi science out of the closet".[509] In the introduction of the article it is mentioned that the psychologist praises the intelligence of Nazi leaders. The headline and the introduction gave rise to the erroneous suggestion that the psychologist was engaged in Nazi science, according to the Dutch Press Council. A headline may contain "an enlargement of the content of the corresponding article". This means that the boundaries of journalistic care are only exceeded if the headline is not justified in the article. "The Press Council concludes that the journalist and JOOP have acted negligently.[510]

In addition to the Guidelines, the Netherlands Press Council also has a code of professional ethics, the Code of the Netherlands Press Council ("**Code**"). The most recent version of the Code has been in force since September 2019. The Code has been updated as a result of digitisation and the social attention paid to 'fake news'.[511] The Code contains separate articles on truthful messages and independent information. These provisions include a ban on the deletion or distortion of essential information.[512] The public may not be misled in any way by image processing or archival material that is not recognisable as such.[513] In addition, a journalist must make a clear distinction for the public between factual reporting and comment.[514]

On 7 June 2018, the chairman of the Netherlands Press Council announced research on improvement. According to the chairman, the reason for this research was s the spread of disinformation: "Self-regulation can make clear the difference between good and bad journalism, between journalists who take themselves and their audience seriously and who do not", according to the chairman of the Dutch Press Council. [515]

Finally, with regard to journalistic developments in the field of disinformation, the Journalism Fund has granted a subsidy to DROG, an organisation whose aim is to inform citizens about deception and polarisation due to disinformation.[516] DROG focuses mainly on young adults.[517] DROG has developed, among other things, the *Bad News game*, which can be used to play a game about disinformation for free via slechtnieuws.nl.[518]

E. National political developments

The possible regulation of disinformation has been the subject of public debate for some time now, and in recent months, in addition to this, the regulation of political advertisements has increasingly been on the political agenda. The following is an overview of the most important recent political developments in this area, some of which are the immediate cause for this report.

507 https://www.gelderlander.nl/nijmegen-e-o/uitspraak-raad-voor-journalistiek-over-klacht-nijmegenaar-jankie~ac33758d/
508 Press Council, conclusion number 2019/46 via https://www.rvdj.nl/2019/46
509 https://joop.bnnvara.nl/nieuws/nederlandse-psycholoog-trekt-opnieuw-nazi-wetenschap-uit-de-kast; https://joop.bnnvara.nl/over-joop
510 Press Council, conclusion number 2019/46 via https://www.rvdj.nl/2019/46
511 https://www.rvdj.be/nieuws/herwerkte-code-met-oog-voor-fake-news-en-digitalisering
512 Article 3 Code of the Netherlands Press Council, p. 9 via https://www.rvdj.be/sites/default/files/pdf/code-rvdj.pdf
513 Guideline to article 3, Code of the Netherlands Press Council, p. 14 via https://www.rvdj.be/sites/default/files/pdf/code-rvdj.pdf
514 Article 4 Code of the Netherlands Press Council, p. 9 via https://www.rvdj.be/sites/default/files/pdf/code-rvdj.pdf
515 https://www.rvdj.nl/over-de-raad/berichten/sterkere-raad-voor-de-journalistiek-is-nu-meer-dan-ooit-nodig
516 https://wijzijndrog.nl/
517 https://www.svdj.nl/nieuws/drog-wil-jonge-mensen-immuun-maken-voor-desinformatie/
518 https://wijzijndrog.nl/serious-game-over-propaganda

i. Report of the State Committee on the Parliamentary System

Of importance is the *Staatscommissie Parlementair Stelsel* (Parliamentary System State Commission), which completed its report '*Lage drempels, hoge dijken*' ("Low thresholds, high dikes") in December 2018.[519] Four of the Commission's recommendations are specifically relevant to this study.[520] Firstly, the Commission proposes that political parties should be obliged to report on the digital campaign instruments they use. The second and third recommendations concern the introduction of a transparency obligation for digital political advertisements under the supervision of an independent regulator. Fourth, the Commission recommends that an independent organisation be appointed to report on the influence of algorithmic classification of political information on online platforms.

More specifically, the Commission recommends that the transparency obligation should include how much money is spent on digital advertisements, on which groups these advertisements are aimed, and on the basis of which data these groups were selected. The Commission also recommends that a limit be set on the percentage of advertisements that are only aimed at a specific group, and that the other advertisements should be displayed in a non-targeted manner.[521] In addition, users of social media must be able to see quickly and easily whether it is a paid advertisement, and who the party behind it is. The Commission also asks for clarity for users about whether, and if so on what basis, advertisements are targeted at them.[522] All of this would be supervised by a new independent regulator to be created. The Commission bases this recommendation partly on the Commission recommendation of September 2018 discussed in chapter 5.[523]

With regard to the role of algorithmic ordering of user-generated information on internet platforms, the Commission notes that algorithmically-driven recommendations favour certain political views.[524] The recommendation that an independent organisation should monitor and report on this mainly serves to gain more insight into this practice. The Commission offers this as a possible solution to the current far-reaching information asymmetry between the Internet companies on the one hand and the government and society on the other hand. Also in a scientific context, the question of the accountability and measuring the dynamics of internet platforms, from the point of view of social impact, is also in the spotlight.

Following the report '*Lage drempels, hoge dijken*' ('Low thresholds, high dikes'), the Cabinet published a Cabinet position in June 2019.[525] The government acknowledges that the report rightly refers to digital risks to the democratic process, such as the loss of voter autonomy through micro-targeting.[526] The government endorses the recommendation to impose statutory conditions on micro-targeting.[527] The Cabinet aims to include such legal conditions in the Political Parties Act.[528] The Cabinet considers the creation

519 Staatscomissie 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. See also: Voerman, G., '*De positie van de politieke partij in het eindrapport van de staatscommissie Parlementair stelsel*', 2018 https://www.denederlandsegrondwet.nl/9353000/1/j4nvih7l3kb91rw_j9vvkl1oucfq6v2/vkurgjfwa8x4/f=/bijdrage_gerrit_voerman.pdf

520 Staatscomissie parlementair stelsel, '*Lage Drempels, Hoge Dijken. Democratie en rechtstaat in balans*' Den Haag 2018, par. 6.4.2 - 6.4.5.

521 Idem, par. 6.4.2.

522 Idem, par. 6.4.3.

523 European Commission, *'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.

524 Idem, par. 6.4.5 based on Hazenberg, H. and others, '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. There is an international discussion on the access of scientists to relevant data from social media companies for research into the impact on democratic processes. See, for example, this recent report from the Social Science Research Council in the US on the difficulties encountered in this context in making the data available to researchers. SSRC, Statement from Social Science Research Council President Alondra Nelson on the Social Media and Democracy Research Grants Program, 27 August 2019, https://www.ssrc.org/programs/view/social-data-initiative/sdi-statement-august-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.

of a separate, independent regulator to be a realistic option in the event of a substantial expansion of duties.[529]

ii. Law on Political Parties

As a result of the above-mentioned report of the *Staatscommissie Parlementair Stelsel* (Parliamentary System State Commission),[530] and the opinion of February 2018 of the *Evaluatie- en Adviescommissie Wet financiering politieke partijen* (Evaluation and Advisory Commission on the Financing of Political Parties Act), discussed in chapter 6.B.,[531] the government has indicated its intention to introduce a new Political Parties Act.[532] The government states that its objective is to further strengthen the independent position of political parties, including by clarifying the legal position of political parties. The Political Parties Act will contain transparency obligations for political parties.[533] The aim is to include in this law the recommended transparency obligations for political parties with regard to digital political campaigns and micro-targeting.[534] The Political Parties Act will provide for a coherent regulation that is currently lacking, with the exception of the Political Parties Funding Act and the Elections Act. [535] The Political Parties Act will include the Political Parties Funding Act and amend parts of the Elections Act. The law will also include a ban on donations from outside the EU to Dutch political parties.

In February 2018, the Evaluation and Advisory Committee on the Financing of Political Parties Act (the Veling Commission) published a report entitled '*Het publieke belang van politieke partijen*' ('The Public Interest of Political Parties'). This report shows, among other things, the government's reluctance in connection with the view of the appropriate distance that the government should maintain.[536] During the preparation of the Political Parties Act, the recommendations of the Veling Commission were examined.[537] These are the recommendations made by the Veling Commission have not yet been taken into account in the revision of the Political Parties (Funding) Act.[538]

iii. Motions

Asscher and Buitenweg

In the context of the Provincial Council elections, on 7 February 2019 the House of Representatives members Asscher and Buitenweg tabled a motion on digital political advertisements. The petitioners want a guarantee from Facebook that there will be full transparency about the disseminators of political advertisements on the platform.[539] The motion was adopted by a majority of 22 votes.

The government responded by letter of 19 February [540] referring mainly to the European self-regulatory code. The motion was partly implemented by means of the ongoing implementation of the *Code of Practice on Disinformation*. The affiliated platforms, including Facebook, would now indicate the sender, the amount paid for each political advertisement in the EU, and the number of people who saw the advertisement. As indicated in chapter 5.D, the Code defines political advertisements fairly narrowly as being directly related to a specific election or election candidate.[541] These advertisements are then placed in a

529 Kamerstuk 34 430, nr. 10 F, p. 12.
530 Staatscomissie 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.
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 Motion by Asscher en Buitenweg, Lower House, 2018-2019 part-session, 35 078, no 21.
540 Lower House of Parliament, session year 2018-2019, 35 078, no. 26.
541 Article 3-4 EU Code of Practice on Disinformation.

public database.[542] However, an investigation by the civil rights organisation Bits of Freedom last May shows that Facebook is not yet able to identify a political advertisement as such, and then apply the right measures.[543]

In addition to these self-regulation measures, the Minister's response to the motion also refers to the forthcoming Political Parties Act and the possible regulations contained therein with regard to political advertisements.[544]

Motion Asscher and van der Molen

On 13 March 2019, Members of Parliament Asscher and van der Molen tabled a motion on the criminal law standards for deliberate online manipulation[545]. The motion was amended on 19 March 2019.[546] The only change to the motion concerned the addition of 'among other things' to the observation that 'among other things' social media companies have too often violated rules with regard to online manipulation. The motion calls on the government to investigate whether current descriptions of criminal offences can be extended to include deliberate online manipulation. The motion relates to situations in which, for example, the message is distributed digitally that the election will not take place or will take place on a different date.[547]

The current Article 127 of the Criminal Code mainly relates to fraudulent acts in relation to the ballot paper.[548] The current Article 129 of the Criminal Code regulates, among other things, the prevention of voting, such as the misappropriation of ballot papers, the opening of a ballot box or the manipulation of a voting machine.[549] Article 129 of the Criminal Code protects the inegrity of elections and their outcome.[550]

Motion Kuiken and Verhoeven

In a motion of 25 June 2019, unanimously adopted by the Lower House of Parliament (*Tweede Kamer*), Member of Parliament Kuiken and Verhoeven asked the government to investigate the possibility of introducing "a legal obligation of transparency for political advertisements on online platforms".[551] The motion by MPs Kuiken and Verhoeven builds on the transparency recommendation of the *Staatscommissie Parlementair Stelsel* in the aforementioned report "*Lage drempels, Hoge dijken*".

iv. Awareness campaign

On 16 November 2017, MPs Verhoeven, Van der Molen, Middendorp, Kuiken and Van der Graaf requested the launch of an information campaign "to raise awareness of the influence of state actors on internal affairs and democratic processes in the Netherlands"[552]. In addition, following a motion by MPs Westerveld and Van den Hul, discussions on media literacy were held with Mediawijzer.net, the Royal Library and the Association of Dutch Municipalities (Koninklijke Bibliotheek en de Verenging van Nederlandse Gemeenten), among others. These discussions have shown that a coherent approach to media literacy is desirable.[553] Between 11 March and 23 May 2019, the Ministry of the Interior and Kingdom Relations,

542 Tweede Kamer, vergaderjaar 2018-2019, 30 821, nr. 74, p. 3; European Commission, *Code of Practice on Disinformation. Intermediate Targeted Monitoring - March report*s , 23 April 2019, https://ec.europa.eu/digital-single-market/en/news /third-monthly-intermediate-results-eu-code-practice-against-disinformation. See further chapter 5.F.
543 NOS, *'Bits of Freedom: 'Facebook gaat de fout in met politieke advertenties'*, 20 May 2019 https://nos.nl/nieuwsuur /artikel/2285561-bits-of-freedom-facebook-gaat-de-fout-in-met-politieke-advertenties.html.
544 Lower House of Parliament, 2018-2019, 35 078, no. 26, p. 2.
545 Motion Asscher- Van der Molen, Lower House, session year 2018/19, 30821, no. 60.
546 Amended motion by Asscher and Van der Molen, Lower House, 2018/19 session, 30821, no. 68.
547 https://zoek.officielebekendmakingen.nl/h-tk-20182019-62-5.pdf
548 Noyon/Langemeijer/Remmelink Criminal Law, section 127 of the Criminal Code, aant. 2 ; HR 10 November 1890, W 5966.
549 Smidt II, p. 64; Noyon/Langemeijer/Remmelink Criminal Law, section 129 of the Criminal Code, aant. 1a.
550 Van der Woude, *'T&C Criminal Law, commentary on article 129 of the Criminal Code', 2019*, Wolters Kluwer.
551 Motion by Kuiken and Verhoeven, Lower House, 2018-2019 session year, 32 761, no. 145.
552 House of Representatives, 2017-2018 session year, 34 775 VII, no. 21
553 Lower House of Parliament, session year 2018-2019, 35000-VIII, no. 91, p. 26.

ran the awareness-raising campaign '*Blijf nieuwschrierig. Blijf kritisch*' ('Stay curious. Stay critical"[554]. On the website *blijvenfkritisch.nl* citizens can find practical tips. The campaign, which consists of radio commercials, and online videos, is part of a broader improvement in media literacy. The website *blijftkritisch.nl* also have, among other things, a checklist '*Is die informatie echt*?' ('Is that information real?').[555] With this checklist, citizens themselves can verify whether information is genuine, for example by investigating sources. The website explicitly states that it is not the task of the government to judge the (in)accuracy of information. Finally, the Consumer and Market Authority (Autoriteit Consument en Markt) and the Dutch Media Authority stated that they would take stock of the possibilities for new initiatives to increase media literacy.[556] The regulators have identified the following risks: suppression of quality news, impoverishment of news offerings, and dilution of the media sector.[557] Minister Ollongren wrote that the coalition agreement has made extra resources available for the strengthening of investigative journalism.[558]

v. Mediawijzer

The *Mediawijzer* initiative is part of the Media Literacy Network (*Netwerk Mediawijsheid*), which also includes*Mediawijsheid.nl* and *HoeZoMediawijs.nl*.[559] The mission of the Media Literacy Network is to make the Netherlands media literate.[560] According to Mediawijzer, media literacy is a collection of competencies that are necessary to be able to participate actively and consciously in the media society.[561] The website of Mediawijsheid has a separate section entitled ' Nepnieuws' ('Fake News').[562] The Media Literacy Network is managed by: the Nederlands Instituut voor Beeld en Geluid (Netherlands Institute for Sound and Vision), the ECP, Human, Kennisnet and the Royal Library.[563] In 2017, disinformation was discussed as part of the Media Literacy Week, organised by Mediawijzer.[564]

vi. NL DIGIbeter 2019

The "NL DIGIbeter 2019: Agenda Digital Government" is part of the Dutch digitisation strategy and is an annually updated document.[565] The NL DIGIbeter 2019 pays attention to public values, among other things. The Ministry of Justice and Security has commissioned an investigation into algorithmic decision-making.[566] This research is carried out by Utrecht University.[567]

The Strategic Action Plan for Artificial Intelligence is in line with the Dutch digitisation strategy 2018.[568] The Strategic Action Plan for Artificial Intelligence, as part of Track 3, includes the continued protection of public values and human rights.[569] The action plan does not discuss how any automatic decision making could affect news in general or disinformation in particular. The report does, however, point out that freedom of expression can be restricted in the case of, for example, the ordering of search results and algorithms that remove content without human intervention.[570]

554 see also: Lower House, session year 2018-2019, 30 821, no. 51, p. 5.
555 https://www.rijksoverheid.nl/onderwerpen/desinformatie-nepnieuws/checklist-tips-tegen-nepnieuws-desinformatie
556 ACM & CoM, '*Digitisation and fake news: a joint exploration of the Consumer and Market Authority and the Commissariat for the Media', 2018,* p. 13; see also Commissariat for the Media: statutory ZBO evaluation, p. 28 via https://zoek.officielebekendmakingen.nl/blg-877381
557 House of Representatives, 2018-2019, 30 821, no. 51, p. 2.
558 House of Representatives, 2018-2019, 30 821, no. 51, p. 2.
559 https://www.mediawijzer.net/over-ons/.
560 https://www.mediawijzer.net/onze-missie/.
561 https://www.mediawijzer.net/van-mediawijzer-net/competentiemodel/.
562 https://www.mediawijsheid.nl/nepnieuws/.
563 Idem.
564 McGonagle, T. et al., '*Inventarisatie methodes om "nepnieuws" tegen te gaan "'*, Institute for Information Law, 2018, p. 65.
565 NL DIGIbeter 2019: Agenda Digital Government, p. 5.
566 NL DIGIbeter 2019: Agenda Digital Government, 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 *Strategic Action Plan for Artificial Intelligence'*, p. 10.
569 *Strategic Action Plan for Artificial Intelligence'*, p. 6.
570 *Strategic Action Plan for Artificial Intelligence'*, p. 41.

vii. Minister Dekker

In a debate of 19 February 2019 in the Senate, the Minister for Legal Protection made a number of promises regarding the regulation of political advertisements in response to a question from MP Duthler. Minister Dekker has promised "to map out the effects of mirco-targeting and to look at the opportunities, but above all at the risks that this entails for specific values and individual freedoms", in which the international components will also be involved.[571]

viii. Letter from Minister Ollongren

On 18 October 2019, Minister Ollongren wrote a letter to the House of Representatives informing it of the policy on misinformation.[572] The letter states that the democratic state under the rule of law needs better protection in terms of digital risks.[573] The Minister writes this in response to the motion by members Middendorp and Verhoeven. [574] The letter discusses the three lines of action of the disinformation strategy: prevention, strengthening the information position and response.[575] The emphasis is on the preventive action line, which in turn consists of four pillars: strengthening the resilience of citizens, increasing the resilience of political office holders, increasing transparency and maintaining a pluralistic media landscape.[576]

F. Overview of national legislation

The wide range of legislation and regulations reviewed in this chapter, as well as in chapter 5, shows the diversity and breadth of the relevant regulatory landscape. The different legal provisions relevant to the problem of disinformation cut across the traditional jurisdictions. This increases the complexity of the problem, as the three general areas of law - private law, criminal law and administrative law - all have their own normative and procedural framework. The various private, criminal and administrative law standards discussed in this chapter are as follows:

Private law	Criminal law	Administrative law
Unlawful act (unlawful press publication)	Offences relating to expression (e.g. libel, slander, slander, hate speech, insult)	Advertising regulation (media law)
	Election offences (including Article 127 of the Criminal Code)	Political Parties Funding Act
Intellectual property rights	Computer crime (Article 138ab of the Criminal Code)	National security
	Dissemination offences (e.g. Article 57e of the Criminal Code)	Critical infrastructure

Figure 3

A first observation from this overview is that at national level the legislation relevant for disinformation mainly relates to the content of a statement. In addition, it is also clear that a large number of forms of disinformation are already regulated. The standards of private and criminal law then have in common

571 Senate, session year 2018-2019, no. 19, item 9, p. 19-20; Senate, session year 2018-2019, no. 19, item 11, p. 25.
572 Lower House of Parliament, session year 2019-2020, 30821, no. 91.
573 House of Representatives, 2019-2020, 30821, no. 91, p. 3.
574 Lower House of Parliament, session year 2019-2020, 30821, no. 63.
575 Lower House of Parliament, session year 2019-2020, 30821, no. 91, p. 2; see also https://www.rijksoverheid.nl/actueel/nieuws/2019/10/18/kabinet-zet-in-op-transparantie-in-strategie-tegen-desinformatie
576 Lower House, 2019-2020, 30821, no. 91, p. 6.

that they are often very context-specific. Especially with regard to tort, the concrete application of these standards is very complex and context specific, which has led to a very nuanced and balanced jurisprudence. The same applies when an expression has to be considered as a protected satire and when not. Criminal law standards that touch on disinformation are also diverse and highly context-sensitive. The legal qualification of offences relating to expression and the associated dissemination offences are highly dependent on the specific context. This considerably complicates the possible regulation of disinformation, as it means that in such cases the legal qualification is difficult to make.

The various relevant self-regulations, mainly the National Advertising Code and the Netherlands Press Council, were also discussed. Both provide an extensive framework of standards that also addresses, among other things, potential disinformation disseminated in the context of commercial advertising or news. Finally, an overview is provided of the various national political developments that are relevant to the regulation of disinformation. This clearly shows that the field is in flux and that new legislation on the financing of political parties is to be expected.

7. Synthesis

- Countries have implemented a broad range of responses to disinformation, including media literacy programmes, media funding, national security strategies, legislation prohibiting disinformation, legislative imposing duties of care on online platforms, legislation targeting foreign influence, legislation on bot and automated software
- Regulation of political advertising cannot be expected to solve many of the challenges related to disinformation
- Current legal and policy framework for the regulation of disinformation and political advertising in the Netherlands involves laws and policies at three interrelated levels: EU, national legal and policy level, and private sector policy level

A. Disinformation

i. Country studies and policy examples

The country studies below survey how a number of countries (UK, France, Germany, Sweden, US and Canada) have approached the issue of disinformation carried or facilitated by internet services. There have a been a range of approaches.

First, governments have implemented new **media literacy** programmes, and increased funding for current programmes, in order to ensure users of internet service are more resilient to disinformation (see e.g. Canada, France, UK, Sweden). These programmes also involve major internet services, and indeed, in France, the media regulator (*Conseil Supérieur de l'Audiovisuel*) has a new legal obligation to monitor internet services' implementation of measures to promote media and information literacy. The UK also has proposals for a new regulator to have responsibility for online media literacy and monitoring the spend by internet services on media literacy programme. The Swedish government also tasked the Swedish Media Council with a new media literacy programme in order to counter disinformation. Other examples would include the Canadian government's funding of its new Digital Citizen Initiative, which is a is a multi-component strategy that aims to support democracy by building citizen resilience against online disinformation. These measures align with the recommendations of the four special international mandates on freedom of expression, the European Commission, and Council of Europe, that strengthening media literacy is one of the best bulwarks against disinformation.[577]

Second, governments have implemented new **media funding** programmes. For example, the UK government injected government funding (18 million pounds) to strengthen independent media and counter disinformation and fake news across Eastern Europe and the Western Balkans. The Swedish government, through the Swedish Innovation Authority, has also injected funding (13.5 million krona) into a new digital platform designed to prevent the spread of false news stories online.

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, par. 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.

Third, disinformation has also been considered by governments in the context of **national security**.[578] For example, the Swedish government treats disinformation as a national security issue, and combatting disinformation during elections is part of the Swedish government's National Security Strategy. In addition, Sweden's Civil Contingencies Agency has published a 50-page handbook on *Countering information influence activities*. Similarly, the United States treats disinformation as a national security issue. It enacted, which allocated $120 million in funding to the US State Department to create an agency 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.

Fourth, certain countries have specific laws which **prohibit disinformation** or false information. The best example is France, which has a specific law which prohibits publication of false news, which has been criminalised for many years under its 1881 Freedom of the Press Law. And the most relevant new French legislation for internet services is the 2018 Manipulation of Information Law, where a court can order an online platform to remove "inaccurate misleading allegations or imputations of fact", which may "alter the sincerity of an upcoming vote", and are "disseminated deliberately, artificially or automatedly", and on a massive scale. The first court judgment under the provision clarified that the content must be sponsored content i.e. the payment of third parties to artificially broaden the dissemination of information, and content promoted using automated tools such as bots.[579] Further, Canada prohibits the publication of certain false statements about a political figure with the intention of affecting the result of an election.

Fifth, governments have imposed, or are planning to impose, new legislative **duties of care** on internet services to implement measures to combat disinformation. In this regard, France has imposed a new duty of cooperation on large internet services, while there are proposals in the UK and Canada to legislate for imposing similar duties of care. For example, under Title III of the 2018 Law on Manipulation of Information, on certain online platforms to fight the dissemination of false information that is likely to disturb public order or to alter the sincerity of certain elections. The legislation *requires* platforms to put in place certain mechanisms to allow users to report false information, and also includes measures platforms may put in place, such as promoting content from certain media companies. The French media regulator (*Conseil Supérieur de l'Audiovisuel*) provides additional guidance on these measures, and platforms are required to report the measures to the regulator. Apart from the French example, there are two similar proposals in the UK and Canada, to create a new regulatory framework in order to tackle illegal and harmful content online, including disinformation. The central element of the proposals would be to impose a new statutory duty of care on certain internet services to take 'reasonable steps' to keep users safe and tackle illegal and harmful activity. In relation to disinformation, internet services would be required to take 'proportionate and proactive measures' to minimise the spread of misleading and harmful disinformation, and crucially, 'increase the accessibility of trustworthy and varied news content'. Crucially, the statutory duty of care would be enforced by an independent regulator, and the regulator would set out how internet services would fulfil their legal, duties through new codes of practice. Notably, the regulator would have considerable enforcement powers, including fines, and possibly the power to block platforms, as an enforcement option of last resort.

Sixth, a further specific policy option that emerges from the country studies is new legislation which imposes an obligation on online platform to remove **manifestly unlawful content** within 24 hours of receiving a complaint, where unlawful content includes a number of current criminal offences which

578 See, Rosenberger, L. & Hanlon, B. 'Countering Information Operations Demands A Common Democratic Strategy' (Alliance for Securing Democracy, 2019), https://securingdemocracy.gmfus.org/countering-information-operations-demands-a-common-democratic-strategy/.

579 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).

apply to false information: such as defamation, intentional defamation, insult, defamation of religions, and dissemination of propaganda material. This system has been put in place in Germany, through the widely discussed NetzDG legislation, and it also provides that platforms must remove or block access to "all unlawful content" within seven days. The German legislation makes it a regulatory offence to contravene the law, and regulatory fines of up to 5 million euro may be imposed on platforms.

Seventh, some countries have legislation targeting **foreign influence**, and has been used to prosecute foreign groups engaging in disinformation.[580] For example, in the United States, campaign finance law prohibits foreign nationals making contributions or expenditures on certain elections, and prohibits individuals, groups and parties from making an expenditure, independent expenditure, or disbursement for certain electioneering communication. Similarly, in Canada, recent legislation has been enacted on foreign influence of elections. The Elections Modernization Act prohibits foreign individuals, companies, groups, parties or governments, unduly influencing electors, by incurring any expense to directly promote or oppose a candidate or party in an election.

Eighth, there has also been new legislation and proposals on **bot and automated software regulation**. For example, in California, it is now unlawful 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. However, there is no duty placed on online platforms to ensure user disclose the use of bots. In this regard, there is a proposal at federal level in the United States (Bot Disclosure and Accountability Act) to regulate the use of bots on social media. This proposal would put social media providers under an obligation to implement procedures to require users to publicly disclose the use of any automated software programme intended to impersonate or replicate human activity online. The US consumer protection agency – the Federal Trade Commission – would be tasked with defining bot software and ensuring compliance with the law.

These policy examples may be summarised as follows:

1. *Media literacy*: media literacy programme to counter disinformation. Possible obligational on a regulator to implement online media literacy programme, and a possible obligation on internet services to promote media literacy online.

2. *Media funding (enabling environment for media)*: funding programmes to support independent media, and well-resourced public service media. As the Council of Europe recommends, the media should have the resources at all times to fulfil their task of providing accurate and reliable reporting on matters of public interest, as quality journalism and reporting are key tools in countering propaganda and disinformation.[581]

3. *Code of practice*: self-regulatory code of practice (or co-regulatory code by government minister or regulator) on tackling harmful content on internet services, including disinformation. The code would set out procedures for reporting and removing harmful content and disinformation. Code would be adopted in consultation with stakeholders and civil society (e.g. UK).

580 https://www.justice.gov/file/1035477/download; https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html.

581 Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership, Section 1.4, Appendix.

4. *Statutory duty of cooperation*: statutory duty of cooperation, focusing on requiring certain processes and structural elements be in place. This duty is imposed on platforms to implement measures to fight the dissemination of false information that is likely to disturb public order or to alter the sincerity of certain elections. Specific measures set out in code of practice issued by regulator (e.g., France).

5. *Statutory duty of care*: statutory duty of care imposed on platforms to take reasonable measures to ensure users are safe and tackle illegal and harmful activity, including disinformation. Specific measures set out in code of practice by regulator, and regulator would have power to issue fine, and seek court-ordered removal of service (e.g., UK).

6. *Platform obligation to remove illegal content*: impose an obligation on platforms to remove reported illegal content under the Dutch Criminal Code that applies to false information, such as insult, defamation, incitement to hatred, (e.g. Germany).

7. *Court-ordered removal of disinformation:* court procedure to order platforms to remove false or misleading information during election-time, with time limits for procedures e.g. 48 hours (e.g., France).

8. *Bot software regulation*: impose an obligation on internet services to implement procedures to require users to disclose the use of any automated software programme; or make is an offence to use a bot on a social network with the intent to mislead people about its artificial identity for the purpose of knowingly deceiving the people about content of the communication in order to influence a vote in an election (e.g. California).

9. *Prohibit publication of false information:* new criminal offence of the publication of false or misleading information (e.g. France).

10. *Prohibit under foreign influence*: prohibit foreign individuals, groups, parties and governments from spending money on elections (e.g., United, Canada).

11. *National security*: treat disinformation as a national security issue, as part of a national security strategy (e.g., Sweden, United States).

ii. Election oversight and disinformation

The European Commission has emphasised how disinformation during elections requires "particular attention".[582] In this regard, it is helpful to refer to the role of the OSCE, which monitors and observes elections throughout Europe, including elections in the Netherlands. The OSCE's report on the 2017 Parliamentary Elections makes a number of recommendations in relation to election oversight, foreign and anonymous donations, the right to appeal election results, and standards under international good practice for free and fair elections.[583]

First, the OSCE noted that Dutch law does not provide a mechanism for parliament's final decision on election results to be appealed to a judicial authority, which was "inconsistent with OSCE commitments and international good practice".[584] Second, the OSCE noted that foreign donations are allowed, and that "contrary to good practice", anonymous donations of up to 1,000 euro are permitted. The Council of

582 European Commission, *'Tackling online disinformation: a European Approach',* p. 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.

Europe has also recommended that States should specifically limit, prohibit or otherwise regulate donations from foreign donors.[585]

Further, in relation to oversight of elections, the European Court of Human Rights has held that it has the competence to review whether elections have been free and fair. This flows from Article 3 of Protocol No. 1 to the European Convention on Human Rights, which places COE member states, including the Netherlands, under an obligation to hold free elections "under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature".[586] Indeed, the ECtHR has held that "as a matter of principle", it has competence to review whether media coverage of elections, and specifically, manipulation of the media, resulted in elections not being free and fair.[587] The ECtHR also emphasised that member states have a positive obligation of a "procedural character" to ensure a domestic system for effective examination of individual complaints and appeals in matters concerning electoral rights.[588] In the case, the ECtHR, the Court found that complaint about unequal media coverage of the elections had been examined by an independent body, and a reasoned judgment was given, and as such, the system of electoral appeals put in place was sufficient to comply with the State's positive obligation.[589]

While the ECtHR has not (yet) considered complaints about online coverage of elections, the above standards do suggest that an important element to ensure elections are protected from online disinformation, would be to establish a proper mechanism to ensure an independent appeal body or court can review whether an election has been free and fair. The Venice Commission's Code of Practice in Electoral Matters provides that the body must have authority over proper observance of election campaign rules and the outcome of the elections, and to annul elections where irregularities may have affected the outcome.[590] This mechanism would provide an important check to review whether online disinformation was so pervasive as to lead affecting the outcome of an election. Of course, this would be an ex ante mechanism, and proactively protecting election against disinformation is an important approach too. However, an effective mechanism to review elections, and the role of online disinformation, is equally important.

iii. Political advertising and disinformation

The issues of disinformation and the regulation of political advertising are related, but from a legal perspective, different issues. In particular at the EU level, they have been somewhat lumped together in relevant policy documents, in the way that updating the regulation of political advertising through internet services will also address the problems of disinformation. Notably, however, the two main independent reports from the EU and Council of Europe on disinformation hardly mention political advertising. The Council of Europe report mentions political advertising only once,[591] while the EU's High-Level Group's report mentions that one possible vulnerability for elections, among many, is non-transparent dissemination of political advertisements.[592] From the outset, it should be acknowledged that there is still a lack of empirical evidence of the problem of disinformation through political advertising, and whether regulating political advertising will actually have any effect on the scale of disinformation. Related to this, the European Commission writes that 'most known cases' of disinformation have involved 'written articles, sometimes complemented by authentic pictures or audiovisual content taken out of context'.[593]

585 https://rm.coe.int/16806cc1f1.
586 Article 3 of Protocol No. 1 to the European Convention on Human Rights.
587 Communist Party of Russia and Others v. Russia (Application no. 29400/05) 19 June 2012, par. 79.
588 Ibid., par. 124.
589 Ibid., par. 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.
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, par. 2.2.

One reason for the shift in focus from regulating disinformation as such, to regulating political advertising, may be that regulation of political advertising is considered more feasible and acceptable. Originally the problem of disinformation was discussed as a problem of 'fake news'. However, independent reports from the EU and Council of Europe, pointed out the misleading and inadequacy of this concept, considering it a 'mechanism by which the powerful can clamp down upon, restrict, undermine and circumvent the free press'.[594] Warnings followed from international special rapporteurs on the dangers associated with attempting to regulate 'fake news'.[595] Given that many of the dangers associated with such regulation still exist in relation to regulating varies forms of disinformation, a narrower focus on political advertising has emerged as a more specific regulatory target.

This latter point is borne out by evidence in the country studies, included in the appendix. France is the only country that has passed specific legislation targeting disinformation (indeed, France has also for many years criminalised publication of false news under its criminal code). Other countries are discussing new legislative frameworks for disinformation, for example the UK government's White Paper on Online Harms.[596] The UK proposal involves a new statutory duty of care on internet services to tackle harm caused by content or activity on their services, overseen by an independent regulator. The proposal includes the more novel issue of disinformation but targets the full breadth of illegal and harmful information online. Commentators have warned for the potential negative impact on freedom of expression "[i]f platforms are required to prevent potentially harmful content from being posted, this incentivises widespread prior restraint".[597]

In contrast, there have been a number of examples of legislation targeting political advertising – in Canada, France, Scotland, United States (California, Maryland, New Jersey, New York, Nevada, and Washington). This regulation has mainly focused on ensuring (different forms of) transparency (see also Section 7.C below). And yet, the regulation of political advertising, in particular requirements of transparency, only cover a very specific part of the problems related to disinformation.

In light of this relationship between the problems of tackling disinformation and the question of legal frameworks for political advertising, it is helpful to summarize the problems related with disinformation identified by the European Commission, and how political advertising transparency might impact on these problems:

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

594 HLEG, *'A multi-dimensional approach to disinformation'*, p. 10; Wardle, C., & Derakhshan, H. '*Information Disorder. Toward an interdisciplinary framework of research and policymaking*', z.p., 2017 p. 5.

595 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",* 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 Killock, J. & Shepherd, A., *'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/.

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]

Coupled with these problems, internet services, according to the Commission, facilitate the rapid and widespread dissemination of disinformation through different mechanics:

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]

It is clear from the above the potential harms from disinformation are quite serious for a democratic society, and that the mechanics of internet services can heighten the potential dangers associated with disinformation. However, regulating political advertising, especially when restricted to political advertising for political candidates in the narrow sense, will not address the problems associated with (a) algorithms, or (b) digital advertising models. The effect of regulating political advertising on (c) technology-enabled amplification, which is facilitated by bots, fake accounts and astroturfing, is dependent on how broad a definition of political advertising is deployed. Restricting particular forms of political advertising, however, could potentially increase problems in other areas.

Crucially though, the major difficulty with regulating political advertising is that while it may be abused to engage in the spread of disinformation, it can be a legitimate method of political communication that has been used for many years to inform the public. Further, modern political campaigns (and many grassroot campaigns) use the technology-enabled amplification methods offered by internet services for perfectly legitimate campaigning in a democratic society. And finally, regulating paid for political advertising more strictly can easily lead to a shift from sponsored communications to organic content strategies, which implies that looking at paid political advertising cannot easily be looked at in isolation. These points must be borne in mind when considering the regulation of political advertising. A further reason to tread carefully is the lack of strong empirical evidence demonstrating widespread use of political advertising to spread disinformation in the Netherlands.

In view of this, this report details the legitimate reasons underlying and the proper policy options that are available for a more effective regulation of political advertising on internet services, while situating this question in the broader discussion of the tackling of disinformation online. It's important to keep in mind, however, that the regulation of political advertising cannot be expected to solve many of the challenges related to disinformation. Moreover, restrictions on political advertising have to be carefully assessed in their effectiveness, as there are other ways in which money can fund the effective distribution of political communications through internet services than through specific channels for sponsored communications.

598 European Commission, *'Tackling online disinformation: a European Approach'*, COM(2018) 236 final.
599 Idem, par. 2.2.

B. Policy levels for regulating disinformation and political advertising

The current legal and policy framework for the regulation of disinformation and political advertising in the Netherlands involves laws and policies at three interrelated levels:

- The European legal framework for relevant internet services and business practices related to online communications generally and (political) advertising. This legal framework consists of relevant EU laws (including limitations on liability for intermediaries, transparency requirements for commercial communications, direct marketing regulation in electronic communications, a distinct set of obligations on audiovisual media services, and data protection law). In addition, it involves the protection of fundamental rights in the EU and Council of Europe context, the right to freedom of expression in particular. It's notable here that the EU is also a leading forum for self- and co-regulation involving internet services with respect to disinformation, and also involving transparency about political advertising.

- The national legal and policy level in the Netherlands, involves the implementation and enforcement of European level frameworks, involving a number of independent regulators, including ACM, het Commissariaat van de Media and de Autoriteit Persoonsgegevens. Of special relevance for the Dutch legislative agenda are areas related to disinformation and political advertising that remain the core or sole competency of the Netherlands, including the functioning of elections and national security.

- The private sector policy level, which consists of the design and offering of amplification and rapid-dissemination tools for disinformation, and political advertising opportunities, in the context of internet services. This policy level includes associated definitions and policies of relevant companies, including through contractual terms, industry self-regulation, disclosures and enforcement.

As clearly follows from chapter 5 and 6, even though there is an extensive range of different laws applicable, there are no specific regulations pertaining to online disinformation and online political advertising on a national level in the Netherlands. In relation to online political advertising, the country studies illustrate that together with Sweden, the Netherlands stands out in the relative lack of regulation concerning political advertising in general. We do not consider this to be the result of a slow response to new dynamics of media and technology developments. The Netherlands is a country that historically does not have much regulation on political advertising, with Sweden deregulating political advertisements via broadcasting only a decade ago (see the study on Sweden in the annex).[600] This lack of regulation can be, at least partially, explained by the notion, dominant in the Dutch political system, that the government should refrain from interfering with political parties and the political debate in society.[601] Particular forms of regulation as well as co-regulation can create a danger that internet services are incentivized to restrict political communications in ways that unduly restrict political expression and harm pluralism. This danger also exists in relation to ongoing developments at the EU level and should be critically monitored from this perspective, and the requirement that interferences with freedom of expression should be prescribed by law.

However, the study has also clearly shown that there does exist a broad range of different regulations that apply to various aspects of online disinformation, and online political advertising, in various ways. This legal framework is mainly characterized by its diversity and its inclusion of many different fields and instruments of law. This relevant legal framework for the legal status and governance of online

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 Evaluation and Advisory Committee for the Political Parties (Funding) Act, *'The Public Interest of Political Parties',* 2018, p. 18-19.

disinformation, and political advertising, that emerged from chapter 5 and 6 can also be viewed through the lens of the following substantive legal areas:

1. The fundamental rights framework, freedom of expression in particular;
2. The generally applicable content-related restrictions on expression and distribution of online content in private and criminal law;
3. Criminal law provisions related to the security and integrity of information systems (cybercrime);
4. Self-regulation relevant to disinformation and (political) advertising, including the 'Nationale Reclame Code' and self-regulation with respect to journalism;
5. Limitations on liability for intermediary service activity;
6. Self- and co-regulatory instruments on a European level involving internet service responsibilities, including the EU Code of Practice on Disinformation;
7. Restrictions on direct marketing through electronic communications services;
8. The regulation of the collection and use of personal data in online manipulation, microtargeting and (political) advertising;
9. Audiovisual media (services) law;
10. Regulations pertaining to (commercial) advertising, including transparency requirements, only some of which currently apply to political advertising;
11. National security law;
12. Transparency and oversight in political party finance law;

Categorising the relevant legal framework analysed in this report in this way is especially helpful for assessing which areas can be addressed on a national level. There are several areas in which the Netherlands has the possibility of creating legislation addressing (parts of) the problems addressing online disinformation and online political advertisements. For example, area 2 regarding the generally applicable content-related restrictions on expression in private and criminal law consists of national law, even though the outer boundaries are formed by the fundamental rights framework. Additions or changes to this general framework on a national level could possibly have a large impact on online disinformation and online political advertising. Such changes, however, should be considered from the perspective of disinformation and illegal and harmful content online more generally, and not on the basis of the related but distinct issue of political advertising.

The European Commission is working on a major overhaul of the general framework for the liability of internet intermediaries (area 5, and related area 6). The scope of the hosting safe harbour, the status of (political) advertising under such rules, internal market mechanisms such as the Country of Origin principle and content moderation and notice and action standards will all be a part of this. The revision of the ECD may also involve a revision of the transparency requirements on commercial communications in ways that further clarifies the obligations of internet services to clearly distinguish organic from sponsored communications. The liability and responsibility of internet services for third party communications and activities, including disinformation and political advertising, should be placed against the background of these rules and developments.

The self-regulation instruments on a national level (area 4) also fall squarely within national policy level. Which is especially relevant considering that self-regulation is the dominant form through which disinformation and political advertising is regulated in the Netherlands. In relation to internet services, however, it's important to note that such self-regulation is not specifically informed or tailored to the specific situation of the Netherlands. This can be considered a distinct regulatory challenge that maps to the much broader challenge of ensuring internationally operating internet services are responsive to particular local impacts of the use of their services.

Another area that is regulated on a national level is national security law (area 11), given the fact that the EU has no legislative competence in this area. In the same vein political party finance law concerns national political party and should be regulated on the national level (area 12).

Finally, much of the EU legislation is made in the form of directives that are in need of national implementation or Regulations that also require oversight and enforcement. This gives the national government, and relevant regulators in the Netherlands room for a specific interpretation that fits properly into the national context. Some Dutch regulators have started to explore the area of political advertising from their perspective, such as the AP, but these actions remain in their infancy and could be served by better coordination and the bundling of relevant expertise and resources.

C. Country studies and policy examples

The country studies below detail how there has been some new legislation targeting political advertising carried by internet services. A number of points must be made here. First, the legislation mainly concerns amendments to *election* legislation (e.g. France's Electoral Code, or California's Political Reform Act), and many of the new rules are *limited to election-time*. It is not the case that legislation has been enacted that regulates political advertising generally outside of election time. Even France's legislation, which is the most far-reaching, only applies in the months prior to an election.

Further, the legislation mainly concerns the protection of elections, rather than protection against disinformation. Otherwise, the regulation would not be limited to election periods. This also explains why some of the legislation only concerns political advertising targeting a political candidate or party, rather than to political advertising on a matter of public interest (sometimes called issue-advertising). Third, there is a broad range of regulation, from no rules, disclosure rules, to a prohibition on paid political advertising. The most common type of regulation consists of transparency requirements.

An analysis of existing laws and regulations with respect to paid political advertising, including through the country studies, illustrate a number of policy options that are available ranging from disclaimer rules, to a total prohibition of paid political advertising:

1. Transparency rules focusing on who paid for an advertisement (see France, Scotland, California, and Maryland). These rules could be imposed on the person posting, such as in California, where political ads require a disclaimer on who paid for it. Or the rules can be imposed on internet services themselves, such as in Canada.
2. Transparency rules focusing on personal data used in targeting of an advertisement (see France). These rules can be imposed on internet services, such as France's 2018 Law on Manipulation of Information, which requires transparent information for users on the use of personal data in the context of sponsored political content.
3. Transparency rules focusing on obligations to archive political advertising (see Canada, California, Maryland). Under Canada's Elections Modernization Act, internet services are required to publish a registry of all partisan advertising messages and election advertising messages. One can also imagine a non-public retention obligation for relevant services.
4. Campaign finance rules focusing on obligations to report spending on online campaigning (see UK and Canada). This option may target political parties and campaign groups, rather than internet services. It can bring transparency to the spending by groups that engage in astroturfing and paying staff to engage in amplification.[602]

602 See also: Benkler, Y., '*Election Advertising Disclosure: Part 1*', Harvard Law Review Blog, 31 October 2017, https://blog.harvardlawreview.org/election-advertising-disclosure-part-1/.

5. Campaign finance rules prohibiting foreign spending on election-time advertising (see Canada). This option can target foreign individuals and groups, and can also be applied to internet services. Canada's Elections Modernization Act prohibits selling advertising space (including online platforms) for election advertising to foreign parties, groups or governments.
6. Prohibiting paid political advertising during election-time (see France). France's Electoral Code prohibition on paid political advertising during election-time extends to online communication.
7. Prohibiting paid political advertising during election-time and outside of election-time. This option only exists in national rules on broadcasting.

When determining whether these different policy options could possibly be implemented in the Netherlands, the following perspectives have to be taken into account.

Before the different policy instruments can be assessed on their merit it is necessary to establish the exact problems these measures will be employed to address. There is a relatively broad consensus, also in the Netherlands, that a lack of transparency in political advertising is an issue that should be looked at and addressed. At the same time, it is as of yet not thoroughly empirically established to what extent there is a problematic situation with respect to political advertisements in the Netherlands; and whether the current (lack of) legislation with regard to online political advertising, including the lack of specific rules on transparency, forms a pressing problem. Even so, specifically for political advertising during election-time, international freedom of expression standards suggest that governments implement (narrowly tailored) transparency measures on paid political advertising.[603]

And the mere possibility that political advertising is used for the distribution of disinformation, or the possibility that paid political advertising is used without clarity about who is paying to influence voters in Dutch elections, can be considered a problem. Seen in a broader context of the debate about dependencies on digital infrastructures,[604] policy measures that are aimed to ensure a readiness to deal with threats to democracy in the area of political advertising (and disinformation more generally) may well be warranted. Such measures should be considered in view of the broader need to address the existing information asymmetries of governments and regulators in relation to relevant internet services. Currently, the Dutch government's information position with respect to the new dynamics facilitated by a handful of dominant internet services and the societal impacts thereof, appears hampered by fragmentation (in addition to the complexity of the underlying phenomenon). Academic research and journalistic investigations into the democratic impact of internet services run into considerable constraints in what information is legally (made) available. These are broader problems, however, that call for a broader discussion and set of solutions.

Given the importance of free political debate and the extensive protection offered to political speech, the impact of any possible policy option on the right to freedom of expression should be thoroughly investigated. From the perspective of subsidiarity and proportionality connected to Article 10 ECHR this also means giving preference to measures that do not touch the content of political advertisements or risk harming pluralism in the Dutch media environment. Transparency rules are one such content-neutral measure. However, even transparency rules must be narrowly targeted, framed in a sufficiently clear manner, and proportionate. The overarching freedom of expression consideration must be to ensure that any such measures, if deemed necessary, must be precisely drawn to mitigate any risk of (self-) censorship which may affect democratic debate.

603 La Rue, F., '*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression'*, Human Rights Council, A/HRC/26/30, 2 July 2014, par. 82, https://undocs.org/A/HRC/26/30.
604 See in particular the recent WRR report *'Preparing for Digital Dislocation'*, September 2019.

It's thus crucial to stress that political advertising and paid political communications generally, is a form of political expression. Political advertising cannot be regulated in the same way as commercial advertisements. Whereas the possibilities of restricting commercial communications are more plentiful, the regulation of political advertising has to adhere to a stricter freedom of expression regime. Political advertising has been mostly left to the market and self-regulation. The media and advertising service environment contain many more de facto, voluntary restrictions on political advertising than for commercial communications, the regulation of which is more solidly anchored in relevant consumer protection and media laws.

The distinction between the regulation of political and commercial advertising is also relevant in the interplay between the national and European policy level. In effect, political advertising opportunities through internet services are governed by a range of existing legal frameworks tackling different aspects. A significant part of the regulatory gaps and issues that do exist are under active consideration at the EU level.

Whereas the harmonization of laws related to commercial communications follows logically from the project of the European single market, there is no robust tradition for the regulation of political advertising at the European level. The connection of political advertising in the narrow sense to (national) elections is one part of the explanation for this. For political advertising in the broad sense, the diversity of political and democratic cultures throughout Europe also imply that the EU would ideally continue to play a supporting and facilitating role. Such role is needed, in particular, considering the proliferation of online political advertising through online services that do not neatly map to national or European boundaries.

Finally, the Netherlands has no relevant history of regulating political advertising and this long tradition of unhindered campaigning for political parties, civil society groups and individuals has to be taken into account when considering regulating online political advertisements moving forward. Introducing relatively restrictive regulation such as already in place in countries with a longer history of political advertisement regulation (e.g. France) seem an unwarranted departure from this tradition.

With this in mind the following picture emerges: option 4 and 5 might be suitable for implementation in the Netherlands, options 1 and 3 are better addressed at an EU-level and options 6 and 7 are too restrictive for the Netherlands. Options 2 lacks urgency considering the applicability of the GDPR and the independent regulatory oversight by the Autoriteit Persoonsgegevens. The main challenge in this area is in ensuring that relevant authorities have the capacity and expertise to make such oversight is effective and up to date with respect to new developments.

Policy option 4 consists of creating campaign finance rules focusing on obligations to report spending on online campaigning. It is directed at the national political parties and is as such best implemented at the Dutch national level. Transparency in spending by political parties on online advertisements offers the possibility of more insight into the extent of the practice and of democratic control on its use. The measure presents a minimal deviation from the current regulatory context given the fact political parties are already under the obligation of keeping a detailed administration and reporting regularly to the government.[605] It also forms a minimal restriction on the freedom of expression. All of these factors indicate that the creation of transparency requirements for political parties in the Netherlands with regard to their spending on online political advertisement would form a good fit with the current regulatory landscape and could offer valuable insight into the actual use of online political advertisements. In sum, this report

605 See Article 21 of the Political Parties (Funding) Act.

offers support for the advice of the commission on the Dutch parliamentary system and the intention of the government to implement such transparency requirement in the 'Wet op de Politieke Partijen'.[606]

In the same vein, parts of policy option 5 could be implemented in the new law. As discussed in chapter 6, the government is already planning on introducing a ban of foreign gifts to political parties in the revision of the 'Wet financiering politieke partijen'. Extending the ban to prohibiting foreign spending on election-time advertising in general can be considered too big a step for the Dutch situation coming from no regulation at all. The activity of foreign actors in national elections partly reflects a world in which many political issues are of a transnational nature. It is also not established that foreign spending in Dutch election poses a substantial problem warranting a ban. Similarly, policy options 6 and 7 also form too big a step for the Netherlands given the strict and extensive regulation these policy options would introduce. Here too, it is not clear that such an extensive restriction on the freedom of expression is proportional in the Dutch context.

606 House of Representatives, session year 2018-2019, 32 752, no. 54; House of Representatives, session year 2018-2019, 34 430, no. 10, p. 10-12. State Mission Parliamentary System, "*Low Thresholds, High Dykes. Democracy and the rule of law in balance*' The Hague 2018, appendix to the House of Representatives, session year 2018-2019, 34 430, no. 9.

8. Summary and conclusions

A. Context & research assignment

The spread of disinformation has become an increasingly clear concern in recent years, also in the Netherlands. It is important to contextualise this concern briefly. A number of structural causes have contributed to this phenomenon. For example, the social debate and the related information and communication has increasingly shifted to channels where there is neither any (or even the possibility of) active control by relevant services of the content and integrity of communication, nor of the processes and actors involved. Apart from the questions that arise with regard to the functioning of editorial media and journalism, the functioning of internet services raises questions. Business models can lead to the retention of user attention outweighing journalistic, scientific or similar quality and integrity criteria for information and communication aimed at public debate. In addition, Internet services will generally aim to offer their services on the widest possible scale and to address any social damage with the lowest possible investment.

Part of the problem lies in the far-reaching new possibilities for influencing the public offered by Internet services, including new channels of communication and data-driven opportunities. It is clear that this relatively open media and communication landscape also offers new opportunities for undue influence by domestic as well as foreign, including state, actors. After all, the cause of disinformation cannot only be located only in economic or technical factors. This is because it is partly due to the social processes facilitated by disinformation, including a strong polarisation of the political playing field, and communication behaviour that can be qualified as undemocratic.

This has led to a political call for more clarity on the regulatory framework for the dissemination of disinformation, resulting in this investigative study. This investigation has been based on seven research questions submitted by the Ministry of the Interior and Kingdom Relations, with questions ranging from very general to very specific, but all essentially related to questioning and studying the existing legal framework. It was commissioned in the context of the government's broader policy to protect democracy against disinformation, that is based on the values and fundamental rights of the rule of law, including freedom of expression and freedom of the press. The main objective is "to protect the stability and quality of our democratic legal order and our open society, including freedom of expression and of the press".[607] The research questions submitted are as follows:

1. What current laws and regulations are aimed at/related to preventing the dissemination of (dis) information, and specifically for/by tech companies?
2. What are the legal and regulatory requirements for the dissemination of information? Are these techniques independently described?
3. How do current laws and regulations take into account the transparency of the origin of information on social media platforms? Are there limits set on possible foreign influences, e.g. with regard to the placing of political advertisements (Asscher/Vd Molen motion)?
4. What supervisory possibilities and sanctions do the laws and regulations on online manipulation offer (Asscher/Vd Molen motion, 62)?
5. Could deliberate online manipulation be brought under the criminal law offences of election manipulation? (motion Asscher- Van der Molen, Parliamentary Papers II, 2018/19, 30821, no. 68).

607 Lower House, 2019-202, 30 821, no. 91 Parliamentary letter 'policy efforts to protect democracy against disinformation'.

6. What significance does the legal form have for the measures that technology companies can or should take with regard to content moderation, the promotion of transparency and the protection of citizens' rights? What is the responsibility of tech companies for distribution via their search engines, social platforms, etc.?
7. How are citizens' rights protected against deliberate misleading information? As well as in the context of the use of personal data (privacy) and freedom of expression (also with regard to the removal of content).

These questions and the way in which this report has addressed them require clarification. For example, this report uses the definition of disinformation as formulated by the European Commission as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm". It was decided to follow this broad European definition, rather than the narrower definition by the Dutch government, as this broader definition lends itself better to a comprehensive analysis of the evolving legal framework on disinformation. Subsequently, instead of the term 'tech companies', this study uses the term 'Internet services' to analyse the legal framework for companies that play a relevant role in the dissemination of (dis)information. This involves a wide range of different services, including social media, search engines and communication services, including *direct messaging services*. In legal terms, these are information society services, so-called *hosting services* with limited liability, electronic communications services or audiovisual media services.

In the following, we first consider the way in which the research questions have been answered. The conclusions for each chapter is discussed, followed by deeper explanations of these conclusions and lastly, ending with recommendations for this report.

Question 1 essentially asks for an overview of the legal framework applicable to (dis)information, and in particular, when disseminated via Internet services. **Question 2** is closely related to the first question. Where question 1 calls for an overview of the relevant legislation, question 2 focuses primarily on the content of this legislation. The analysis carried out shows, firstly, that there is no legislation or regulation in the Netherlands that specifically deals with disinformation, as is the case in France, for example. Secondly, the legal framework that does apply is very broad and it intersects with the classic areas of private law, criminal law, and fundamental law protection. It also includes various sector-specific legislation, including media and telecommunication law. Where personal data is used in the distribution of (dis)information, the right to the protection of personal data also applies. An overview of the relevant legislation is given in Chapter 4 (constitutional framework), Chapter 5 (European legislation, as well as Dutch implementation) and Chapter 6 (national legislation). This overview always includes the question of the legal position of different types of Internet services, as well as the question of the liability and responsibility of so-called Internet intermediaries for unlawful and/or harmful content.

Question 3 focuses more specifically on the existence of transparency obligations for social media services regarding the origin of information. There are several legal transparency obligations, mainly pertaining to commercial communications. These are standards that focus on the primary source of the information, which are discussed in chapters 5 and 6. Chapter 4 also considers in detail the possibility of transparency requirements from the perspective of freedom of expression and the protection of pluralism. Subsequently, the general laws and regulations with regard to foreign influences and national security are discussed in Chapter 4 and Chapter 6.C. Question 3 focuses on political advertisements, where there is currently no Dutch regulation on the transparency of political advertisements. Chapter 5 delves into the relevant self-regulation agreed at European level by a number of social media providers, where this type of self-regulation includes rules on transparency regarding the origin of political advertisements. Chapter 7 discusses in detail the various options for transparency obligations for political advertisements based on the country studies.

Question 4 focuses on the monitoring and enforcement possibilities with regard to online manipulation. The term is understood to mean surreptitiously influencing someone's decision making by technological means. Question 4 is therefore in line with questions 1 and 2 on the relevant legislation for the dissemination of (dis)information and its content. During the discussion of the various legal standards in Chapters 5 and 6, the relevant enforcement and supervision options were discussed in each case. The enforcement regimes are as broad as the legal framework, as the legal framework cuts across private, criminal and administrative law. Specifically, with regard to "online manipulation", the ACM and the AP as supervisors are relevant.

Question 5 focuses on a specific sanctioning possibility for (political) deception in an electoral context through the criminal law protection of the integrity of the electoral process. Chapter 6.B discusses the current criminalisation of online manipulation in the context of article 127 of the Criminal Code, article 138ab of the Criminal Code and the various offences of dissemination.

Question 6 examines whether the type of service and the business form of an Internet service affects the legal responsibilities with regard to disinformation. In Chapter 3, the various Internet services were discussed on the basis of the relevant legal definitions, the relevant earning models and the enforcement modalities with regard to the dissemination of (dis)information. Sections 5 and 6 then indicate, where relevant, the type of service to which they apply when the standards are discussed.

Finally, **question 7** focuses on the protection of citizens against disinformation. The fundamental legal framework, with freedom of expression in particular, has been dealt with in detail in Chapter 4. In addition, the question of how to protect users' rights has been explicitly addressed in Chapter 5, inter alia, when discussing the Electronic Commerce Directive, the General Data Protection Regulation and consumer law.

As indicated in the introduction, given the breadth and diversity of the research questions, it was decided to follow the structure of the legal framework in the study. Within this structure, the research questions have been answered through the course of the report. The results of the research can be summarised per chapter as follows.

B. Summary & conclusions

The conceptual framework of disinformation in **chapter 2** shows the breadth and complexity of the problem. It can be seen that the concept lends itself mainly to the marking of a new policy area and not as a demarcated legal category. A first complicating factor are the various actors involved in the process of disseminating disinformation: the creator or client of the disinformation, the Internet service through which the information is (further) disseminated and the public receiving and further disseminating the disinformation. A second layer of complexity is that there is not one type of source of disinformation. Disinformation can be created by state actors, political parties or, for example, individual internet users. A third complicating factor is that disinformation cannot be divided into one legal category. It includes illegal, unlawful, as well as permitted but potentially harmful expressions. Furthermore, of even greater relevance, is that the occurrence of harmful effects mainly happens when disinformation is disseminated on a large scale as a result of socio-technical processes. A final complicating element is that disinformation occurs in a variety of contexts, such as news, *hate speech*, commercial expressions, foreign influence and political advertisements. These contexts all have their own regulation and legal logic.

Chapter 3 looks at the various Internet services that play a central role in the online dissemination of disinformation. These different services can be considered on the basis of their legal qualification, business forms and earning models, and on the basis of the enforcement modalities available to a specific service. From a legal perspective, the following types of services are relevant: information society services, elec-

tronic communications services and audiovisual media services. The concept of *hosting service provider* in the E-Commerce Directive is also important as this limitation of liability can be invoked by many of the services concerned. Of specific importance to the problem of disinformation are the social media services, which work on the basis of content generated by their users and offer opportunities for data-driven and targeted advertising. Also relevant are the *direct messaging* services that enable users to communicate one-to-one or in groups. Through new possibilities for targeted communication through these platforms and the possibility of large-scale distribution of content by users, the dissemination of information through these services can have a similar social impact as in the case of traditional mass media. The enforcement possibilities with regard to disinformation are related to the technical set-up of the specific service, the policy of the service, and the actual enforcement of the policy in practice.

The relevant legal framework for disinformation disseminated via Internet services has subsequently been analysed in **chapters 4 to 6,** from which it can be seen, firstly, through the breadth and diversity of the legislation concerned and, secondly, that different forms of disinformation are already regulated in some way through this legislation. The outermost layer of the relevant legal framework is fundamental rights and freedom of expression in particular. After all, all laws and regulations must operate within these limits. The analysis of the relevant case law in the field of freedom of expression in chapter 4 underlines that the right to freedom of expression implies not only that the State should not impose certain restrictions, but also that the State has positive obligations to enable citizens to exercise their freedom of expression. The most relevant positive obligations in this respect are the obligations to ensure pluralistic democratic debate and to prevent capitalist groups from gaining the upper hand in political debate, for example through political advertisements. Transparency obligations, in particular on the origin of (political) advertisements, can also play a positive role in this context. The legal prohibition of certain information solely on the grounds that information is incorrect or misleading, without additional requirements, is difficult to reconcile with freedom of expression. It is important here that disinformation in some cases qualifies as political expression and as such, enjoys broad protection. Furthermore, specific political advertisements are in principle also covered by the extended protection of political expressions under Article 10 ECHR.

Next, the analysis of the legal framework for the dissemination of disinformation at European and national level, in **Chapters 5 and 6,** shows in particular the diversity and enormity of the regulations concerned. The regulations cut across the existing classic areas of law and sector regulations where the relevant framework in a specific case depends on the specific context and the techniques used (e.g. commercial or political expression, private messages or public, hosting provider or service with editorial control and responsibility). The EU framework consists of the Electronic Commerce Directive, the AVMSD, the e-Privacy Directive, the Commercial Practices and Advertising Directives, the AVG and relevant self-regulation. Evidently, it is a very dynamic legal framework. Many elements of the relevant European regulatory framework are very recent (AVG & AVMSD) or are in the process of being revised (e-Privacy Directive and E-Commerce Directive). As stated above, the relevant national legal framework for disinformation cuts across private, state, administrative and criminal law. Within private law, there is the doctrine of tort, which is relevant to unlawful publications, and intellectual property law, including portrait law. Within criminal law, there are the specific crimes of expression, electoral crimes, the developing doctrine of computer crime and crimes of dissemination. Within Dutch state and administrative law, there is the regulation of advertising, the regulation of the financing of political parties, and legislation in the area of national security and critical infrastructure. As far as self-regulation is concerned, the Dutch Advertising Code and the Netherlands Press Council are particularly important. At the national level, there are also a number of (self-)regulatory initiatives in the field of disinformation that have been discussed in chapter 6.

Before moving on to Chapter 7, we will now discuss the conclusions that follow from the analysis of the legal framework in Chapters 5 and 6.

On the basis of the overview of the legal framework provided, it can be concluded in a general sense that a large number of types of disinformation already fall partly under an existing legal category (misleading advertising, libel, unlawful press publication, etc.) and as such are already regulated. It also appears that the applicable regulations depend on the type of Internet service, the content qualification of any (dis) information and the context in which it is disseminated (e.g. commercial, political, private). Not surprisingly, given the breadth of the problem, a large number of different supervisors are subsequently involved in the enforcement of these existing standards. The main ones are the AP, the ACM, the AFM and the Dutch Media Authority (*Commissariaat voor de Media*). These general conclusions will now be further developed with regards to the liability of internet intermediaries, the protection of personal data, the relevant regulators, the criminalisation of online manipulation and the relevant self-regulation.

The **liability of Internet services** for illegal and unlawful content has a central position in the legal framework. Crucial to this is the Electronic Commerce Directive which provides for a conditional horizontal exclusion of liability for illegal and unlawful content at European level. The exact scope of these standards will also determine the way in which Internet services are designed, along with their approach to disinformation, as it may potentially be in their interest to avoid liability. Further, the prohibition for Member States to impose general surveillance obligations on Internet services is a clear limitation to possible regulation of disinformation. In addition to this conditional horizontal exclusion of liability, there are also a number of sector-specific, vertical, liability grounds such as those in the AVMSD that are already shaped in accordance with the space in which Internet services operate. These standards have all been formulated at European level. The new European Commission has announced its intention to revise the legal framework for the liability of intermediaries in the coming years by means of the *Digital Services Act*.

The **protection of personal data** and the effective enforcement of the applicable rules is of great importance to the problem of disinformation. New methods of dissemination via Internet services often rely on the collection, analysis and use of personal data from the public. These data-driven forms of online influencing fall under the AVG and can be tackled on that basis. This applies to the senders of communication, such as an organisation that conducts targeted campaigns via communication services and social media. But it also applies to the Internet services themselves, including the collection of data about their users, and the analysis and use of this data in the light of the opportunities offered to advertisers and other parties for targeted communication with the public. Partly in view of the Cambridge Analytica scandal, there is already quite a bit of attention for disinformation and micro-targeting in the literature on data protection law. Supervisors have also put the subject on the agenda. However, there is currently little effective enforcement of data protection law, while this is seen as an important general safeguard against certain aspects of disinformation.

Subsequently, the **relevant supervision of Internet services** is fragmented and relatively weakly developed, while the complexity requires a high degree of expertise and resources. A large number of regulators are involved, with the ACM, the AP and the Dutch Media Authority playing key roles in the Netherlands. Depending on the specific context, supervisors such as the AFM and the Dutch Food and Consumer Product Safety Authority are also involved. In relevant cases, supervision is also exercised by a ministry, as in the case of the Political Parties (Funding) Act or by, for example, the Fiscal Intelligence and Investigation Service - Economic Control Service for the Dutch implementation of the transparency obligations under the Electronic Commerce Directive.

The GCM is often involved in the context of the protection of consumer interests, the AP in the protection of personal data and the *Commissariaat voor de Media* with regard to media regulation. The working area of these regulators overlap on a number of points, for example with regard to the enforcement of the ban on spam in Section 11.7 of the Telecommunications Act, where both the AP and the ACM have powers. With regard to the problem of disinformation, possible overlap in terms of concrete legal provisions is not the most important point of attention. More important is the substantive overlap where

supervisors are responsible for different elements of the same problem. For example, the AP and the GCM are involved in different aspects of political micro-targeting: the AP as regards targeted dissemination based on personal data and the GCM as regards the content of commercial communications. In advertising distributed on video platforms, all three supervisors are involved in different aspects. Due to this overlap in content, it is important that the various supervisors work together in their approach.

	Authority Personal data	Commissariaat voor de Media	Consumer and Market Authority
Typing	Protection of personal data, monitoring compliance with the AVG.	Media regulation, supervision of the Media Act and the Fixed Book Prices Act.	Protecting consumer rights and monitoring competition.
Connection disinformation	Targeted information dissemination based on personal data (micro-targeting).	Disinformation disseminated through traditional media and advertising regulation.	Regulation of commercial communications and consumer protection.

Figure 4

Furthermore, the use of **criminal law** and the **security services** are an important component of the legal framework. Criminal law is the most far-reaching regulation of disinformation and must be used very reluctantly and only in a deliberate manner in order to protect the freedom of expression. The security services have a role to play in tackling the dissemination of disinformation by foreign States. The concern for improper foreign influence and propaganda is not new and there is extensive case law on the admissibility of possible measures. More importantly to note, Article 10 ECHR explicitly guarantees the right to freedom of expression 'regardless of frontiers'.

A specific part of this study highlights the possible criminal standardisation of online manipulation of elections. The conclusion of this report is that there are currently no grounds for additional criminal law standards relating to misleading or inaccurate online statements. In this context, Article 127 Sr has been discussed extensively. The reason was the Asscher/Van der Molen motion and the fifth research question that this report has been based thereon.[608] Section 6.B discusses the various existing criminal law provisions relating to the improper influencing of the electoral process. Consideration was also given to cybercrime, given the possible integrity breaches on Internet services that may occur when disinformation is disseminated, and the various criminal dissemination offences. In relation to disinformation and online manipulation, Article 127 Sr turned out to be the most relevant penal provision. The article criminalises a "deceptive act" which results in or makes "worthless" a voice or the *error in persona.* Where the required causal link is interpreted extensively, the penalty provision includes expressions that can be qualified as disinformation. Whenever disinformation results in a vote becoming worthless, or a voter has voted for another person than he or she thinks, this is prohibited under Article 127 Sr. Consideration should be given to situations in which a voter is misinformed about the required voting method, which invalidates his or her vote. Thus, although the criminal provision includes forms of online manipulation or disinformation, the most well-known examples of disinformation fall outside the scope of the offence description.

Disinformation that results in people not voting or in people lying about a candidate's election programme is not punishable by article 127 Sr because the damage in these examples is not covered by the article.

608 Lower House, session year 2018/2019 30 821, no. 68.

Any extension of the specific offence definition of Article 127 Sr or other standards relating to the *content of* an expression is problematic from the perspective of freedom of expression. Now that these are political expressions and criminal law has to be considered as an *ultimum remedium*, there is little room for expansion. This was also recognised at the time of the introduction of the penalty provision, when it was emphasised that the courts and the government must remain outside the political debate. It follows that there are no grounds for new criminal standards or offences relating to incorrect or misleading content.

On the other hand, there may be scope in the context of the further development of cybercrime in combination with data protection law. Misleading and manipulative processes based on data that misuse an internet service and influence the election process are not effectively standardized under current law. With the current computer peace clause from Article 138a of the Criminal Code, it is unclear what the role of the terms of use of an Internet service is to qualify an act as 'unlawful intrusion' and thus as punishable. It is undesirable to make the penal determination of a breach of computer peace in this way dependent on the terms of use that an Internet service itself imposes (integrity of the service). However, given the importance of these Internet services for the democratic debate (integrity of the public debate), the possibility of systematically abusing such services in order to manipulate people is so problematic that one should think of a possible standard setting. This standard-setting should also be seen in combination with data protection law, since this type of influence is generally data-driven. Such specific standardisation of data-driven systematic manipulation techniques requires further empirical and legal research.

The various **self-regulatory instruments** in the field of information quality are also important for the broader approach to disinformation. In the Dutch context, the Dutch Advertising Code and the Netherlands Press Council are essential for setting sector-wide standards that monitor the quality of information and thus also providing an important guarantee for disinformation. At European level, self-regulatory instruments such as the *EU Code of Practice on Disinformation* are important. The individual policies of the Internet services themselves also have a major influence on the possible dissemination of disinformation. Finally, the regulation of the **financing of political parties** can also be an important guarantee for the dissemination of disinformation in the form of political advertisements.

To conclude the summary and conclusions of the report, **Chapter 7** remains to be considered**.** This chapter contains a synthesis of the legal framework in force in the Netherlands, the approach to disinformation and the results of the country studies carried out (United Kingdom, France, Germany, Sweden, the United States and Canada). The chapter also provides an overview of how the current legal and policy framework for disinformation and political advertising in the Netherlands covers law and policy at three coherent levels: European, national and self-regulation. On the basis of the country studies, different possible approaches to tackling disinformation can be identified, including (a) new media literacy programmes, and additional funding for existing programmes aimed at strengthening the critical capacity of Internet users to deal with disinformation, (b) new programmes to subsidise independent media, (c) tackling disinformation in the context of national security, (d) specific new legislation prohibiting disinformation and misinformation during elections, (e) new duties of care for Internet services regarding the implementation of measures to deal with disinformation, (f) an obligation for Internet services to remove disinformation that qualifies as manifestly unlawful within 24 hours, (g) new legislation addressing foreign influence and prohibiting foreigners from contributing to or spending on elections; and (h) new regulation of bots and automated software.

Chapter 7 also considers the various regulatory options with regard to political advertisements. Although this will not solve the broader problem of disinformation, it can offer a solution to the specific problem of disinformation contained in political advertisements. The outcome of the analysis was that the report supports the committee's advice on the Dutch parliamentary system and the government's intention to include further financial transparency for political parties in the 'Political Parties Act'. The same legislation can also be used to set limits on the ability of foreign actors to finance Dutch political parties.

C. Recommendations

A number of concrete recommendations can be distilled from the study. For example, the concept of disinformation should be considered as a **policy term** and not as a defined legal concept. This is also clear from the country studies. In almost all countries examined - Sweden, the United States, the United Kingdom, Germany and Canada - disinformation is not legally defined, but seen as a policy area. The only outlier is France, which has had a law on "false news" for years, has more recently adopted new legal definitions of "false information" and "manipulation of information" in the context of elections.

In order to set **new standards** in the Dutch context, this report recommends further research into the standardisation of new forms of manipulation, such as the large-scale and data-driven manipulation of communication processes on relevant Internet services. This is not about banning new forms of false or misleading information, but about the regulation of communication processes and the integrity of relevant means of communication from a democratic point of view.

Furthermore, recognising the stratification and **different legal policy levels** is one of the most important starting points for the further development of policy on disinformation. The role and responsibility of different types of services in the dissemination of (dis)information is rightly a central point of attention in the debate, but from a legal point of view, the applicable framework is very layered and complex. Part of the disinformation problem is directly related to the specific design of Internet services, particularly social media, and the possibilities it offers for the (further) dissemination of (dis)information. The policies of relevant services are developing under pressure from national governments, however, there is mainly an international dynamic at play. The question is how the choices made by relevant services and the self-regulation agreed elsewhere should be viewed from a Dutch perspective.

There is also an **area of tension in the regulation** of various aspects of disinformation between the European and Dutch levels. The focus of the relevant European legislation is on market organisation and safeguarding the European internal market. It also follows logically that the European legislator plays a relatively dominant role in setting and harmonising rules for relevant Internet services. However, there is a relative lack of competence with regard to laying down rules to protect democratic debate and national political processes. It is precisely this dimension that ultimately lies at the heart of the problem of disinformation. It is therefore important that European legislation on social media and other Internet services play a facilitating role in relation to national problems, leaving room for individual choices and considerations in the member states. As the European Court of Human Rights has considered, there is a "wealth of historical, cultural and political differences within Europe so that it is for each State to mould its own democratic vision"; and because of "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". 622

Where a European supervisor for disinformation is not obvious, the European Union could, for example, ensure the improvement (if necessary, under mandatory law) of the information positions of national governments and regulators with regard to relevant Internet companies. Related to this, of course, the legal, political and practical limitations on the jurisdiction of national law and related restrictions on extraterritorial effect should also be considered. Internationally, there is no unambiguous answer to the approach to disinformation in Internet services. In the light of freedom of expression, it must be prevented that the final standardisation and enforcement ends up at the lowest common denominator.

The best general basis for regulation and policy regarding disinformation and political advertising is the **guarantee of pluralism**. Article 10 ECHR allows, or rather requires, through the doctrine of positive obligations, structural measures to be taken in connection with the promotion of media pluralism. These include the regulation of mass media aspects of social media, the imposition of restrictions on political advertisements, in particular through transparency requirements, and the public funding of (independent) media.

Further research is needed on which possible measures are most appropriate and necessary to address the dissemination of disinformation through Internet services. This could include certain obligations relating to the organisation of the service (e.g. possibilities to report illegal or harmful content and the obligation to respond adequately), as well as obligations of (procedural) transparency with regard to the use of the service in question, as well as investments in the online activities of the public service media.

Strict liability for illegal and unlawful forms of disinformation poses problems for freedom of expression and the E-Commerce Directive. In any event, the standards laid down with regard to the **responsibility of Internet intermediaries** should be consistent with the social role of the services concerned and not merely maximise the possibility of control by intermediaries without regard to the negative consequences. A more fruitful direction of standard setting is the possibility of general standards with regard to the organisation of the service in question and related processes. This could include, for example, an obligation to offer an easily retrievable option to report disinformation, to receive a response within a certain period of time, clear warnings regarding conditions of use, monitoring and reporting on unlawful use of the service. More research is needed into the possibility of setting such standards and reporting them in relation to different services.

Where there is removal or blocking of content by Internet services, there is currently a lack of clear rules on the **rights of the users** whose communications are concerned. This is a subject that can be considered both from the point of view of consumer law and freedom of expression. It is an issue that will have to be addressed in the planned review of the European framework and is already being considered in the European Commission's official policy documents on illegal and harmful content.

Relevant **monitoring** of the problem of disinformation is fragmented. Further cooperation between mainly the ACM, the AP and the Dutch Media Authority (*Commissariaat voor de Media*) is important for effective supervision of existing rules and the strengthening of relevant expertise. The protection of personal data is an important general safeguard for certain data-related aspects of disinformation and online manipulation. However, there is currently little effective enforcement of data protection law on relevant aspects.

A general concern is the **lack of transparency** with regard to communication processes, as well as the enforcement by Internet services of disinformation. As a result, the information position of relevant authorities, as well as the social field, is relatively poor. Science and journalism are sending increasingly strong signals that access to data necessary for the study of disinformation is insufficiently guaranteed. It is important to note that different social actors have different information needs in the performance of their tasks and social functions. The government, journalism, sciences, NGOs, and regulators all have their own information needs. Effective transparency regulation would require further identification of what these needs are and how additional regulation through transparency requirements can meet them. Self-regulatory initiatives by social media have so far failed to deal with this problem. Given the democratic interests involved in assessing the social impact of Internet services, and social media in particular, this is a subject where a more active attitude on the part of the government is desirable.

References

J. Aalberts, *Het mysterieuze voortbestaan van de zendtijd van politieke partijen,* Tijdschrift voor Mediageschiedenis, 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, *Verkennend 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*, via: 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 January 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. Dkhlia, *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, F*acebook, 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 vestors 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 Audiovisual 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*, 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*, 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*, 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 politcal 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,* 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*, 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*, via: https://www.bundestag.de/resource/blob/566942/a5eb997872bbe5dbca3f47112eb04c46/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,* 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*, 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* , 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*, 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.

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.

European Data Protection Board, *Annex 1 on national DPA guidance,* 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,* via: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

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,* via: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

European Commission, *Communication on Securing free and fair European elections*, available via: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0637:FIN.

European Commission, *Action Plan against Disinformation*, via; https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

European Commission, *EU Code of Practice on Disinformation*, via: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

European Commission, *Tackling online disinformation: a European Approach,* COM(2018) 236 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236.

European Commission, *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-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-ssubversion-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,* 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*, 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, 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/Remmelink 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.

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,* 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 worl*d, 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 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,* via: https://support.google.com/adspolicy/answer/6014595?hl=en.

Google, *An update on our political ads policy,* 20 November 2019, via: https://blog.google/technology/ads/update-our-political-ads-policy/

Google, *Election ads in Canada,* 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*, 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,* 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*, via: https://www.ivir.nl/publicaties/download/IRIS_Special_2017_1.pdf.

GRECO, *Third Evaluation Round. Second Compliance Report on the Netherlands. Transparency of Pary 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,* 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,* 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*, 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%2FC%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*, 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*, 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 Politcal 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*, via: http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf.

J.-B. Jeangène Vilmer, A. Escorcia, 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*, 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 uitingsvrijheid 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*, via: https://undocs.org/A/HRC/26/30.

Lage Drempels, 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,* 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*, 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.
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. Nieuwenhjuis, *Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief,* Amsterdam: Cramwinckel 2000.

Microsoft, *Disallowed Content Policies - Political and religious content*, 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 May 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.

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 May 2019 https://nos.nl/nieuwsuur/artikel/2285561-bits-of-freedom-facebook-gaat-de-fout-in-met-politieke-advertenties.html.

Noyon, Langemeijer & Remmelink, Strafrecht, artikel 125 Sr, aant. 7.

ODIHR Election Expert Team, *Sweden General Elections 2018*, 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 Franc Presidential Election 23 April and 7 May 2017, OSCE/ODIHR Election Expert Team Final Report,* via*:* https://www.osce.org/odihr/elections/france/337346?download=true.

OSCE, *Election Expert Team, Elections to the Federal Parliament (Bundestag) 24 September 2017,* 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*, 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*, 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*, 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,* 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*, 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_Initatives_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*, 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,* via: https://www.ourcommons.ca/Content/Committee/421 /ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf.
Swedish Civil Contingencies Agency, C*ountering information influence activities – A handbook for communicators* (MSB, 2019), https://rib.msb.se/filer/pdf/28698.pdf.

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.

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*, 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, S*ocial 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*, 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.

Cannataci, 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"*, 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,* 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),* via: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-e.

K. Verhoeven, *Actieplan Digitale Advertenties*, 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. Vliegenthart & 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: Routlegde, 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.

WhatApp, "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 ontwrichting,* 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 Ontwrichting", September 2019.

Zuiderveen Borgesius et al 2018, *"Online Political Microtargeting: Promises and Threats for Democracy",* Utrecht Law Review 2018.

Appendix: Country studies

For each country, we present the general overview, followed by a description of disinformation regulation (including proposed regulation), and political advertising regulation.

A. Introduction to the Country Studies

The following sections describe the regulation of disinformation and paid political advertising in six countries (UK, France, Germany, Sweden, US and Canada).

Many national governments are examining the issue of disinformation, with government and parliamentary reports, such as from the United Kingdom,[609] France,[610] and Germany.[611] However, in terms of follow-up regulation in the form of legislation, France is the only country that has adopted specific legislation designed to target disinformation, in its 2018 Law on Manipulation of Information (see below). While Germany enacted the 2018 Network Enforcement Act, which targets internet services, this does not have a specific provision on disinformation, as it concerns 22 criminal offences already in existence (see below).

There are many government non-legislative initiatives to help identify and counter disinformation, which fall short of regulation in terms of legislation, such as through the publication of toolkits. Examples would be the UK Government Communication Service's *Counter-disinformation toolkit,*[612] or Sweden's Civil Contingencies Agency's handbook on *Countering information influence activities.*[613] Helpfully, the Poynter Institute for Media Studies maintains an updated *Guide to anti-misinformation actions around the world* on the measures in the UK, France, Germany, Sweden, the United States, and Canada.[614]

In relation to political advertising, it should be noted at the outset that very different rules apply depending upon whether the political advertising is placed in a newspaper, broadcast on television, or carried/facilitated by an internet service. The rules applicable to each medium are included to help better inform possible policy options for the regulation of political advertising carried/facilitated by internet services in the Netherlands. Before the analysis of the regulation of paid political advertising, the state of disinformation regulation is presented, as well as an overall assessment of the legal system's treatment of disinformation and political advertising. In the country studies, we focus on the specifics of each country. We do not discuss the applicable rules at the EU level which have been implemented in national law, such as the GDPR, ePrivacy, or AVMSD.

In contrast to disinformation generally, there are a number of examples of new legislation targeting political advertising on internet services. Since 2018, Canada, France, and number of US states (see below) have introduced legislation, mainly on transparency, and the effect has been quite pronounced: some

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 Ibid.

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.

internet services have stopped allowing political advertising completely for elections in certain countries and US states.

For example, in the US, Google Inc., no longer allows political advertisements for elections in Maryland, New Jersey, Nevada, and Washington.[615] Microsoft Inc. is also no longer accepting political candidate and ballot measure advertisements in the US, due to "regulators from states across the country have taken new steps to bring additional transparency and accountability to political advertising."[616] This ban has now been extended worldwide. Similarly, in France, Twitter Inc., does not permit political campaigning and issue advocacy ads.[617] While in Canada, Google Inc. announced that political advertising would not be allowed on Google platforms during the 2019 Canadian federal elections from June - October 2019.[618]

B. United Kingdom

i. General characterisation

The issue of disinformation and online political advertising has been high on the political agenda in the UK since the 2016 Brexit referendum. There have been numerous reports from the UK government,[619] parliament,[620] and investigations by the Information Commissioner's Office (**"ICO"**),[621] and the Electoral Commission,[622] concerning disinformation and online political advertising. In July 2019, the UK government announced £18 million of government funding to strengthen independent media and counter disinformation and fake news across Eastern Europe and the Western Balkans.[623] The UK government also established a High-Level Panel of Legal Expert on Media Freedom in July 2019, chaired by a former President of the UK Supreme Court.[624] Further, in September 2019, the BBC and the European Broadcasting Union announced a new industry collaboration to tackle misinformation, including with major news publishers, and Google, Twitter and Facebook. The new collaborative initiatives will include (a) creation of creating 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 around elections, so there is a common way to explain how and where to vote.[625] The communications regulator OFCOM also recently published a report on online market failures and onlineword platforms.[626]

---

615 See: 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.

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.

In relation to online political advertising in particular, the ICO has stated that it found a "disturbing disregard for voters" personal privacy by players across the political campaigning eco-system - from data companies and data brokers to social media platforms, campaign groups and political parties".[627] The Electoral Commission has recommended a number of reforms to election laws applicable to online political advertising, including (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. Disinformation Regulation

First, a provision in election legislation has rules on false statements of fact relating to a political candidate. Under the Representation of the People Act 1983, it is an offence, for the purpose of affecting the return of any candidate at the election, to publish any false statement of fact in relation to the candidate's personal character or conduct.[629] In 2019, the High Court quashed a summons against the British politician Boris Johnson for the offence of misconduct in public office for "endorsing and making statements which were false and misleading, without justification concerning the cost of European Union membership."[630] The Court discussed the limited range of the false statement law, and stated that parliament deliberately "excluded any other form of false statement of fact, including those relating to publicly available statistics."[631]

Second, under the Digital Economy Act 2017, the government must issue a code of practice to online social media platforms in relation to how platforms take action against use of platforms for certain harmful behaviour, including bullying, insult, or behaviour likely to intimidate or humiliate individuals.[632] In 2019, the Code of Practice for providers of online social media platforms was published, following public consultations.[633] The four key principles are social media platforms should (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) give clear information to the public about action they take against harmful conduct. The code's guidance is in advance of a new regulatory framework.

Third, in April 2019 the UK government published proposals to create a new regulatory framework in order to tackle illegal and harmful content online, including disinformation[634] (civil society has also published responses to the White Paper[635]). The government stated it was "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)". The central element of the proposal is to impose a new statutory duty of care on certain technology companies to take "reasonable steps to keep their users safe and tackle illegal and harmful activity on their services".[636] Crucially, the statutory duty of

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 Johnson v Westminster Magistrates Court [2019] EWHC 1709 (Admin), 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.

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 Ibid, p. 42.

care would be enforced by an independent regulator, and the regulator would set out how companies would fulfil their legal duties under new codes of practice. The regulation would target "companies of all sizes" that provide services enabling users to share user-generated content, or interact with each other, including social media companies and public discussion forums. Notably, the framework will apply a different approach for private communication, where requirements to scan or monitor content for tightly defined categories of illegal content will not apply to private channels.[637]

The statutory duty of care would apply to tackling disinformation by requiring technology companies to take "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". The new regulator would flesh out these requirements in a code of practice, including (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. Notably, companies will be required to "ensure that algorithms selecting content do not skew towards extreme and unreliable material in the pursuit of sustained user engagement".[638]

Finally, the proposal sets out the regulator's enforcement powers, which would include the power to issue fines. However, the proposal also includes possible additional powers, including forcing third-party companies to withdraw any service they provide that directly or indirectly facilitates access to the service; Internet Service Provider blocking of non-compliant websites or apps; and senior management liability. Notably, on the question of general monitoring, the proposal includes that to "ensure effective oversight of the take-down of illegal content", the new framework "will introduce specific monitoring requirements for tightly defined categories of illegal content".[639]

iii. Political Advertising Regulation

Different rules on political advertising apply depending upon whether it involves print, broadcasting, or online.

1. Newspapers and broadcasting

While there is no specific regulation of paid political advertising in newspapers outside of election-time; during election-time, certain political advertising in newspapers is subject to a transparency rule. Thus, under the Political Parties, Elections and Referendums Act 2000, "election material" which is an "advertisement" in a newspaper must include the "name and address of the promoter of the material," and the name of any person on behalf of whom the material is being published.[640]

In contrast, paid political advertising on television is prohibited at all times, including during election-time.[641] Importantly, in 2013, the ECtHR held that this prohibition on political advertising, as applied to an animal rights association's political advertisement, did not violate the right to freedom of expression under Article 10 ECHR.[642] The ECtHR accepted the UK government's reasons for the ban, including the need to protect the democratic debate and process from distortion by powerful financial groups. It should

637 Ibid. p. 50.
638 Ibid., p. 72.
639 Ibid., p. 63.
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).

be noted, however, that *non-paid* party-political broadcasts and referendum campaign-group broadcasts are permitted at certain times in the form of free airtime, but subject to considerable regulation.[643]

2. Internet services

In England and Wales, there is no specific regulation of paid political advertising online. Notably, in Scotland, a special transparency rule was added under the Scottish Independence Referendum Act 2013, which only applied in Scotland, that required any material, including online material, which related to the Scottish referendum, to include the "name and address of the promoter of the material".[644] The UK's Electoral Commission recommended in 2017 that a similar rule should be enacted across the UK, stating that an "appropriate level of imprint information should be required on online and electronic referendum campaign material".[645] The Commission again recommended in 2018 that UK law should be reformed so that "digital material must have an imprint saying who is behind the campaign and who created it".[646]

While paid political advertising is not specifically restricted online through regulation, a number of important election spending rules are applicable to spending on political advertising. The UK Electoral Commission has emphasised that election spending rules "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]

Finally, the ICO has issued Guidance on political campaigning,[648] and how the rules under the GPDR and ePrivacy Directive apply to political campaigning, whether in the form of online political advertising, direct marketing, or viral campaigns.

C. France[649]

i. General characteristics

Similar to the UK, disinformation and online political advertising have been contentious issues in France, particularly following the '#MacronLeaks' on the eve of the 2017 French presidential election.[650] There have been numerous government reports on disinformation, and on the regulation of online platforms.[651] Indeed, the French government has published English-language reports, including *Information Manipulation: A Challenge to Our Democracies*, making a number of recommendations, including that States must be able to implement the following measures when necessary: (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, the French government also published a 34-page

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.
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. & Dakhlia, 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. Escorcia, 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

report entitled, *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision*.[653] The report recommends "public intervention to force the biggest [social media network] players to assume a more responsible and protective attitude to our social cohesion." The regulation would focus on accountability of social networks, implemented by an independent administrative authority and based on three obligations for the platforms: (a) obligation of transparency of the function of ordering content, (b) obligation of transparency of the function which implements the Terms of Service and the moderation of content, and (c) duty of care towards its users. The imposition of a duty of care would mean social media networks "commit[ting] to be accountable for their users regarding abuses by other members and attempts to manipulate the platform by third parties".[654]

ii. Disinformation Regulation

France is the only country so far that has followed up with specific legislation targeting disinformation. However, it should also be noted that French law has criminalised the publication of "false news" ("*nouvelles fausses*") for many years, under Article 27 of the 1881 Freedom of the Press Law.[655] In 2018, Law no. 2018-2012 on Manipulation of Information was enacted, which provides that during the three months prior to an election, a court can order an online platform to remove "*des allégations ou imputations inexactes ou trompeuses d'un fait*" ("inaccurate or misleading allegations or imputations of fact"), which may "alter the sincerity of an upcoming vote", and are "disseminated deliberately, artificially or automatedly", and on a massive scale.[656] The court is required to deliver a decision within 48 hours, and any appeal decision must be delivered within 48 hours.

The first decision under this procedure was delivered in May 2019, with the Paris Regional Court rejecting an application by a French opposition senator against Twitter to have a tweet by the French Interior Minister blocked.[657] The Court clarified that the content must be "sponsored content - i.e. the payment of third parties to artificially broaden the dissemination of information, and content promoted using automated tools such as bots".[658] The Court also held that "inaccurate or misleading allegations or statements do not include partial inaccuracies or simple exaggerations, but only allegations or statements whose inaccuracy can be objectively proven. In addition, the inaccurate or misleading nature of the allegations must be "clear", as must the risk that they might unduly affect voting behaviour in elections."

Title III of the 2018 Law on Manipulation of Information introduces a "duty of cooperation" on certain online platforms to fight the dissemination of false information. The online platforms are those defined in Article L. 111-7 of the Consumer Code whose activity exceeds five million unique visitors per month, per platform, calculated on the basis of the last calendar year. Article 11 requires that these online platforms take measures to fight the dissemination of false information that is likely to disturb public order or to alter the sincerity of certain elections. In particular, platforms are required to put in place an "easily-accessible and visible mechanism enabling users to report false information that is likely to disturb public order or affect the sincerity of the election, particularly when such information arises from content promoted on behalf of a third party". Article 11 also provides that platforms implement other measures

/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 Ibid., p. 21.

655 Law of 29 July 1881 on freedom of the press, Article 27, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722ateTexte=vig

656 Law n° 2018-1202 of 22 December 2018 on the fight against the manipulation of 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 Ibid.

that "may" include: (a) transparency of algorithms; (b) promotion of content from press companies and news agencies and from audiovisual communication services; (c) combatting accounts disseminating false information on a massive scale; (d) the identity of individuals providing remuneration in return for the promotion of information content;(e) information on the nature, origin and modalities for dissemination of content; and (f) promote media and information literacy. Platforms are required to provide an annual declaration to the French media regulator (*Conseil Supérieur de l'Audiovisuel*) (CSA) of the methods of implementation of each of the measures taken pursuant to Article 11.

Under Article 12, the French media regulator (*Conseil Supérieur de l'Audiovisuel*) (CSA) may issue recommendations to online platforms with a view to improving the fight against the dissemination of false information that is likely to disturb public order or to affect the sincerity of the election. In May 2019, the CSA issued its first Recommendations to online platforms on the duty to cooperate to fight the dissemination of false information.[659] There are detailed recommendations on how platforms implement the measures set out in Article 11.

Notably, in relation to combatting accounts disseminating false information on a massive scale, platforms are encouraged to set up "appropriate procedures allowing for the detection of accounts disseminating false information on a massive scale", and "proportionate procedures intended to hinder the actions of these accounts (warnings, deletion, quarantine, restriction of user rights or of the scope of the content disseminated, etc.), in compliance with the freedom of expression and communication".[660] The Recommendation also states that platforms provide users with "clear and detailed information on practices that are likely to result in action being taken by the operator (creation of abnormal numbers of accounts, sharing of content at abnormal rates, use of false, stolen or misleading information, etc.)".[661]

Further, in relation to promotion of content from press companies, the CSA recommends that platforms "deploy technological means aiming to highlight information from these sources and particularly "fact-checking" content in search engine results, newsfeeds and other dissemination channels using automated classification techniques".[662]

iii. Political Advertising

In contrast to all other countries, France regulates election-time political advertising in newspapers, broadcasting, and online. Outside of election-time, there are fewer restrictions.

1. Newspapers and broadcasting

Political advertising is prohibited in newspapers during election time, but permitted outside election periods. Article L. 52-1 of the Electoral Code prohibits, during the six months prior to an election, "the use, for the purpose of election propaganda, of any commercial advertising in the press or any means of audiovisual communication".[663] Further, during election periods, press advertisements must not contain "references, verbal or visual, to candidates or election-related issues".[664] However, Article L. 52-8 of the Electoral Code allows candidates to "advertise in the press for authorised donations" in order to finance their campaigns.

---

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.

660 Ibid., p. 4.

661 Ibid.

662 Ibid.

663 Electoral Code, Consolidated version as at 3 August 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 Audiovisual Observatory, 2017.

Similarly, in relation to broadcasting, Article L. 52-1 prohibits during the six months prior to an election, the use, for the purpose of election propaganda, of any commercial advertising in the press or any means of audiovisual communication. Legislative provisions determine the overall length of campaigns for the various elections, and how airtime should be distributed between the different candidates, parties or groups. The French media regulator lays down the rules concerning conditions for the production, scheduling and broadcast of programmes during the official campaign before each election.[665]

2. Internet services

Political advertising is also prohibited online during election-time; and new rules were enacted in 2018 on transparency. First, the Article L. 52-1 prohibition above also covers online public communication.[666] For example, during the 2017 French Presidential, the OSCE's Election Expert Team's report noted that online media were subject to the "prohibition of purchasing and publishing paid political advertising, which extends to all type of media".[667]

Further, under Article L. 48-1 of the Electoral Code, the prohibitions on the distribution of election propaganda expressly apply to "any message with the character of election propaganda disseminated to the public by any electronic communication method". This type of election propaganda is not defined in the legislation, but as noted by the OSCE, is similar to paid political advertising. Further, Article 49 prohibits communication to the public of *any* electoral propaganda on the day of the election and on the previous day.

Most recently, under Law no. 2018-1202 on Manipulation of Information, the Electoral Code was amended to include that during the three months prior to an election, certain online platform operators must provide users with "fair, clear and transparent information" (a) about the identity of the person or company which pays the platform for the promotion of "information content related to a debate of general interest", and (b) on the use of personal data in the context of the promotion of information content related to a debate of general interest; and also create a publicly-accessible register of this promoted content.[668] As such, during election time, certain paid content concerning debates of general interest are subject to transparency rules.

Thus, France has one of the most interventionist regulatory frameworks for political advertising. But it should be emphasised that these rules are limited to election time.

D. Germany[669]

i. General characteristics

In current discussions of disinformation and political advertising, Germany is sometimes lumped together with countries enacting legislation targeting disinformation and fake news, due to its enactment of the 2018 Network Enforcement Act (NetzDG). It is sometimes reported that the NetDG law applies to removal

665 Article 14, par. 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.

667 OSCE, '*Republic of Franc 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 Law n° 2018-1202 of 22 December 2018 on the fight against the manipulation of information, article 1, https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/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.

of "fake news".[670] It is important to note therefore, that while the legislation targets internet services such as social media platforms, it does not contain specific provisions on fake news, false news, disinformation or political advertising. As Tworek and Leerssen emphasise, 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] The Act targets large social network platforms, with more than 2 million users located in Germany, and requires these platforms to provide a mechanism for users to submit complaints about illegal content. Once they receive a complaint, platforms must investigate whether the content is illegal. If the content is 'manifestly unlawful', platforms must remove it within 24 hours. Other illegal content must be taken down within 7 days, and platforms that fail to comply risk fines of up to €50 million.[672]

However, the German government has stated, in its submission to the UN Special Rapporteur on freedom of expression, that the main reason for the NetzDG law was "[n]ot only hate speech, defamation and malicious gossip," but "also the spread of "fake news" on social media platforms".[673] Therefore, the law's applicability to combating disinformation will be discussed below.

ii. Disinformation regulation

The NetzDG applies to "profit-making" internet platforms which "enable users to share any content with other users or to make such content available to the public (social networks)", and have at least two million registered users in Germany. It does not apply to platforms designed to "enable individual communication or the dissemination of specific content". The Act operates as follows: first, section 3(1) places an obligation on platforms to maintain an "effective and transparent procedure for handling complaints about unlawful content", and must "supply users with an easily recognisable, directly accessible and permanently available procedure for submitting complaints about unlawful content".[674] Unlawful content is defined as content within the meaning of 22 criminal offences under the German Criminal Code. It is helpful to set out these offences, as they apply to an enormous amount of expression:

> insult; defamation; intentional defamation; defamation of religions, religious and ideological associations; dissemination of depictions of violence; dissemination of propaganda material of unconstitutional organisations; using symbols of unconstitutional organisations; treasonous forgery; public incitement to crime; incitement to hatred; preparation of a serious violent offence endangering the state; encouraging the commission of a serious violent offence endangering the state; breach of the public peace by threatening to commit offences; rewarding and approving of offences; distribution, acquisition and possession of child pornography; threatening the commission of a felony; forgery of data intended to provide proof.

Section 3(2) then sets out how the procedure must operate: first, platforms must take "immediate note" of any complaint and check "whether the content reported in the complaint is unlawful and subject to removal or whether access to the content must be blocked". Second, and crucially, platforms must remove or block access to "content that is *manifestly unlawful* within 24 hours of receiving the complaint" (emphasis added). The Act does not provide a definition of manifestly unlawful.

---

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 Ibid., 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.

673 https://www.ohchr.org/Documents/Issues/Opinion/Legislation/GermanyReply9Aug2017.pdf.

674 Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) 2017, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2.

Third, platforms must remove or block access to "all unlawful content immediately, this generally being within 7 days of receiving the complaint". Notably, the 7-day time limit may be exceeded where (a) the decision regarding the unlawfulness of the content is dependent on the falsity of a factual allegation or is clearly dependent on other factual circumstances (the social network can then give the user an opportunity to respond to the complaint before the decision is rendered); or (b) the social network refers the decision regarding unlawfulness to a recognised self-regulation institution under the NetzDG within 7 days of receiving the complaint and agrees to accept the decision of that institution. In this regard, section 3(6) provides for the recognition of a self-regulatory body if it satisfies a number of statutory criteria, such as its independence and has facilities for "prompt analysis" of unlawful content with 7 days.

Fourth, the NetzDG imposes reporting obligations on social media platforms to publish reports on the handling of complaints about unlawful content on their platforms. The legislation sets out the required content on these reports, including (a) description of the mechanisms for submitting complaints about unlawful content and the criteria applied in deciding whether to delete or block unlawful content, (b) number of incoming complaints about unlawful content, and (c) time between complaints being received by the social network and the unlawful content being deleted or blocked.

Finally, the Act makes it a regulatory offence to contravene the Act, and regulatory fines of up to 5 million euro may be imposed. As mentioned above, the NetzDG does not introduce any new criminal offences. However, it should be noted that the offences covered by the NetzDG are very broadly worded, and are applicable to false information. Indeed, the UN Special Rapporteur on freedom of expression has raised concerns due to "vague and ambiguous vague and ambiguous criteria, such as "insult" or "defamation".[675] Indeed, the German Criminal Code criminalises insult under Article 185, and does not provide a definition, merely stating that an "insult shall be punished with imprisonment not exceeding one year or a fine".[676] Further, even if a statement is true, it may be a criminal insult, as under Article 192, "[p]roof of truth of the asserted or disseminated fact shall not exclude punishment under section 185 if the insult results from the form of the assertion or dissemination or the circumstances under which it was made". Of course, German law on insult is mainly elaborated upon and explained in case law, but the important point is that the Criminal Code itself provides little guidance of what constitutes an insult.

Further, defamation is criminalised under Article 186, and is defined as: "disseminating a fact related to another person which may defame him or negatively affect public opinion about him, unless this fact can be proven to be true."[677] Similarly, intentional defamation is criminalised under Article 187, and is defined as: "intentionally and knowingly disseminating an untrue fact related to another person, which may defame him or negatively affect public opinion about him."

Various platforms have published transparency reports on the operation of the Act, including Facebook, YouTube, and Twitter. In its latest report for January – June 2019, Facebook reported that the highest number of content blocked concerned Insult (140), followed by Incitement to hatred (70) and Defamation (39).[678] In YouTube's latest report for the same period, it reported that the highest number of content removed or blocked concerned Incitement to hatred and defamation of religious, religious

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

and ideological associations (23,567), followed by defamation and insult (14,985). Further, 87% of content was removed or blocked within 24 hours of the complaint.[679] Notably, in July 2019, the Federal Office of Justice issued a 2 million euro fine on Facebook for incomplete information provided in its published report on the number of complaints received about unlawful content.[680] The Office stated that the NetzDG reporting form is not made sufficiently transparent, and was too hidden.

iii. Political advertising

1. Newspapers and broadcasting

In Germany, there are no specific legislative provisions governing election advertising or election reporting in the print media. Political parties are, in principle, allowed to advertise, since the regional legislators responsible have not prohibited it in the regional press laws.[681] If election advertising or reporting appears in the written press, the publisher – unlike broadcasters – is not required to respect the equal opportunities of the parties or party-political neutrality.[682]

In contrast, under Article 7(9)(1) of the *Rundfunkstaatsvertrag* (RstV) (Inter-State Broadcasting Agreement) advertising of a political, ideological or religious nature is prohibited.[683] However, exemptions apply during election campaigns. For example, all public service broadcasters except Radio Bremen, Radio Berlin-Brandenburg and Saarländischer Rundfunk are obliged to allocate airtime for election advertising free of charge. As far as national broadcasters are concerned, for Zweites Deutsches Fernsehen (ZDF) this requirement is set out in Article 11(1) of the ZDFStaatsvertrag (ZDF Inter-State Agreement – "the ZDF-StV"), under which parties are entitled to a reasonable amount of airtime in the run-up to Bundestag and European Parliament elections if they feature on at least one state list or nomination.[684]

2. Internet services

The regulation of election advertising and election reporting in the online sector depends not only on the online service itself but also on its provider. German law distinguishes between broadcasting and telemedia. The transmission of a linear programme according to a schedule (especially live streaming services) via the Internet is classified as broadcasting and must comply with the prohibition of political advertising.[685] Telemedia content, on the other hand, is governed by Articles 54 et seq. of the RStV. Election advertising via on-demand audiovisual media services is prohibited under Article 58(3)(1), in conjunction with Article 7(9) of the RStV and, in other telemedia, must be separated from other content, in accordance with Article 58(1) of the RStV. However, the UWG (Unfair Competition Act), which is by far the most important instrument for the regulation of Internet advertising in Germany, does not apply to political advertising. For journalistic telemedia – especially on-demand online services of newspapers and broadcasters – Article 54(2) the RStV also states that recognised journalistic principles should apply. However, this does not cover telemedia that fall beneath the journalistic threshold, which typically include social media platforms such as Facebook and YouTube, as well as political parties' online offerings.[686]

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/?loclr=eaglm.

681 Etteldorf, C. *"DE-Germany"* in Cappello, M. (ed.), *'Media coverage of elections: the legal framework in Europe',* European Audiovisual Observatory, 2017, p. 33.

682 Ibid.

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://wwwen.uni.lu/content/download/31281/371474/file/Germany_translation_1.pdf).

684 Ibid.

685 Ibid., p. 32.

686 Ibid.

Further, as mentioned above, the NetzDG does not contain specific provisions concerning political advertising, although it does target online platforms.[687] Kruschinski and Haller also have an overview of how German data protection law applies to online political microtargeting.[688]

Finally, in contrast to countries such as the UK, it should be noted that in the 2017 OSCE Election Expert Team's report on German federal parliament elections, it emphasised that "[t]here are no limits set to campaign expenditures for parties and candidates," and 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. Sweden

i. General characteristics

There has been a great deal of research and discussion on disinformation in Sweden, particularly related to disinformation during election periods.[690] Indeed, the Swedish government treats disinformation as a national security issue, and combatting disinformation during elections is part of the Swedish government's National Security Strategy.[691] However, Sweden has adopted a distinctly non-legislative approach, which has been described as a 'proactive approach' to disinformation by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs in its study on *Disinformation and propaganda: impact on the functioning of the rule of law in the EU and its Member States.*[692] Similarly, the French government report on *Information Manipulation: A Challenge to Our Democracies*, also points to Sweden's policies as methods to combat disinformation.[693] While there has also been empirical research focusing on Sweden, such as the Oxford Internet Institute study on junk news during the Swedish General Election on Twitter,[694] and a London School of Economics (LSE) study on the 2018 Swedish elections concerning bots and amplification. [695]

Further, in relation to online political advertising, Sweden is a notable case study for its approach to political advertising in general, where there is little regulation, and there was indeed deregulation on political advertising on TV recently.

687 See: 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 Kruscinski, S. & Haller, A., *'Restrictions on data-driven political microtargeting in Germany'*, 2017, Internet Policy Review, 6(4). DOI: 10.14763/2017.4.780.

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.

693 Jeangène Vilmer, J.B., Escorcia, 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.

ii. Disinformation regulation

Sweden has not adopted legislation targeting disinformation, but a number of notable non-legislative measures have been implemented. First, there are information campaigns. For example, in 2019, Sweden's Civil Contingencies Agency published a 50-page handbook on *Countering information influence activities*, which includes methods on how to counter disinformation, and other methods of "information influence techniques," such as '[m]alicious rhetoric'.[696] The European Parliament has also highlighted the Swedish government's announcement of the setting up an authority in to counter disinformation and foreign influence campaigns. The authority's main purpose is to strengthen resilience against disinformation, and provide 'psychological defence' (psykologiskt försvar) for the population.[697] the Swedish Civil Contingencies Agency has worked with the Swedish Election Authority, the security police and the national police to tackle foreign interference in the 2018 election.[698]

Second, there is an increased focus on, and funding of, media literacy programmes. For example, in 2018, the Swedish government adopted a national initiative to increase media literacy.[699] Further, September 2019, the Swedish government tasked the Swedish Media Council with strengthening media literacy through a new media literacy programme, in order to counter disinformation and propaganda.[700] As the European Parliament study has noted, Sweden has increased funding for new media literacy programmes, where as part of the official school education in Sweden, resources are dedicated to the education of future voters and citizens by means of developing their critical thinking, and critical perception of propaganda and disinformation.[701]

Third, there are collaborative media programmes to combat disinformation. For exmaple, Swedish Television, and two of the Sweden's largest newspapers Dagens Nyheter and Svenska Dagladet, and Swedish Radio, are collaborating in order to combat disinformation and raise awareness about evaluating information and the sources it comes from.[702] The Swedish government has also, through the Swedish Innovation Authority, Vinnova, injected 13.5 million krona (1.3 million euro) into a new digital platform designed to prevent the spread of false news stories online. Funded in collaboration with Swedish Television and other Swedish broadcasters, the platform contains three functions to help citizens filter news: An "automated news assessment service" for evaluating news, a "personalized engine" for counteracting filter bubbles, and a "fact assistant" for automating fact-checking processes and discarding fake and irrelevant news.[703]

Finally, there are national security programmes. The Swedish Security Service released a report on its activities in the run up to the 2018 election, and attempts to influence confidence in the election process. This included fake social media accounts, and disinformation spread via social media with the aim of polarizing society before the elections. The Security Service dedicated extensive resources to information, education and cooperation in order to increase awareness of the fact that influence operations aiming to damage public confidence in the election process and democratic system may happen.[704] Fourth, the

696 Swedish Civil Contingencies Agency, '*Countering information influence activities – A handbook for communicators',* 2019, MSB, https://rib.msb.se/filer/pdf/28698.pdf.

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 Govenrment 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 Contribution to the Member States of the European Union to strengthen the labour market for the provision of information and communication services, Diary number: Ku2019/01659/MD, 27 September 2019, https://www.regeringen.se /regeringsuppdrag/2019/09/uppdrag-till-statens-medierad-att-forstarka-arbetet-for-okad-medie--och-informationskunnighet/

701 Ibid., 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

Swedish Defence Research Agency has conducted research on the role of automated accounts on Twitter during the election campaign found a substantial presence of bots engaging in the Swedish political debate.[705]

iii. Political advertising[706]

1. Newspapers and broadcasting

Johansson has noted that there are 'few regulations' on election campaigning in Sweden generally, and little on political advertising in particular.[707] There is no specific regulation of political advertising in newspapers, but the press has to consider the Freedom of the Press Act, which has rules on defamation. Further, political advertising must be consistent with Sweden's Fundamental Law on Freedom of Expression, which has provisions on expressing contempt for groups based on race, etc.

Notably, while Sweden had a long history of prohibiting political advertising in broadcasting, in 2006, following the switch to a digital terrestrial broadcast system, political advertising was permitted on the commercial broadcaster TV4. Since then, under the Radio and Television Act 2010, political advertising is not regulated for television, unless it is part of the licence concession.[708] Thus, the Radio and Television Act 2010 provides that "[i]n broadcasts subject to conditions of impartiality, there may be no messages broadcast at the request of a third party which are aimed at gaining support for political or religious opinions or opinions regarding labour market issue."[709] Further. the Elections Act does not contain specific provisions relating to political advertising.[710] Johansson has detailed the Swedish experience with political advertising on television since deregulation in 2006.

2. Internet services

There is also no specific regulation of political advertising carried or facilitated by internet services. The OSCE Election Expert Team's report on the 2018 Swedish elections noted that political parties' expenses "related to campaigning in social media are much higher than in previous elections."[711] An academic report from the London School of Economics (LSE) on the 2018 Swedish elections found "[n]o bots or amplification tactics that could be tied to the Kremlin were detected",[712] and there was no mention of the use of political advertising by malign interests.

F. United States[713]

i. General characteristics

The current global discussion on disinformation can be mainly traced back to the 2016 US presidential election. As detailed in the US Special Counsel's Report on interference in the 2016 US presidential election, there was foreign interference in the election through the use of internet services.[714] Crucially, the

705 https://www.foi.se/rapportsammanfattning?reportNo=FOI%20MEMO%206458.
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 Ibid., p. 271.
709 Radio and Television Act 2010:696, Chapter 5, section 6, http://www.mprt.se/documents/styrdokument/radio%20and%20television%20act.pdf/.
710 The Elections Act (2005:837), https://www.government.se/49150c/contentassets/4e2fdee5a8e342e88289496d34701aec/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.

Report detailed how a Russia-based group engaged in a 'social media campaign designed to provoke and amplify political and social discord in the United States', and the group's operations included the 'purchase of political advertisements on social media in the names of U.S. persons and entities'.[715] The group operated Facebook groups and Instagram accounts that had 'hundreds of thousands of U.S. participants', and controlled Twitter accounts that had 'tens of thousands' of followers.[716] In addition, the current US president Donald Trump routinely used the term 'fake news' to disparage the media during the election campaign, and also during his presidency.

In terms of political advertising carried/facilitated by internet services, it should be noted that there are many state laws imposing transparency rules on online political advertising. Importantly, while it is widely-known that protection of freedom of speech under the First Amendment is arguably one of the strongest worldwide, it should be emphasised that the US Supreme Court has held that transparency rules are fully consistent with the First Amendment: disclaimer requirements 'may burden may burden the ability to speak, but they do not prevent anyone from speaking',[717] and instead 'ensure that the voters are fully informed about the person or group who is speaking'.[718]

ii. Disinformation regulation

The US treats disinformation as a national security issue, although there are also state-level measures on media literacy programmes.[719] In late 2016, the US enacted the Countering Foreign Propaganda and Disinformation Act, as part of the National Defense Authorization Act 2016. The Act does not regulate disinformation, but rather allocated $120 million in funding to the US State Department to create an agency 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'.[720]

Notably, in order to expressly mitigate the effectiveness of efforts by foreign entities to influence United States elections through the use of social media bots to spread misinformation and propaganda, there is currently a proposal. The Bot Disclosure and Accountability Act is designed to regulate the use of automated software programs intended to impersonate or replicate human activity on social media.[721] The law would task the Federal Trade Commission (FTC) with defining the term "automated software program or process intended to impersonate or replicate human activity online" broadly enough so that the definition is not limited to current technology. The law would also require the FTC to ensure social media providers establish and implement "policies and procedures" to require users to publicly disclose the use of any automated software program or process intended to impersonate or replicate human activity online on the social media website. In addition to the disclosure rule, social media companies would be placed under an obligation to implement (a) a process to take reasonable "preventative and corrective action to mitigate" efforts by a user to use an automated software program or process intended to impersonate or replicate human activity online without disclosure; and (b) a process to remove posts, images, or any other online activity of a user or profile making use of an automated software program or process intended to impersonate or replicate human activity online that is not in compliance with the disclosure rule.

At state level, there has been some new legislation targeting the use of bots, such as California's SB 1001, makes it 'unlawful for any person to use a bot to communicate or interact with another person in Cali-

715 Ibid., p. 4.
716 Ibid., pp. 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_Initatives_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.

fornia 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] However, there is no liability where the person 'discloses that it is a bot'. The law also does not impose a duty on service providers of online platforms, including, but not limited to, Web hosting and Internet service providers.

Further, there is considerable legislation on foreign influence. First, campaign finance law prohibits foreign nationals from making contributions, donations, expenditures, or other disbursements in connection with federal, state, or local candidate elections, and prohibits anyone from soliciting, accepting, or receiving such contributions or donations.[723] Second, foreign nationals are also barred from making "an expenditure, independent expenditure, or disbursement for an electioneering communication."[724] However, the term expenditure does not include any news story, commentary, or editorial distributed through the facilities of any broadcasting station, newspaper, magazine, or other periodical publication, unless such facilities are owned or controlled by any political party, political committee, or candidate.[725]

Finally, a separate task force has been set up in the United States to combat, among other things, the spread of disinformation by foreign influences, the Foreign Influence Task Force.[726] In the United States, the Department of Justice has charged the Russian woman Elena Alekseevna Khusyaynova for interfering in the 2016 presidential elections.[727] The text is entitled '*Conspiracy to defraud the United States'.*[728] In full, there is a *federal crime,* if: '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'. This includes influencing the elections. Elena Alekseevna Khusyaynova worked as a financial assistant for the IRA and GlavSet, Russian troll farms, among others. As a member of the conspiracy, she was suspected of drawing up fake accounts, '*to address divisive U.S. political and social issues or advocate for the election or electoral defeat or particular candidates*[729]'. The case is still pending and the companies themselves are also being prosecuted by the FBI.

iii. Political advertising

Under US federal and state law, certain paid political advertising is required to include what is called a "disclaimer", which is a statement that identifies the person who paid for a communication and whether the communication was authorised by a political candidate.[730] As mentioned above, as strong as the First Amendment's guarantee of freedom of speech is, the US Supreme Court has held that disclaimer requirements are fully consistent with the First Amendment: disclaimer requirements "may burden may burden the ability to speak, but they do not prevent anyone from speaking,"[731] and instead "ensure that the voters are fully informed about the person or group who is speaking".[732]

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.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001. 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, par. 16. https://www.justice.gov/usao-edva/press-release/file/1102591/download.

730 See 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 (internal quotations omitted).

732 Citizens United v. Federal Election Commission, 558 U.S. 310 (2010), 368.

1. Newspapers and broadcasting

Paid political advertising is permitted in newspapers. However, under the Federal Election Campaign Act, and Federal Election Commission (FEC) regulations, certain political advertisements in newspapers must include a statement that identifies the person who paid for the political advertisement and whether it was authorised by a candidate.[733] Further, "[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]

Paid political advertising is permitted on television. However, under the Federal Election Campaign Act, FEC and Federal Communications Commission (FCC) regulations,[735] there are disclosures rules for political advertisements on television, including that some must include "in a clearly spoken manner, the following audio statement: '[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. Internet services

Paid political advertising is permitted online. However, under the Federal Election Campaign Act, and FEC regulations, all "public communications" that expressly advocate the election or defeat of a clearly identified candidate, and all public communications that solicit any contribution, require a disclaimer that identifies the person who paid for a communication and whether the communication was authorized by one or more candidates.[737] Public communications include electioneering communications and any other form of general public political advertisement, including "communications placed for a fee on another person's website".[738] Notably, the FEC found in its Advisory Opinion 2017-12, that a non-profit organisation must include disclaimers on its paid Facebook image and video advertising which expressly advocated the election or defeat of clearly identified federal candidates.[739]

In June 2019, the FEC published a proposal for a new rule on online political advertising disclaimers. The proposed rule would extend the definition of general public political advertising to include "(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] Also, in May 2019, a bipartisan federal Honest Ads Act bill was published, which is designed to improve "disclosure requirements for online political advertisements".[741]

3. State regulation of political advertising

In addition to US federal law, a number of US states have enacted new legislation targeting political advertising on internet services. Notably, some internet services have stopped allowing political advertising for elections in US states, such as Google Inc., which no longer allows political advertisements on its platform for state and local elections in Maryland, New Jersey, Nevada, and Washington.[742] Microsoft Inc.

733 52 U.S. Code § 30120, https://www.law.cornell.edu/uscode/text/52/30120. See also, 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.
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 See: 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).

also announced that it was no longer accepting political candidate and ballot measure advertisements in the United States, due to "regulators from states across the country have taken new steps to bring additional transparency and accountability to political advertising."[743] In April 2019, Microsoft Inc. announced that it had made the decision to "disallow advertising for election related content, political parties, candidates, and ballot measures globally".[744] Further, in December 2018, Facebook Inc. and Google Inc. paid a $455,000 fine to settle a lawsuit brought by the Washington state Attorney General, for failing to abide by Washington state laws on political advertising transparency.[745]

Three examples of state laws are illustrative: in 2018, California enacted the Social Media Disclosure Act,[746] which requires political advertising on online platforms to include a disclosure on who paid for the advertisement; and requires platforms to keep a publicly available database of the political ads. In 2018, Maryland enacted similar legislation in its Online Electioneering Transparency and Accountability Act.[747] While New York state also enacted its Democracy Protection Act,[748] which amended New York election legislation to require paid internet and digital political advertisements be held to the same disclosure and attribution standards as all other traditional media outlets.

These state laws provide helpful legislative definitions of online platforms, and possible policy options for the regulation of political advertising, including transparency rules.

G. Canada

i. General characteristics

Similar to other governments, the Canadian government considers tackling disinformation as a 'priority'.[749] The measures adopted include allocating funding to the Digital Citizen Initiative, which is a is a multi-component strategy that aims to support democracy and social cohesion in Canada by building citizen resilience against online disinformation.[750] Further, a parliamentary report was also published in late 2018 entitled *Democracy Under Threat: Risk and Solutions in the Era of Disinformation and Data Monopoly*.[751] Notably, Canada enacted legislation in 2018 targeting online political advertising under the Elections Modernization Act, discussed below.

ii. Disinformation regulation

The parliamentary report mentioned above made a number of recommendations concerning disinformation. First, the government should '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] Second, there should be a duty imposed on platforms to (a) to clearly label content produced automatically or algorithmically

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 Ibid.
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.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2188.
747 See: http://mgaleg.maryland.gov/webmga/frmMain.aspx?id=sb0875tab=01id=billpageab=subject3s=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.
750 Ibid.
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.

(e.g. by 'bots'); (b) to identify and remove inauthentic and fraudulent accounts impersonating others for malicious reasons; (c) o adhere to a code of practices that would forbid deceptive or unfair practices and require prompt responses to reports of harassment, threats and hate speech and require the removal of defamatory, fraudulent, and maliciously manipulated content (e.g. "deep fake" videos). The government launched a Digital Charter in 2019, which includes that the Government of Canada will defend freedom of expression and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institution.[753] The Candian government's Department of Canadian Heritage is also injecting $19.4 million over four years in a new Digital Citizen Research Program to help Canadians understand online disinformation, and $7 million to promotes civic, news and digital media literacy.[754]

iii. Political advertising

1. Press and broadcasting

Paid political advertising is permitted in newspapers. However, section 282.4 of the Canada Elections Act (introduced by the Elections Modernization Act 2018) prohibits the selling of "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] Also, paid political advertising is permitted on television, but where paid advertising time is sold to any party or candidate, advertising time must be made available on an equitable basis to rival parties and candidates.[756]

2. Internet services

As mentioned above, in late 2018, Canada enacted the Elections Modernization Act, which included new obligations on online platforms concerning online political advertising registries.[757] The Act provides that an 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] Notably, Google Inc. announced that political advertising would not be allowed on Google platforms during the 2019 Canadian federal elections from June - October 2019.[759]

The Act also includes a number of expenditure-reporting rules, including reporting requirements for 'third parties' engaging in partisan activities, partisan advertising, and election advertising. It also has rules on 'undue influence by foreigners', which limits the permitted election activities of foreign individuals, political parties, groups and governments.[760] Finally, Canada's Elections Modernization Act prohibits selling advertising space (including online platforms) for election advertising to foreign parties, groups or governments.[761]

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. See also 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 Section 325.1(2).
759 See: 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 - Institute for Information Law
P.O. Box 15514, 1001 NA Amsterdam, the Netherlands

https://www.ivir.nl/