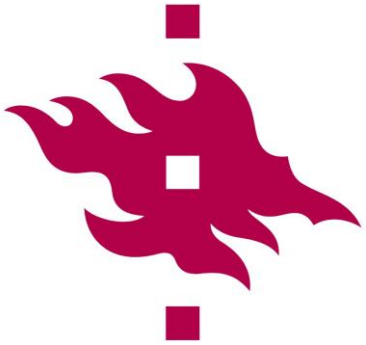

UNIVERSITY OF HELSINKI
FACULTY OF LAW

Online political advertising and disinformation during elections: Regulatory framework in the EU and Member States

MIIKKA HILTUNEN

LEGAL STUDIES RESEARCH PAPER SERIES
Paper No 68

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

OIKEUSTIETEELLINEN TIEDEKUNTA
JURIDISKA FAKULTETEN
FACULTY OF LAW

Online political advertising and disinformation during elections:

Regulatory framework in the EU and Member States

Miikka Hiltunen*

Abstract

Online political advertising and its implications for liberal democracies has become a topic of considerable scholarly and regulatory interest in recent years. The report is guided by the question of how online political advertising is regulated in Europe, especially in the context of elections but also more generally. Its aim is to map the existing, and to some extent upcoming, regulatory framework of online political advertising in the EU and in selected Member States of Germany, France, Spain, Ireland and Poland. After a brief analysis of key concepts, the report maps the EU regulation of data protection and electronic commerce, and other complementary regulation within the Union's competence. Lastly, the report contains the five case studies of Member State election and online media law. While the relevant EU law is in flux with new regulatory initiatives being processed in the fields of data protection, e-commerce and artificial intelligence, uncertainties also remain concerning the interpretation of existing laws, for instance, on data protection obligations and intermediary liability. In turn, the addressed Member States currently a lack proper electoral and media law framework that would systematically take into account the deployment of online services in the dissemination of election propaganda. However, there is increasing attention paid to online services by national regulators that focuses primarily on information disseminated via the largest online services.

* Doctoral Candidate, Erik Castrén Institute of International Law and Human Rights, Faculty of Law, University of Helsinki. Email: miikka.hiltunen@helsinki.fi. I wish to thank Prof. Päivi Leino-Sandberg, Prof. Susanna Lindroos-Hovinheimo and Sam Wrigley for their insightful comments and Marta Paricio Montesinos for her invaluable research assistance.

This report is a deliverable of the 'Information in the EU's Digitalized Governance (INDIGO)' project. The project INDIGO is financially supported by the funding organisations AEI, AKA, DFG, FNR involved in the NORFACE Joint Research Programme on Democratic Governance in Turbulent Ages, which is co-funded by the European Commission through Horizon 2020 under grant agreement No 822166.

Table of Contents

Introduction **1**
Aim and scope of the report 1
Structure of the report 2
PART I: Conceptual framework **4**
Disinformation 4
Disinformation in different contexts 7
Commercial communications online 8
Online political advertising 11
Summary of conceptual framework 13
PART II: EU Law – Regulation of the Digital Single Market **14**
Data protection 14
Data collection under GDPR 14
Profiling and automated decision-making under GDPR 20
ePrivacy Directive 25
Data Governance Act 26
Electronic commerce 27
e-Commerce Directive 27
Digital Services Act 29
Media regulation 31
Artificial Intelligence Act 33
Unfair commercial practices 35
Self-regulation 36
PART III: Member State Law – Electoral and media regulation **39**
Media pluralism and freedom of expression under the ECHR 40
Germany 43
France 46
Spain 50
Ireland 53
Poland 56
Conclusive Summary **60**
References **62**

Introduction

Aim and scope of the report

The use of online services to influence and threaten democratic processes and spread disinformation have become a focus of much attention during the last five years both in Europe and in the US. In particular, a number of high-profile incidents such as the operations of Cambridge Analytica around the 2016 US presidential elections[1] and alleged Russian interference into the UK elections[2] have spurred efforts to understand the effects of online influence campaigns.[3] As part of such efforts, online political advertising has received increased attention from scholars and civil society observers.[4] Consequently, there is an increasing demand from these actors for responses from European policy makers and regulators.[5]

[1] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' *The Guardian* (17 Mar 2018) <www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 6 Apr 2021.

[2] UK Digital, Culture, Media and Sport select committee, 'Disinformation and 'fake news': Final Report' (18 Feb 2019) paras 240–273 <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179104.htm> accessed 6 Apr 2021.

[3] See e.g. Lisa-Maria N Neudert, 'Computational Propaganda in Germany: A Cautionary Tale' (2017) University of Oxford Computational Propaganda Research Project Working Paper No. 2017.7 <www.oii.ox.ac.uk/blog/computational-propaganda-in-germany-a-cautionary-tale/> accessed 6 Apr 2021; Dipayan Ghosh and Ben Scott, '#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet' (23 Jan 2018) New America Policy Paper <www.newamerica.org/pit/policy-papers/digitaldeceit/> accessed 6 Apr 2021; and Camille François, 'Actors, Behaviors, Content: A Disinformation ABC Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses' (20 Sep 2019) Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression Working Paper <www.ivir.nl/twg/publications-transatlantic-working-group/> accessed 6 Apr 2021. For summaries of disinformation incidents, see e.g. Alice Marwick and Rebecca Lewis, 'Media Manipulation and Disinformation Online' (15 May 2017) Data & Society Report, 50–56 <https://datasociety.net/library/media-manipulation-and-disinfo-online/> accessed 6 Apr 2021; and Judit Bayer and others, 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States' (Feb 2019) Study commissioned by European Parliament's LIBE Committee, PE 608.864, 188–195. For an earlier exploration of influencing voters through online media, see Jonathan Zittrain, 'Engineering an Election' (2014) 127 Harvard Law Review Forum 335.

[4] See e.g. van Hoboken and others, 'The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising' (Dec 2019) Final Report, Institute for Information Law (IViR), University of Amsterdam; and Frederik J Zuiderveen Borgesius and others, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14(1) Utrecht Law Review 82.

[5] See e.g. High Level Expert Group, 'A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation' (Mar 2018) 35 <https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en> accessed 23 Mar 2021; Jean-Baptiste Jeangène Vilmer and others, 'Information manipulation: A challenge for our democracies' (Aug 2018) Report to the Minister for Europe and Foreign Affairs, 167–183; Claire Wardle and Hossein Derakhshan, 'Information Disorder: Toward an interdisciplinary framework for research and policymaking' (Sep 2017) Council of Europe report DGI(2017)09, 82; and Bayer and others, 'Disinformation and propaganda', 141–152. Bayer and others advocate regulatory action under the label of 'militant democracy'. Ibid 141.

However, prior to such responses it is often advisable to see how the regulatory structure already in place relates to new information and communication technologies.

The report is guided by the question of how online political advertising is regulated in Europe, especially in the context of elections but also more generally. Its aim, therefore, is to map the framework of existing and to some extent also the upcoming regulation of online political advertising in the European Union (EU) and in selected Member States. Additionally, to deliver a clear mapping exercise, it is first important to provide some conceptual rigor for the analysis. The preliminary analysis of key concepts serves as an analytical framework for understanding the fluid and interconnected phenomena of disinformation and online political advertising. In other words, clarifying the conceptual framework lays out the basis for the further analysis of the regulatory framework.

Structure of the report

Firstly, this report analyses relevant concepts and then locates the respective regulatory competences in the process of online political advertising in Part I: Conceptual framework. This part also sets out the scope and structure of the upcoming analysis of the regulatory field in more detail. The remainder of the report strives for offering an overview of regulation both on the EU level and in selected Member States. Thus, it is structured to follow the two-level regulatory system of the EU.

The operations of digital service providers, including data processing and profiling as related to data protection, have been considered to largely lie within the regulatory competence of the EU, as parts of the internal market project, often referred to as the Digital Single Market.[6] If the EU regulates these activities, it very likely affects political campaigns' and public issues advertisers' possibilities to disseminate their messages online. I address the regulatory framework on the EU level in Part II: EU Law – Regulation of the Digital Single Market.

In turn, the regulation of democratic processes and political actors such as campaigns is primarily within the competence of Member States.[7] Therefore, it is possible to intervene in online political advertising also on this second regulatory level. I address the regulatory

[6] However, Treaty on the Functioning of the European Union (TFEU) contains a specific article of competence for data protection. Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, Art 16.

[7] Commission, 'Tackling online disinformation: a European Approach' COM(2018) 236 final, 3.

framework on the Member State level in Part III: Member State Law – Electoral and Media Regulation. Not all the Member States are included here, but instead the analysis focuses on a selection of five Member States. These have been chosen by the aim of reaching roughly equal representation of different parts of Europe but also with an eye to the respective populations of Member States. The included Member States are Germany, France, Spain, Ireland, and Poland. Also, even if Member States' regulation would not implicate EU law, their regulation can still be contrasted with another supranational legal framework, that is, the European Convention on Human Rights (ECHR) and its interpretation by the European Court of Human Rights (ECtHR).[8] As freedom of expression and information is often implicated both in the online context and in political processes, the relevant jurisprudence of the ECtHR on the regulation of political advertising will be visited in the third part of the report as well. Finally, a brief summary is presented in Conclusive Summary. However, given its somewhat descriptive focus, the report does not end with a detailed list of 'policy prescriptions' but it rather orients normative regulatory endeavors of the subject matter. Thus, it should serve as a basis for deeper normative analyses.

The source material of the report firstly consists of legal materials of the EU, ECHR and relevant Member States. Secondly, the report relies on EU policy documentation, earlier reports commissioned by different EU bodies and other authoritative entities, and reports produced by transnational organizations and independent research and civil society initiatives. Especially the analysis of conceptual framework relies on the existing policy contributions and analyses to make the report align with ongoing policy and scholarly discussions. Finally, the analysis is complemented with insights from scholarship in the fields of law, policy, and media and communication studies.

[8] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended).

PART I: Conceptual framework

As mentioned, it is essential to start with some conceptual groundwork, especially as the policy and regulatory discussions around disinformation are buzzing with terms whose respective meanings within the realms of law or policy are not necessarily intuitive.[9] The first sub-chapter defines the broad, umbrella-like term of 'disinformation'. The second sub-chapter identifies different legal contexts in which it is possible to situate disinformation and then proceeds to define online political advertising and online political micro-targeting and connects disinformation with online advertising.

Disinformation

While in policy discussions and scholarship the phenomenon labelled 'disinformation' has been defined in various ways, many of them roughly share the same basic elements. One authoritative definition is by the European Commission, which conceptualized disinformation 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'.[10] Prior to the Commission's communication on the European approach to disinformation, the independent ad-hoc High Level Expert Group (HLEG) set up by the Commission had put forward a highly similar definition in its final report. HLEG conceptualized disinformation as 'false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit'.[11]

From the definitions, three shared elements arise. Firstly, there is the objective element of verifiable falsity or misleading character of information. By contrast, misleading information

[9] Joshua A Tucker and others, 'Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature' *Hewlett Foundation* (Mar 2018) 55.

[10] Commission, 'Tackling online disinformation: a European Approach' COM(2018) 236 final, 3–4. Later in December 2020, the Commission furthered a slightly simplified definition in the EU Democracy Action Plan: '[D]isinformation is false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm'. Commission, 'On the European democracy action plan' COM(2020) 790 final, 18.

[11] High Level Expert Group, 'A multi-dimensional approach to disinformation' 10.

'is not false, but simply exaggerated, biased or presented in a very emotional way'[12] or 'genuine information presented in the wrong context'.[13]

Secondly, one can point out three 'phases' in the trajectory of disinformation: creation, presentation, and dissemination. A report commissioned by the Council of Europe (CoE) identified the phases of creation, (re)production, and distribution of disinformation. These seem to correspond with the activities of creation, presentation and dissemination included in the Commission's definition. In the second presentation phase of disinformation, the message first created 'is turned into a media product' such as pieces of news or social media posts. Distribution means the phase where the message is publicized.[14] While most attention is paid to the distribution of disinformation, differentiation between phases is important since different actors may be involved in earlier phases of the trajectory. The breakdown into phases can reveal this plurality of actors involved in disinformation phenomenon.[15] For instance, messages created by some may be turned to media products by others, and finally, a variety of different actors may contribute to the dissemination of information. These disseminators may be ordinary people using Internet who share and click links through different services, or companies that facilitate technological tools for the dissemination of media products.

Thirdly, there is the subjective element of the intention of the actor involved. For the Commission, the intention must be to deceive the public or to gain economic profit, while for the HLEG the intention must be to cause public harm or gain profit. By contrast, the intention of economic gain is not included in the definition of the CoE report, which defines disinformation as '[i]nformation that is false and deliberately created to harm a person, social group, organization or country'.[16] However, the intention to profit is important because it recognizes that the dissemination of disinformation is not solely a politically motivated endeavor but has an economic aspect as well.[17] False information may be disseminated online solely to create advertising revenue and the economically motivated actor may be entirely disinterested in the politically implicated content itself. One notable case in this regard is the

[12] Jean-Baptiste Jeangène Vilmer and others, 'Information manipulation: A challenge for our democracies' (Aug 2018) Report to the Minister for Europe and Foreign Affairs, 20.

[13] Judit Bayer and others, 'Disinformation and propaganda' 122.

[14] Wardle and Derakhshan, 'Information Disorder' 23.

[15] ibid 23.

[16] ibid 20.

[17] Commission, 'European Commission Guidance on Strengthening the Code of Practice on Disinformation' COM(2021) 262 final, 2.

'Macedonian teenagers case' before the US presidential election in 2016.[18] If the information meets the other criteria of disinformation, by the Commission definition that information is still disinformation even though the actor does not intent to cause public harm. The HLEG definition states that where profit is intended there would be no more need to look for public harm, whereas the Commission's definition requires that for purely profit-seeking dissemination of falsehoods there must still be the objective chance for public harm. In that sense, the Commission's definition is slightly narrower.

Intention is sometimes thought to differentiate disinformation from *mis*information, which is defined as 'misleading or inaccurate information shared by people who do not recognize it as such'[19] or information 'that is false, but not created with the intention of causing harm'.[20] This report adheres to this distinction and does not focus on unintentional sharing of false information. It is good to point out, however, that the same information can be classified as disinformation when it is shared to cause public harm or to profit, but misinformation when that same information is, for instance, further shared by social media users who do not know it is false.[21] Through sharing, people may unintentionally amplify disinformation.[22]

The notion of 'public harm' in these definitions merits closer examination as well. According to the HLEG, 'harm includes threats to democratic political processes and values, which can specifically target a variety of sectors, such as health, science, education, finance and more'.[23] In turn, the CoE report's definition seems to include a broader scope of harms since it includes harm to 'a person, social group, organization or country'.[24] In their report on disinformation presented to the Dutch Ministry of the Interior and Kingdom Relations, van Hoboken and others note that in many definitions 'it remains unclear what exactly is meant by this [harm]'. However, they see that harm can contain 'damaging public debate, democratic processes, the

[18] Samanth Subramanian, 'Inside the Macedonian Fake-News Complex' *WIRED* (15 Feb 2017) <www.wired.com/2017/02/veles-macedonia-fake-news/> accessed 16 Mar 2021. For another example regarding Spain, see also, Fernando Peinado, 'The business of digital manipulation in Spain' *El País* (24 May 2018) <https://english.elpais.com/elpais/2018/05/24/inenglish/1527147309_000141.html> accessed 16 Mar 2021.

[19] High Level Expert Group, 'A multi-dimensional approach to disinformation' 10.

[20] Wardle and Derakhshan, 'Information Disorder' 20. Similar delineations are followed by e.g. Vilmer and others, 'Information manipulation: A challenge for our democracies' 20; Commission, 'On the European democracy action plan' COM(2020) 790 final, 18; and Bayer and others, 'Disinformation and propaganda' 26.

[21] Judit Bayer and others, 'Disinformation and propaganda', 26.

[22] High Level Expert Group, 'A multi-dimensional approach to disinformation' 10.

[23] ibid 10.

[24] Wardle and Derakhshan, 'Information Disorder' 20.

open economy or national security'.[25] Thus, the notion of harm seems to open disinformation to be thought of in a variety of contexts. This has some important implications for the relation between disinformation and law, which I address in more detail below.

Disinformation in different contexts

So far, we have found out that disinformation is a wide and complex phenomenon that opens in many directions. Therefore, Hoboken and others note that disinformation is, and should be, understood as a policy term.[26] Legal analysis often requires a conceptually crisper framework than policy discussions, and thus, for such analysis it is advisable for disinformation to be broken down to different contexts. For the purposes of this report, the breakdown to different contexts provides a useful tool for delimitation of inquiry. The breakdown also enables the re-focus on the notion of 'public harm' in the Commission's definition of disinformation. Public harm may be a challenging term for legal conceptualization. Different contexts can help to zoom in from disinformation as an umbrella policy term to different harms that are more specific and thus translate it better into legal vocabulary.

Hoboken and others identify four imbricated contexts in which one can approach disinformation. It can be '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'.[27] Firstly, the context of news is related to the (pseudo)journalistic content and journalistic standards, secondly, disinformation as extremist expression can be understood for instance in terms of libel law and incitement to violence. Thirdly, the context of foreign influence formulates disinformation as a national security issue, or 'hybrid threat'. Hoboken and others note that a lion share of attention to disinformation has been within the context of foreign influence.[28] For instance, while the Commission's European Approach to Disinformation took a somewhat generic stance toward the phenomenon, the subsequent EU Action Plan against Disinformation paints disinformation as a national security issue. Here the primary threat is influence from foreign states, most notably from Russia.[29]

[25] van Hoboken and others, 'The legal framework on the dissemination of disinformation' 17.

[26] ibid 15, 123.

[27] ibid 23.

[28] ibid 26.

[29] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final, 2–3.

Nevertheless, in this report I address disinformation primarily in the fourth context mentioned by Hoboken and others, namely that of commercial expression, and even more precisely, online political advertising. I have made this decision to delineate the scope more neatly around political advertising in the times of elections. This does not mean other contexts would be (or could be) left aside entirely or that hate speech, conduct of the press, or foreign state influence would be irrelevant to election integrity. Covering the legal implications pertaining to different forms of hate speech, national security and hybrid threats, and journalistic content would, however, expand the relevant regulatory framework beyond the title and purpose of this report.

It should be stressed that disinformation is not tied to any specific medium.[30] Relevant online information technologies for disinformation include search engines, web hosting services, electronic communication, social networking, online marketplaces, media sharing platforms, rating and review services, online games and so on.[31] However, the choice to focus on political advertising limits the relevant services further to those relying on advertising as their business model. This means that the primary services focused are for instance social networking platforms, search engines, and online advertising networks. Again, the legal treatment may vary across services, which is considered more closely below in Part II. In the next sub-chapter, I briefly turn to address the issues to which the context of online political advertising guides our interest.

Commercial communications online

According to van Hoboken and others, the link between disinformation and commercial communications:

> should take into account the commercial interests of the disseminator […], 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*

[30] For instance, there exists a lot of research on how legacy media has participated in disseminating propaganda. Alice Marwick and others, 'Critical Disinformation Studies: A Syllabus' (2021) Center for Information, Technology, & Public Life (CITAP), University of North Carolina at Chapel Hill, 4–5 <https://citap.unc.edu/critical-disinfo> accessed 6 Apr 2021.

[31] van Hoboken and others, 'The legal framework on the dissemination of disinformation' 32–34.

advertising industry and the dissemination of disinformation are closely linked.[32] (Emphasis added)

Put most simply, online services offer preferential placement for actor's messages on users' online interfaces, usually in different information 'feeds'.[33] Therefore, the dissemination of disinformation may be amplified through the advertising tools built in services such as search engines (e.g. Google Search), advert services integrated into websites (e.g. Google AdSense), social networking (e.g. Facebook), micro-blogging (e.g. Twitter), and content aggregation (e.g. YouTube, Instagram).

However, the picture is also more complex. The online advertising business model relies on the assemblage of behavioral data processing techniques for finding preferred audiences for different adverts. While it is not possible to delve deep into the intricacies of the business, it is helpful to identify the basic elements. According to the European Data Protection Supervisor (EDPS), mostly online behavioral data is used to determine the user online experience through 'a three-stage cycle from data collection (a form of data processing under EU law) through profiling to microtargeting or personalisation'.[34] Dobber and others put forward a similar three-step process of micro-targeting that includes '1) collecting personal data, 2) using those data to identify groups of people that are likely susceptible to a certain message, and 3) sending tailored online messages'.[35]

People's data profiles include a myriad of attributes that enable grouping and re-grouping them to valuable audience segments predicted to be receptive to a particular advertiser's messages.[36] Targeting information based on inferences from online behavior comprises the practice of micro-targeting. According to Dobber and others: 'Micro-targeting differs from regular targeting not necessarily in the size of the target audience, but rather in the level of homogeneity, perceived by the political advertiser. Simply put, a micro-targeted audience receives a message tailored to one or several specific characteristic(s)'.[37] For instance, an actor may distill false or misleading information into advertisements and use the Facebook advert

[32] van Hoboken and others, 'The legal framework on the dissemination of disinformation' 25.

[33] Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP 2019) 43–44.

[34] EDPS, 'Opinion 3/2018' 7.

[35] Tom Dobber, Ronan Ó Fathaigh and Frederik J Zuiderveen Borgesius, 'The regulation of online political micro-targeting in Europe' (2019) 8(4) Internet Policy Review 1, 2.

[36] Cohen, *Between Truth and Power* 70.

[37] Dobber, Ó Fathaigh and Borgesius, 'The regulation of online political micro-targeting in Europe' 2–3.

tools to target the group of people Facebook predicts to be 'interested in pseudoscience'.[38] One of the most data-intensive and widely-used advertising models run by online service providers is the so-called Real Time Bidding (RTM), which is based on automated auctioning of advert slots in real time as people use online services.[39] Here, also the price of advert is partly determined by how 'relevant' the online service provider predicts it to be for the respective audience. Adverts that are more relevant are cheaper.[40]

Often on a service, commercial communications are distinguished from 'user-generated content' or 'organic content' that is not sponsored. Yet in practice the line is hard to maintain. Firstly, information not originally produced and disseminated as adverts can be promoted for payment later. Moreover, on social networking sites businesses, political groups and other entities often establish general 'social media presence' to maintain and improve overall reputation quite disentangled from any specific product or advocacy project. Such presence includes the creation of ordinary posts and other content, whose reach may be later enhanced with purchased extra visibility.[41] Advertisers promoting their messages can be 'followed' like others users, and their organic content as well as proper adverts can both be 'liked', 'retweeted', 'upvoted', or 'shared' by users like any information posted by an ordinary person.[42]

Secondly, actors do not necessarily have to buy visibility directly from the service operator, but they can also use indirect means to promote their messages. The delivery of both advertisements and user-generated content seeks to maximize people engagement. Simulated engagement is available for instance from the so-called 'clickfarms' that utilize bots to create simulated engagement,[43] or it can be created by employed people as well.[44] As regards search, 'search

[38] Aaron Sankin, 'Want to Find a Misinformed Public? Facebook's Already Done It' *The Markup* (23 Apr 2020) <https://themarkup.org/coronavirus/2020/04/23/want-to-find-a-misinformed-public-facebooks-already-done-it> accessed 14 Dec 2020.

[39] Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2021) German Law Journal (forthcoming) 3–4 <https://osf.io/preprints/socarxiv/wg8fq/> accessed 11 June 2021.

[40] See e.g. Facebook for Business, 'About ad auctions' <https://en-gb.facebook.com/business/help/430291176997542?id=561906377587030> accessed 19 Mar 2021. For an example on how ad auctions may instantiate significant differences between the ads of different political actors, see Jeremy B Merrill, 'Facebook Charged Biden a Higher Price Than Trump for Campaign Ads' *The Markup* (29 Oct 2020) <https://themarkup.org/election-2020/2020/10/29/facebook-political-ad-targeting-algorithm-prices-trump-biden> accessed 19 Mar 2021.

[41] Cohen, *Between Truth and Power* 83–84.

[42] Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018) 203.

[43] Wardle and Derakhshan, 'Information Disorder' 46.

[44] Vilmer and others, 'Information manipulation: A challenge for our democracies' 84–87.

engine optimization' (SEO) companies seek to 'reverse engineer the moving target of Google's search algorithm in order to modify websites to achieve a higher search rank'.[45] Some of these methods, so-called 'black hat SEO', are not accepted by search engine companies and 'are designed to trick the algorithm and dominate search results for a few hours of the news cycle' before the distortion is corrected by the operator.[46] All the above techniques may involve payment, but not to the service operator.[47] Moreover, the techniques are covert in the sense that they seek to give people the impression that the popularity of promoted information is organic.[48] In sum, the line between commercial communications and 'organic content' in online environments is liquid and easily crossed.

Online political advertising

As regards public harm, in the context of commercial communications many focus on potential harm that especially online political advertising poses for democratic processes.[49] For instance, disinformation 'is likely to intensify before/during significant democratic decision-making processes such as referenda […] and elections'.[50] Interest in political advertising naturally increases close to elections and other decision-making processes as well. This further narrows the focus to commercial communications with political significance. Political advertising can be used 'to persuade, inform, or mobilise, or rather to dissuade, confuse or demobilise voters'.[51] However, when disinformation is combined with elections, undistorted public debate and possibly even the integrity of elections may arguably become under threat.

Broadly speaking, there are two common ways to determine whether an advert is 'political'. Firstly, an actor-based understanding delineates political advertising based on the actor behind the advert. As noted, disinformation includes several actors during the trajectory of the phenomenon. The actor here refers primarily to traditionally political campaigns of parties,

[45] Ghosh and Scott, '#DigitalDeceit' 18.

[46] ibid 17.

[47] van Hoboken and others, 'The legal framework on the dissemination of disinformation' 28–29.

[48] Mark Leiser, 'AstroTurfing, "CyberTurfing" and other online persuasion campaigns' (2016) 7(1) European Journal of Law and Technology 1, 4.

[49] E.g. Judit Bayer, 'Double harm to voters: data-driven microtargeting and democratic public discourse' (2020) 9(1) Internet Policy Review 1, 2–3; Borgesius and others, 'Online Political Microtargeting' 87; and Damian Tambini, 'Internet and electoral campaigns: Study on the use of internet in electoral campaigns' (Apr 2018) Council of Europe study DGI(2017)11, 15 and 18.

[50] Bayer and others, 'Disinformation and propaganda' 29.

[51] Dobber, Ó Fathaigh and Borgesius, 'The regulation of online political micro-targeting in Europe' 2.

coalitions, and candidates which create or commission adverts as media products to be disseminated. In addition to the targeting tools for messages dissemination provided by online services, available strategies for political campaigns may include the purchase of data on citizens from data brokers or the use of digital marketing services from specialized providers such as Blue State Digital or Momentum Campaigns.[52] Of particular concern has been the possibility to tailor campaign messages to suit the preferences of different voter segments (even with contradictory messages).[53]

Secondly, the issue-based conceptualization of political adverts is increasingly important in online contexts. The relative ease of use and inexpensiveness of online promotion tools have placed advertising within the reach of far wider category of actors than during the time where only broadcast and print advertising was available. As Gillespie notes, 'advertisers are no longer just corporate brands and established institutional actors; they can be anyone. Persuading someone through an ad is as available to almost every user as persuading him through a post'.[54] Here, an advert is political if it is about a matter of public interest. Of course, it is again far from clear what issues in society are of public interest. It has been criticized that, at the moment, the important line between political and non-political is often drawn by online service providers themselves.[55]

Despite a lot of attention, it should be noted that, in general, the effects of micro-targeting are hard to verify empirically.[56] Thus, there is a lack of empirical evidence of the actual usage and effectiveness of data-driven campaigning especially in Europe[57] and also behavioral advertising more generally.[58] The lack of such evidence of course does not mean that online political advertising is not or could not be regulated nevertheless.

---

[52] Katharine Dommett, 'Data-driven political campaigns in practice: Understanding and regulating diverse data-driven campaigns' (2019) 8(4) Internet Policy Review 1, 5 and 6–7.

[53] ibid 12.

[54] Gillespie, *Custodians of the Internet* 203.

[55] Mike Ananny, 'Making up Political People: How Social Media Create the Ideals, Definitions and Probabilities of Political Speech' (2020) 4(1) Georgetown Law Technology Review 1, 11–12.

[56] S C Boerman and others, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46 Journal of Advertising 363, 373.

[57] Dommett, 'Data-driven political campaigns in practice' 5. For even more skeptical account on effectiveness, see Jessica Baldwin-Philippi, 'Data campaigning: Between empirics and assumptions' (2019) 8(4) Internet Policy Review 1, 12–13. Regarding Germany see also, Simon Kruschinski and André Haller, 'Restrictions on data-driven political micro-targeting in Germany' (2017) 6(4) Internet Policy Review 1, 16–17, where it was found that only the main parties see the use of data for voter targeting important to their actual campaigns.

[58] For skepticism, see generally, Gilad Edelman, 'Ad Tech Could Be the Next Internet Bubble' *WIRED* (10 May 2020) <www.wired.com/story/ad-tech-could-be-the-next-internet-bubble/> accessed 3 Feb 2021; Jesse Frederik

Summary of conceptual framework

In the above, I have sought to establish the underlying conceptual framework for the upcoming analysis of regulation. I base my conceptualization of disinformation on the definition of the Commission and I stated that I understand disinformation primarily as a policy term. I proceeded to break disinformation down to be thought in different contexts**.** I then directed the focus on disinformation in the context of commercial communications, and more specifically on online political advertising. I lastly set out that the online advertising business model, including political advertising, is overwhelmingly based on the collection (processing) and sorting of behavioral data and conveying tailored information to people based on this data analysis. This can be referred to as political micro-targeting. I also outlined some problems that scholars have associated with political micro-targeting especially during elections.

and Maurits Martijn, 'The new dot com bubble is here: It's called online advertising' *The Correspondent* (6 Nov 2019) <https://thecorrespondent.com/100/the-new-dot-com-bubble-is-here-its-called-online-advertising/13228924500-22d5fd24> accessed 3 Feb 2021; and Tim Hwang, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet* (FSG Originals 2020).

PART II: EU Law – Regulation of the Digital Single Market

Data protection

This part of the report seeks to map the legal framework of EU law. As already explored in Part I, micro-targeting, whether political or not, generally starts with the processing of vast amounts of personal data. Thus, the regulation of data collection and automated profiling of people is a vital part of the legal framework. Specifically, the central pieces of regulation are the General Data Protection Regulation (GDPR)[59] and the Directive on privacy and electronic communications (ePrivacy Directive).[60]

Data collection under GDPR

The GDPR came into force on 25 May 2018. It both facilitates and restricts the processing of personal data of people in the EU, in accordance with its double aim of ensuring data protection as a fundamental right and guaranteeing the free flow of data in the EU.[61] Therefore, the GDPR does not impose absolute prohibitions on data-based political or economic activities but rather governs these practices to ensure that data processing is handled with care and due consideration for the interests of data subjects.[62] In general, data must be processed lawfully, fairly, transparently, for specified and legitimate purpose and in accordance with other data protection principles.[63] As its name suggests, the GDPR is a general regulation exemplified in its wide definition of personal data, which 'means any information relating to an identified or identifiable natural person'.[64] The actor primarily responsible for the lawfulness of data practices is the 'controller', which 'alone or jointly with others, determines the purposes and

[59] Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1. Hereafter in footnotes 'GDPR'.

[60] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

[61] GDPR Art 1(1).

[62] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union general data protection regulation: What it is and what it means' (2019) 28 Information & Communications Technology Law 68, 76–77.

[63] GDPR Art 5.

[64] ibid Art 4(1).

means of the processing of personal data'.[65] In turn, 'processor' is an actor that 'processes personal data on behalf of the controller'.[66]

Firstly, if data collection, which falls under the broad category of 'processing' in GDPR terminology,[67] does not have a lawful basis, it is prohibited.[68] The six lawful bases under the GDPR are (a) data subject's consent, (b) necessity for the fulfillment of a contract, (c) necessity for the fulfillment of a legal obligation, (d) necessity for the protection of the vital interests of the data subject or of another natural person, (e) necessity for the performance of a task carried out in the public interest or in the exercise of official authority, and (f) necessity for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.[69]

What bases in practice would work for political micro-targeting is not clear-cut and depends on the specific actors and strategies involved. Insofar micro-targeting utilizes the data-driven solutions offered by private sector, the most relevant ones could be (a) consent, (b) necessity for the fulfillment of a contract, and (f) legitimate interest of the controller that Hoofnagle and others have described 'the catchall basis' for processing.[70] However, as regards micro-targeting on social media, the European Data Protection Board (EDPB) has stated that 'there are two legal bases which could theoretically justify the processing that supports the targeting of social media users: data subject's consent (Article 6(1)(a) GDPR) or legitimate interests (Article 6(1)(f) GDPR)'.[71] In the practice of online advertising, both consent and legitimate interest are currently relied on.[72] Nevertheless, in the broader electoral context beyond the use of social media and other for-profit online services, the basis of public interest may be relevant as well,

[65] GDPR Art 4(7).

[66] ibid Art 4(8).

[67] ibid Art 4(2).

[68] ibid Art 6(1).

[69] ibid Art 6(1).

[70] ibid Art 6(1)(a, b, f). Hoofnagle, van der Sloot and Borgesius, 'The European Union general data protection regulation' 79, 81; and Frederik J Zuiderveen Borgesius, 'Personal data processing for behavioural targeting: Which legal basis?' (2015) 5 International Data Privacy Law 163, 165.

[71] European Data Protection Board (EDPB), 'Guidelines 8/2020 on the targeting of social media users' para 43. For the same argument in scholarship and concerning micro-targeting in general, see also Borgesius, 'Which legal basis?' 167.

[72] Veale and Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' 20 and 24.

for instance, in the case of political party acting as the sole controller, or when national electoral authorities manage electoral records.[73]

In practice, under the Real Time Bidding advertising model, many website hosts and online service providers currently rely on coded Consent Management Platforms, which are embedded into the user interface and supplied by specialized consultancies. Through these platforms, dozens of 'vendors' in the advertising industry can seek legal basis simultaneously for their processing.[74] Since consent is one of the most important lawful bases for processing, the requirements for a valid consent under the GDPR merit some outlining. Consent 'means any freely given, specific, informed and unambiguous indication of the data subject's wishes'.[75] The EDPB and CJEU have interpreted these requirements of valid consent further. According to the EDPB guidelines, 'freely given' indicates that consent cannot be 'bundled up as a non-negotiable part of terms and conditions' and, in general, attention should be paid to the power imbalances between the controller and data subject.[76] In addition, a controller cannot usually tie its service to the collection of data that is not necessary for the performance of a contract and use consent as basis.[77] Also, consent is not free where there is 'deception, intimidation, coercion or significant negative consequences if a data subject does not consent'.[78] The controller should be able to show that its service allows for withdrawing consent and this does not bring negative consequences to the data subject.[79]

The requirement of specificity demands rigorous specification of different processing purposes and corresponding granularity in consent requests. There should also be '[c]lear separation of information related to obtaining consent for data processing activities from information about other matters'.[80] Specificity is related to the principle of purpose limitation in Article 5, which requires the purpose to be specific and legitimate. EDPB's predecessor, Article 29 Data

[73] Commission, 'Commission guidance on the application of Union data protection law in the electoral context: A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018' (12 Sep 2018) COM(2018) 638 final, 5.

[74] Veale and Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' 24.

[75] GDPR Art 4(11).

[76] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) para 13.

[77] GDPR Art. 7(4); and EDPB, 'Guidelines 05/2020 on consent' paras 14–15 and 25–41. But see para 35, which notes that 'there might be very limited space for cases where this conditionality would not render the consent invalid'.

[78] EDPB, 'Guidelines 05/2020 on consent' para 47.

[79] ibid para 48.

[80] ibid para 55.

Protection Working Party, has earlier clarified that 'a purpose that is vague or general, such as for instance "improving users' experience", "marketing purposes", "IT-security purposes" or "future research" will - without more detail - usually not meet the criteria of being "specific"'.[81]

The element of 'informed' seeks to ensure that the data subject understands what she is agreeing to.[82] Article 13 of the GDPR indicates the minimum information that the controller must provide while asking for consent.[83] Moreover, the information must be presented clearly, that is, the request should be 'in an intelligible and easily accessible form, using clear and plain language'.[84] Controllers cannot present lengthy privacy policies in legal language unintelligible to layperson.[85] Thus, there is some balancing to be exercised 'to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand'.[86]

Finally, the unambiguous indication of the data subject's wishes points to the need of affirmative action of the data subject. The CJEU has stated that the GDPR requires active consent and pre-ticked boxes that the data subject must de-select do not suffice.[87] Likewise, 'merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation'.[88]

We can then move to the basis of controller's legitimate interest. Following the CJEU, it contains three cumulative conditions that must be met:

> First, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal

[81] Article 29 Data Protection Working Party (WP29), 'Opinion 03/2013 on purpose limitation' (WP 203, 2 Apr 2013) 16.

[82] EDPB, 'Guidelines 05/2020 on consent' para 62.

[83] See also GDPR recital 42; and EDPB, 'Guidelines 05/2020 on consent' paras 64–65.

[84] GDPR Art 7(2).

[85] EDPB, 'Guidelines 05/2020 on consent' para 67.

[86] ibid para 69.

[87] Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, EU:C:2019:801, paras 62–65. See also GDPR recital 32, which states that '[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent'. Recently, the CJEU restated parts of its *Planet49* reasoning in Case C-61/19, *Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, EU:C:2020:901.

[88] EDPB, 'Guidelines 05/2020 on consent' para 84.

> data for the purposes of the legitimate interests pursued; and third, the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence.[89]

A legitimate interest of an online service provider that facilitates micro-targeting of adverts could be for instance its right to conduct a business enshrined in Article 16 of the Charter. Furthermore, processing must be necessary in light of such an interest, and finally a balancing exercise between the rights and interests of data subject and controller.[90]

Moreover, and importantly for political advertising, data revealing political opinion is considered extra sensitive, a 'special category of personal data'. Processing such data is prohibited unless an exception applies.[91] As regards online political advertising, the most relevant exceptions could be the qualified 'explicit' consent of data subject, the specific exception for non-profit entities with a political aim, or the fact that the data subject has made the sensitive data 'manifestly public'.[92] However, the applicability of exceptions must again be determined with due regard to context. As regards explicit consent, some extra effort compared to 'regular' consent is needed from the controller. Explicit refers to the manner the consent is expressed by the data subject.[93] Yet, there is no one clearly determined way to obtain such a qualified consent. In the digital context, the EDPB has stated that explicit consent could be obtained through 'an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance "I, hereby, consent to the processing of my data", and not for instance, "It is clear to me that my data will be processed"'.[94]

Political parties and arguably also certain non-governmental organizations (NGOs) with a political aim can base their processing on the exception intended specifically for their activities.[95] This is explicitly prescribed also in recital 56 of the GDPR:

---

[89] Case C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, EU:C:2019:629, para 95. Hereafter in footnotes *Fashion ID*.

[90] Borgesius, 'Which legal basis?' 167. For the use of legitimate interest as basis, see also EDPB, 'Guidelines 8/2020 on the targeting of social media users' (version 1.0, 2 Sep 2020) paras 44–50.

[91] GDPR Art 9.

[92] GDPR Art 9(2)(a, d, e). See also EDPB, 'Guidelines 8/2020 on the targeting of social media users' paras 112–113, considering that the available exceptions for the processing of sensitive data for both the social media provider and an environmental organization would be either explicit consent or that data subject has made the data manifestly public.

[93] EDPB, 'Guidelines 05/2020 on consent' paras 92–93.

[94] ibid para 96.

[95] Dobber, Ó Fathaigh and Borgesius, 'The regulation of online political micro-targeting in Europe' 6.

> Where 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.

Processing must also relate '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'.[96]

As explored in Part I, both disinformation and political micro-targeting involve several actors, especially concerning the dissemination of messages online. How actors' respective roles translate in terms of data protection regulation thus merits a brief consideration. In practice, assigning legal roles to actors involved is not always obvious and the EDPB has underscored careful case-by-case analysis for deciding on the respective roles and responsibilities.[97] In addition to the roles of the controller and processor, the GDPR provides that: 'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation'.[98]

As regards the services of platform companies, the CJEU has considered the question of roles and corresponding obligations concerning data collection and the use of social media. For instance, joint controllership exists between an actor and Facebook where that actor sets up a fan page on Facebook to promote its operations and influences the collection of data by Facebook that occurs when a person visits that Facebook fan page.[99] Similarly, joint controllership exists where a website operator decides to place a social plugin (Facebook 'Like' button) on its website that enables collection and transmission of data relating to the website visitors.[100] Joint controllership does not require access to the collected data by each controller.[101] However, 'the existence of joint responsibility does not necessarily imply equal

[96] GDPR Art 9(2)(d).

[97] EDPB, 'Guidelines 8/2020 on the targeting of social media users' 34–37.

[98] GDPR Art 26(1).

[99] Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, EU:C:2018:388, paras 36–44. Hereafter in footnotes *Wirtschaftsakademie*.

[100] Case C-40/17, *Fashion ID*, EU:C:2019:629, paras 79–85.

[101] ibid para 82.

responsibility of the various operators involved in the processing of personal data'.[102] Therefore, controllership over different processing activities in the processing chain may vary, highlighting again the need for due regard to 'all the relevant circumstances of the particular case'.[103]

The Commission has issued a non-binding guidance to clarify the roles in the electoral context as well. It contains a suite of rules of thumb for determining the actors' roles, corresponding to the scenario 'where political parties are collecting data themselves […] and use the service from data brokers or data analytics companies with the objective to target voters through social media platforms'.[104] Generally, parties or political foundations are controllers, data brokers/data analytics providers processors or joint controllers depending on their level of control over processing, and platform companies are usually joint controllers with other organizations that utilize their services.[105]

Profiling and automated decision-making under GDPR

After data collection, we can then shift attention to automated profiling, which the GDPR defines as:

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[106]

So, as already implied, micro-targeting does not include mere processing of data on political opinion or any other specific category of data but behavioral data in general and on large scale. Then, processing of heterogenous and seemingly innocuous (or meaningless) data, sometimes called 'digital breadcrumbs', may be turned into inferred data that do reveal valuable information on citizens' inclinations as regards for instance voting behavior or prominent public

[102] Case C-210/16, *Wirtschaftsakademie*, EU:C:2018:388, para 43.

[103] ibid.

[104] Commission, 'Commission guidance on the application of Union data protection law in the electoral context' COM(2018) 638 final, 10.

[105] ibid 10–11.

[106] GDPR Art 4(4).

issues.[107] The GDPR understands such activities as 'large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk'.[108]

A specific issue in this regard is that observed data can be processed so that they become a proxy for sensitive data concerning for instance political opinion.[109] The EDPB has clarified that in many cases triggering Article 9 cannot be evaded by inferring sensitive data from non-sensitive:

> Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods.[110]

Further, the EDPB has put forward the following practical scenario:

> A social media provider uses information actively provided by Ms. Allgrove on her social media profile page about her age, interests and address and combines it with observed data about the websites visited by her and her "likes" on the social media platform. The social media provider uses the data to infer that Ms. Allgrove is a supporter of left-wing liberal politics and places her in the "interested in left wing liberal politics" targeting category, and makes this category available to targeters for targeted advertising.[111]

---

[107] EDPS, 'Opinion 3/2018' 8.

[108] GDPR recital 91.

[109] Profiling under the GDPR Art 4(4) means 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

[110] WP29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (last revised and adopted on 6 Feb 2018) 15. See also Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, EU:C:2016:779, paras 39–49, in which the CJEU confirmed that a dynamic IP address registered by the operator of a website was personal data even though it did not directly reveal the identity of a natural person. This was because *its combination with another data* held by a third party enabled the identification of a person behind the IP address.

[111] EDPB, 'Guidelines 8/2020 on the targeting of social media users' 31.

The EDPB considers the above situation as processing special categories of data, which triggers Article 9 requirements, irrespective of whether Ms. Allgrove 'really' is left wing liberal or not, that is, whether she would agree how she is being profiled. It is equally irrelevant that the profile is termed 'interested in' rather than 'supporter of' left wing politics.[112]

Again, it should be noted that the GDPR does not categorically forbid automated profiling or other automated individual decision-making, but it may be subject to specific restrictions. It is further prescribed in Article 22(1) that 'the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, *which produces legal effects concerning him or her or similarly significantly affects him or her*' (Emphasis added). The EDPB has clarified that the 'right' is in fact a general prohibition, which protects the data subject irrespective of subject's invocation of a right.[113] Still, there are exceptions from the prohibition. It is lifted if the decision is necessary for the performance of a contract between a data subject and a controller, or if it is authorized in Union or Member State law, or the data subject has given explicit consent.[114] In case where special categories of data are involved as well, the requirements of Articles 9 and 22 combined leave only explicit consent and legal authorization standing as available exceptions, as necessity for the performance of a contract is not an available exception for processing special categories of data.[115] Even in these lawful cases, however, specific safeguards are mandatory attendants.[116]

In terms of the applicability of Article 22(1) prohibition in the first place, the notion of legal or similarly significant effects is crucial. As noted in Part I, the actual effects of micro-targeted

---

[112] EDPB, 'Guidelines 8/2020 on the targeting of social media users' 31, para 118.

[113] WP29, 'Guidelines on Automated individual decision-making' 19–20.

[114] GDPR Art 22(2).

[115] GDPR recital 71 states: 'Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions'.

[116] GDPR Art 22(3). WP29 refers to recital 71, which states that safeguards 'should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child'. See WP29, 'Guidelines on Automated individual decision-making' 19. The existence and contents of the so-called 'right to explanation' of automated decision-making as part of the safeguards in Art 22 or recital 71 has been a topic of active scholarly debate. See e.g. Sandra Wachter, Ben Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76; Lilian Edwards and Michael Veale, 'Slave to the Algorithm: Why a Right to an Explanation is Probably Not the Remedy You are Looking for' (2017) 16 Duke Law & Technology Review 18; and Maja Brkan and Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas' (2020) 11 European Journal of Risk Regulation 18. For a condensed analysis of the discussions around the GDPR and automated decision-making, see Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34 Computer Law & Security Review 398.

adverts are often somewhat unclear and disputed. Moreover, it has been remarked that the significance of the effects of micro-targeting may depend on whether one adopts individualistic or group-based/systemic perspective.[117] One could argue that maintaining the integrity of elections requires a systemwide perspective and that the possible effects on the democratic system as a whole do not manifest themselves on the level of the individual. The EDPB has considered that while in many cases advert targeting based on profiling does not cross the threshold,[118] '[p]rofiling connected to targeted campaign messaging may in certain circumstances cause "similarly significant effects"'.[119] Similarly, the Commission states that: 'Given the significance of the exercise of the democratic right to vote, personalised messages which have for instance the possible effect to stop individuals from voting or to make them vote in a specific way could have the potential of meeting the criterion of significant effect'.[120] According to the EDPB, the circumstances to be especially considered when making such an assessment are:

- the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- using knowledge of the vulnerabilities of the data subjects targeted.[121]

In sum, it cannot be ruled out that (political) adverts targeted based on profiling of large quantities of different types of data produce 'similarly significant effects' within the meaning of Article 22(1).

Moreover, automated profiling that produces legal or similarly significant effects is treated as high-risk, which in turn imposes some additional primarily procedural obligations on controllers, most notably the requirement to carry out a data protection impact assessment.[122]

---

[117] Lilian Edwards and Michael Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018) 16 IEEE Security & Privacy 46, 47–48.

[118] WP29, 'Guidelines on Automated individual decision-making' 22.

[119] EDPB, 'Statement 2/2019 on the use of personal data in the course of political campaigns' (adopted 13 Mar 2019) 2; and WP29, 'Guidelines on Automated individual decision-making and Profiling' 22.

[120] Commission, 'Commission guidance on the application of Union data protection law in the electoral context' COM(2018) 638 final, 8.

[121] WP29, 'Guidelines on Automated individual decision-making and Profiling' 22.

[122] GDPR Art 35(3)(a).

The impact assessment may imply measures for risk mitigation.[123] In addition, there are rights for data subjects. The rights include, for instance, the right to transparent information[124] and the right to data erasure[125].

Data protection principles themselves may limit some data-intensive practices as well. For instance, political parties buying data from third parties such as commercial data brokers may be against purpose limitation principle.[126] In a similar vein, the principles may play a role in limiting processing, for instance, through 'data protection by design and default' under Article 25. The article obligates controllers to implement appropriate technical and organisational measures, 'which are designed to implement data-protection principles' and which ensure that 'by default, only personal data which are necessary for each specific purpose of the processing are processed'. However, apart from a mention of 'pseudonymisation', it is not prescribed what such technical or organisational measures would more concretely be. The EDPB has sought to elaborate and exemplify compliance measures in a guidance.[127]

Finally, it should be noted that the extent of which GDPR practically hinders or prevents micro-targeting in general is still quite undetermined and the Commission has remarked some deficiencies in the enforcement of the regulation.[128] Specifically:

> Commission consistently stressed the obligation for Member States to allocate sufficient human, financial and technical resources to national data protection authorities. […] Given that the largest big tech multinationals are established in Ireland and Luxembourg, the data protection authorities of these countries act as lead authorities in many important cross-border cases and may need larger

[123] GDPR Art 35(7)(d).

[124] E.g. GDPR Arts 12–13.

[125] GDPR Art 17.

[126] Commission, 'Commission guidance on the application of Union data protection law in the electoral context' COM(2018) 638 final, 6.

[127] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (version 2.0, 20 Oct 2020) 14–28. GDPR Art 25(3) foresees a possibility for certification under Art 42 to demonstrate compliance with data protection by design and default. However, at the time of writing no such certification mechanism had been registered with the EDPB. See EDPB, 'Register of certification mechanisms, seals and marks' <https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en> accessed 15 Apr 2021.

[128] Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' COM(2020) 264 final, 5–6.

resources than their population would otherwise suggest. However, the situation is still uneven between Member States and is not yet satisfactory overall.[129]

ePrivacy Directive

In the European data protection framework, ePrivacy Directive[130] complements the GDPR. Basically, the consent of a recipient is needed for tracking technologies (e.g. so-called 'cookies').[131] However, the directive is being revised and the Commission published its proposal for new ePrivacy Regulation in January 2017.[132] The regulation would extend the scope of the rules to cover new electronic communications services, such as communications services on the internet.[133] I would also reform the rules on the lawful processing of communications metadata and content data in the spirit of the GDPR.[134] Similarly, the requirements for valid consent remained tied to those of the GDPR.[135]

New Articles 9(2) and 10 of the proposal sought to channel people's management of consent on the internet toward browser settings to ease the need for repetitive consenting while browsing.[136] However, the Council agreed its own position in early 2021, deleting the prescriptions for the use of such software from the articles and relegating the encouragement of these solutions to recitals.[137] It also specifically excluded targeted adverts on websites and

[129] ibid 6.

[130] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

[131] Directive on privacy and electronic communications Art 5(3). On the applicability of consent requirements of the GDPR, see EDPB, 'Guidelines 05/2020 on consent' paras 6–7.

[132] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life 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. Hereafter in footnotes 'Proposal for ePrivacy Regulation'.

[133] Proposal for ePrivacy Regulation recitals 11–12.

[134] ibid Arts 5–11.

[135] ibid Art 9(1).

[136] See also, Proposal for ePrivacy Regulation, recital 22, which stated that '[g]iven the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent'.

[137] See Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP' (10 Feb 2021) 6087/21, pages 26 and 64 and recital 20a. Hereafter in footnotes 'Council position on ePrivacy Regulation'.

platforms from the scope of regulation's rules on direct marketing communications.[138] During the writing of this report, the proposal remains in the legislative process.

Data Governance Act

The EU is also processing a new regulation on data that would facilitate sharing of personal and non-personal data within the Union and would build on top of the data protection framework.[139] In late 2020, the Commission gave its proposal for Data Governance Act, which would firstly seek to increase the re-use of data held by public sector bodies and is subject to rights of others (e.g. rights under data protection or proprietary rights such as trade secrecy or intellectual property).[140]

Secondly, it would create a legal framework with notification obligations for 'data sharing services', which would serve as intermediaries between data holders and data users. According to the Commission, the framework is designed to ensure that those services operate collaboratively, 'empowering natural and legal persons by giving them a better overview of and control over their data',[141] and thus the framework 'actually increases in practice the control that natural persons have over the data they generate'.[142] Therefore, in terms of personal data, a special category of data sharing service providers would cover also those actors that seek to 'enhance individual agency and the individuals' control over the data pertaining to them'.[143] Finally, Data Governance Act would set up a framework for 'data altruism' under which designated non-profit 'data altruism organisations' could, on the basis of consent, collect and pool data for general interest purposes such as scientific research.[144] However, the practical effects of Data Governance Act on the abilities of different actors to gather and analyse data for political micro-targeting is yet unclear.

[138] Council position on ePrivacy Regulation recital 32 and Art 4(3)(f).

[139] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)' COM(2020) 767 final. On the compatibility of Data Governance Act with the GDPR, see recitals 6, 28, 38.

[140] Proposal for Data Governance Act Chapter II.

[141] Proposal for Data Governance Act, Explanatory Memorandum, 7–8. See Proposal for Data Governance Act Chapter III.

[142] Proposal for Data Governance Act, Explanatory Memorandum, 6.

[143] Proposal for Data Governance Act recital 23. See also recital 24 on data cooperatives, which would arguably also be understood as providing 'data sharing services'.

[144] Proposal for Data Governance Act Chapter IV and recital 38–39.

Electronic commerce

e-Commerce Directive

The regulation of myriad for-profit online services is principally codified in the Directive on electronic commerce (e-Commerce Directive), whose objective is 'to create a legal framework to ensure the free movement of information society services between Member States'.[145] The broad category of 'information society services' includes 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.[146] Therefore, the e-Commerce Directive limits our attention to those actors that facilitate political micro-targeting as part of their suite of information society services. Thus, unlike the GDPR, it does not directly regulate for instance political parties or other political NGOs insofar they do not also provide information society services.

The most relevant and intensively debated provisions of the e-Commerce Directive concern the liability exemption of illegal information for information society service providers. Under the e-Commerce Directive, providers of mere information conduit (e.g. internet connection), caching services that provide temporal storage (e.g. search engine), and hosting services (e.g. social networking platform) can benefit from liability exemption on specific conditions.[147] Basically, such a service provider is not liable as long as it is not aware of the illegality of information. In addition, the exemption is maintained only where the provider acts 'expeditiously' to remove the content after becoming aware of it.[148] According to the CJEU, in terms of hosting this effectively requires that the platform is 'neutral'.[149] On the other hand, Member States cannot impose service providers 'a general monitoring obligation' to seek illegal information facilitated by their services.[150]

---

[145] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1, recital 8. Hereafter in footnotes 'e-Commerce Directive'.

[146] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1, Art 1(1)(b).

[147] e-Commerce Directive Arts 12, 13, 14.

[148] ibid Arts 13(1) and 14(1).

[149] Joined Cases C-236/08–C-238/08, *Google France and Google Inc. v Louis Vuitton Malletier and others* [2010] ECR I–2417, para 114; and Case C-324/09, *L'Oréal SA and Others v eBay International AG and Others* [2011] ECR I–6011, paras 112–113, 116.

[150] e-Commerce Directive Art 15.

In recent years, the relationship between the awareness of illegal information, expeditious removal, and the prohibition on general monitoring has become increasingly strained as all sorts of dubious information have received more scrutiny, including rising concern on proliferating disinformation. The CJEU has sought to reconcile monitoring of re-appearing illegal messages with the prohibition on general monitoring obligation by stating that injunctions to prevent the possible re-appearing of identical illegal information do not amount to general monitoring obligation.[151] Moreover, a general monitoring obligation is not imposed even if the monitoring injunction covered also carefully specified 'equivalent information', as long as the nature of such information 'does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies'.[152]

The need of balancing intervention and absence of general monitoring is strongly influenced also by freedom of expression and information, guaranteed in Article 10 of the ECHR and Article 11 of the Charter. While the elaboration of this fundamental right has been somewhat thin in the relevant jurisprudence of CJEU,[153] ECtHR has quite specifically addressed the extent of intermediary responsibility in light of freedom of expression, with explicit references to the e-Commerce Directive and CJEU jurisprudence.[154] In case *Delfi v Estonia*, the imposition of liability on a hosting service provider for illegal hate speech of third parties did not breach freedom of expression and information.[155] The damages were awarded against an online news portal that hosted a comment section on the side of online news articles to which the comments were uploaded automatically without prior editing or moderation. Given the circumstances and especially the clearly illegal nature of the comments, the take-down of comments after six weeks was not considered expeditious enough and the awarded compensation of EUR 320 was found reasonable.[156] However, later in case *MTE v Hungary*, where the ECtHR found the

[151] Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, EU:C:2019:458, para 37. Hereafter in footnotes *Glawischnig-Piesczek*.

[152] ibid paras 46–47.

[153] For instance, in case *Glawischnig-Piesczek* the relevance of freedom of expression is merely stated and the meaning and permissible limits of the right are not properly reflected on. See Case C-18/18, *Glawischnig-Piesczek*, EU:C:2019:458, paras 65 and 74.

[154] *Delfi v Estonia* ECHR 2015–II 319, paras 50–57.

[155] ibid para 162.

[156] ibid paras 156, 160.

allegedly illegal speech to be in fact legitimate criticism, damages against a Hungarian intermediary amounted to a violation of Article 10.[157]

Digital Services Act

Like the ePrivacy Directive, the e-Commerce Directive is currently being revised and will be replaced by a regulation. In December 2020, the Commission published its proposal for Digital Services Act that would revamp the rules of the directive that predate the currently commonplace forms of digital business.[158]

Commission's proposal builds on and extends the regulatory choices of the e-Commerce Directive. Chapter II of the proposal reproduces the liability exemptions for different intermediary service providers (mere conduit, caching and hosting) with only minor refinements and additional specifications.[159] Draft Article 6 seems to induce providers towards more voluntary effort by promising that they 'shall not be deemed ineligible for the exemptions from liability (…) *solely* because they carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content' (Emphasis added). Yet uncertainty seems to persist on whether too much own-initiative effort leads to the loss 'neutrality', that is, the general unawareness of the nature of information on their services.[160] Similarly, some tensions with freedom of expression and information are likely to continue.

The extension of rules contains a suite of due diligence obligations that form a cumulative tiered framework. Firstly, all intermediary service providers would need to designate points of contact/legal representatives in the Union and some basic amount of transparency on their operations.[161] On the second tier, all hosting service providers are required to put in place proper

[157] *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* App no 22947/13 (ECtHR, 2 Feb 2016) paras 89–91.

[158] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final. Hereafter in footnotes 'DSA Proposal'.

[159] DSA Proposal Arts 3–9.

[160] See Aleksandra Kuczerawy, 'The Good Samaritan that wasn't: Voluntary monitoring under the (draft) Digital Services Act' *Verfassungsblog* (12 Jan 2021) <https://verfassungsblog.de/good-samaritan-dsa/> accessed 20 Jan 2021.

[161] DSA Proposal Arts 10–13.

notice and action mechanisms to facilitate the notification and removal of specific pieces of illegal information.[162]

Online platforms are subject to the third tier of obligations. An online platform means 'a provider of a hosting service which, at the request of a recipient of the service, stores *and disseminates to the public* information, unless that activity is a minor and purely ancillary feature of another service' (Emphasis added).[163] Micro and small platform businesses are to be exempted from these obligations (but not from the obligations of all intermediaries and hosting service providers).[164] Among others, these provisions offer users redress options to challenge content removals and they also impose further transparency requirements on service providers.[165] Specifically, in terms of advert transparency it is proposed that:

> Online platforms that display advertising on their online interfaces shall ensure that the recipients of the service can identify, for each specific advertisement displayed to each individual recipient, in a clear and unambiguous manner and in real time:
>
> (a) that the information displayed is an advertisement;
>
> (b) the natural or legal person on whose behalf the advertisement is displayed;
>
> (c) meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed.[166]

Finally, the fourth tier imposes the most stringent obligations on the so-called very large online platforms. A very large online platform has the amount of monthly active users of the service corresponding with 10% of the Union population. Currently, the Commission has estimated this to be 45 million users.[167] Due to the systemic risks that such large services may pose for society, these service providers are required to conduct risk assessments and mitigate risks, which may include 'targeted measures aimed at limiting the display of advertisements in association with the service they provide' among others.[168] They must also submit to independent audits, hire

[162] DSA Proposal Arts 14–15.

[163] ibid Art 2(h).

[164] ibid Art 16.

[165] ibid Arts 17–24.

[166] ibid Art 24.

[167] ibid Art 25.

[168] ibid Arts 26–27.

compliance officers, and provide one more layer of transparency, including an access for vetted researchers to platform data.[169] Consequentially for political advertising, very large online platforms that display advertisements are required to compile a publicly accessible repository containing information on all adverts on their platform.[170]

The proposal also foresees an enforcement network of public authorities that is lacking under the e-Commerce Directive. It introduces Digital Service Coordinators as oversight authorities in Member States, a new advisory body titled 'European Board of Digital Services', and specific enforcement powers for the Commission especially for the supervision of very large online platforms.[171] On most violations, the sanctions are fines up to 6% of the service provider's total turnover in the preceding financial year.[172]

To summarize, Digital Services Act will be highly relevant for political micro-targeting and will likely affect how information will be disseminated online. However, one cannot make definite conclusions on the nature of obligations while the regulation is in legislative process. In addition, the Commission intends to present a separate legislative proposal on the transparency of political advertising in late 2021 that would complement the transparency requirements of very large online platforms proposed in Digital Services Act.[173]

Media regulation

While the regulation for guaranteeing media pluralism has traditionally considered to lie partly within Member States' competence, the EU has sought to harmonize rules on the provision of audiovisual media services with the provision of certain minimum standards.[174] The previous version of the Audiovisual Media Services Directive (AVMSD) did not contain rules on online intermediary services. The latest revision changes that and includes 'video-sharing platform services' in its scope. Video-sharing platform service means:

[169] DSA Proposal Arts 28–33.

[170] ibid Art 30.

[171] ibid Arts 38–58.

[172] ibid Art 59.

[173] Commission, 'On the European democracy action plan' COM(2020) 790 final, 4–5.

[174] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending 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) in view of changing market realities [2018] OJ L303/69, Art 4(1). Hereafter in footnotes 'AVMSD'.

> 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.[175] (Emphasis added)

An obvious example of such a video-sharing platform is Google's YouTube service, but the provisions concern also e.g. social networking platforms like Facebook and Twitter to the extent these platforms host audiovisual content.[176] However, only certain provisions of the AVMSD apply to video-sharing platform services.[177] In relation to the e-Commerce Directive or the upcoming Digital Services Act, AVMSD is *lex specialis*.[178]

In the context of advertising, the AVMSD regulates audiovisual commercial communications, that is, video adverts. It mandates Member States to ensure that video-sharing platform service providers act appropriately to protect minors and the general public against user-generated videos and audiovisual commercial communications that incite terrorism or violence, or threaten to impair minors' physical, mental or moral development.[179] Moreover, the service providers are required to comply with the requirements set out in Article 9(1) with respect to audiovisual commercial communications that are marketed, sold or arranged by those video-sharing platform providers.[180] Article 9(1) requires, among others, that audiovisual advertisements are readily recognizable as such and do not deploy 'subliminal techniques' that could be considered manipulative practices.[181]

---

[175] AVMSD Art 1(1)(aa).

[176] Commission, 'Digital Single Market: Updated audiovisual rules' MEMO/18/4093.

[177] AVMSD Arts 28a–28b.

[178] DSA Proposal, Explanatory Memorandum, 4.

[179] AVMSD Art 28b.

[180] ibid Art 28b(2).

[181] ibid Art 9(1)(a–b).

The implementation period for the revised AVMSD ended in September 2020. However, in November 2020 the Commission launched infringement proceedings against 23 Member States (excluding Denmark, Hungary, the Netherlands, and Sweden) for failing to transpose the directive in time.[182]

Artificial Intelligence Act

Another important ongoing regulatory initiative, which does not have a clear precedent, is the regulation on artificial intelligence, the proposal of which was released in April 2021.[183] There an artificial intelligence system would mean 'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with'.[184] The proposal takes a risk-based approach to artificial intelligence systems and contains four risk categories: unacceptable risk, high-risk, limited risk, and minimal risk. Draft Article 5 lists systems with unacceptable risk that will be banned. Importantly in the context of this report, according to Article 5(1), prohibited is:

> (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;
>
> (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;

Moreover, recital 16 of the proposal stresses the requirement of intention:

---

[182] Commission, 'Audiovisual Media: Commission opens infringement procedures against 23 Member States for failing to transpose the Directive on audiovisual content' IP/20/2165 <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2165> accessed 1 Feb 2021.

[183] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM(2021) 206 final. Hereafter in footnotes 'Proposal for Artificial Intelligence Act'.

[184] ibid Art 3(1). Annex I specifies that techniques contain among others '[m]achine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning'. Machine learning approaches are ubiquitously deployed for the provision of different online services.

> Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of children and people due to their age, physical or mental incapacities. They do so with the intention to materially distort the behaviour of a person and in a manner that causes or is likely to cause harm to that or another person. The intention may not be presumed if the distortion of human behaviour results from factors external to the AI system which are outside of the control of the provider or the user.

As regards point Article 5(1)(b), it seems to be limited to systems that target specific vulnerable groups. Indeed, the Commission confirms this aim by explaining that:

> Other manipulative or exploitative practices *affecting adults* that might be facilitated by AI systems could be covered by the existing data protection, consumer protection and digital service legislation that guarantee that natural persons are properly informed and have free choice not to be subject to profiling or other practices that might affect their behaviour.[185] (Emphasis added)

However, several parts here would still need some further clarification as it is not, for instance, clear what methods 'subliminal techniques' would cover or what specific harms would fall within the notion of 'psychological harm' in Article 5(1)(a). As mentioned above, Article 9(1)(b) of the AVMSD already forbids the use of subliminal techniques in audiovisual adverts. While the designated high-risk artificial intelligence systems seem to exclude applications in media and advertising,[186] the transparency requirements imposed on systems with limited risk may again prove relevant in the context of online political advertising and disinformation. According to draft Article 52(3):

> Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep

[185] Proposal for Artificial Intelligence Act, Explanatory Memorandum, 13.

[186] As listed in Annex III of the proposal, high-risk artificial intelligence systems are restricted to applications in the following sectors: Biometric identification, operation of critical infrastructure, education, employment, access to and enjoyment of essential private services and public services and benefits (including e.g. credit scoring for the management of credit applications), law enforcement, migration, asylum and border control management, and administration of justice and democratic processes. The last sector, administration of justice and democratic processes, mentions 'AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts' as the sole example of systems in that sector.

fake'), shall disclose that the content has been artificially generated or manipulated.

This would indicate that the use of systems that generate 'deep fakes' are not among the subliminal techniques referred to in Article 5. However, there is an exemption even from the transparency requirement in case the use of deep fakes is 'necessary' to exercise of the right to freedom of expression or the right to freedom of the arts and sciences.[187]

Unfair commercial practices

EU consumer law may in some cases complement the regulation on data protection and information society services. The Unfair Commercial Practices Directive (UCPD) applies to unfair business-to-consumer commercial practices.[188] In scholarship, it has been argued that online behavioral advertising in general as an advertising practice falls within the consumer protection of the UCPD and it could impose additional limitations on such practices.[189] An online intermediary service provider facilitating also political adverts may have to comply with certain requirements if it qualifies as 'trader' under the UCPD.[190] The Commission has released a non-binding guidance on the application of the UCPD.[191] It states that a platform may be considered as trader, following a case-by-case analysis, if it for instance 'draws revenues from targeted advertising'.[192] Under the UCPD, platforms providing targeted advertising must maintain 'professional diligence' in their commercial practices in accordance with Article 5(2)(a).[193] In addition, platforms must refrain from unfair commercial practices that mislead

[187] Proposal for Artificial Intelligence Act, Art 52(3).

[188] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L149/22, Art 3(1). Hereafter in footnotes 'UCPD'.

[189] Johann Laux, Sandra Wachter and Brent Mittelstadt, 'Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice' (2021) 58(3) Common Market Law Review 719, 739. For a similar argument concerning data collection practices more broadly, see Nico van Eijk and others, 'Unfair Commercial Practices: A Complementary Approach to Privacy Protection' (2017) 3(3) European Data Protection Law Review 325, 333–337.

[190] UCPD Art 2(b).

[191] Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses' SWD(2016) 163 final.

[192] ibid 110.

[193] ibid 111.

their users.[194] As part of misleading commercial practices, Article 6 of the UCPD defines misleading actions and Article 7 misleading omissions. Finally, Annex I of the UCPD lists a set of specific commercial practices that are always unfair.

Self-regulation

In addition to binding regulation, EU has facilitated several self-regulatory initiatives. The most important instrument regarding political advertising and disinformation is the EU Code of Practice on disinformation that was agreed in 2018.[195] The Code does not cover all the providers of any particular online service but has 13 service providers as signatories. It was originally signed by Facebook, Google, Twitter, and Mozilla, as well as by advertisers and parts of the advertising industry. Others have joined later.[196]

In the Code, the signatories made commitments 'which correspond to the product and/or service they offer, their role in the value chain, their technical capabilities and their liability regimes as provided under EU Law, which vary depending on the role they play in the creation and dissemination of the content at stake'.[197] In general, the signatories recognized among others that it is important to '[e]nsure transparency about political and issue-based advertising, also with a view to enabling users to understand why they have been targeted by a given advertisement'.[198] Moreover, signatories '[c]onsider 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'.[199] The Code is annexed with a list of 'best practices' of different signatories that list the most important internal technical and organizational measures taken.[200]

---

[194] ibid 114.

[195] Commission, 'Code of Practice on Disinformation' (Apr 2018) <https://ec.europa.eu/digital-single-market/en/code-practice-disinformation> accessed 1 Feb 2021.

[196] ibid.

[197] ibid 1–2.

[198] ibid 3.

[199] ibid 3–4.

[200] Commission, 'Code of Practice on Disinformation: Annex II: Current best practices from Signatories of the Code of Practice' (Apr 2018) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54455> accessed 18 Mar 2021.

The effectiveness of the Code was evaluated through several assessments in 2020. While the value of the Code was broadly recognized, several points of criticism were also raised. The European Regulators Group for Audiovisual Media Services (ERGA) stated in its report that the measures of the Code are too broad and vague, not all the relevant service providers have agreed to the Code, and there is a lack of transparency on how the signatories are implementing the Code. Thus, 'steps are required to increase the effectiveness of the measures of the Code itself and also the oversight\reporting structures if it is to evolve into an effective tool in combating disinformation'.[201]

Later, the Commission acknowledged that 'the Code should be further improved in several areas by providing commonly-shared definitions, clearer procedures, more precise commitments as well as transparent key performance indicators and appropriate monitoring, all taking into account applicable regulatory frameworks'.[202] In the EU democracy action plan, the Commission announced its intention to upgrade the Code of Practice on Disinformation in 2021 and the revision would include setting up 'a permanent framework for the monitoring of the code'.[203] In spring 2021, the Commission published its blueprint for strengthening the Code. The renewed Code would contain more detailed commitments from online service providers and other signatories, development of key performance indicators for monitoring compliance, and the set-up of a more formalized monitoring body, a 'permanent task-force', to adapt the Code to various societal developments.[204] The task-force would be chaired by the Commission and include the signatories and representatives from ERGA, European Digital Media Observatory and European External Action Service, and it could 'invite relevant experts to support its work'.[205]

Finally, it should be mentioned that some service providers have prohibited or strictly limited political advertising on their services as an own-initiative measure. For instance, Twitter has

[201] European Regulators Group for Audiovisual Media Services (ERGA), 'ERGA Report on disinformation: Assessment of the implementation of the Code of Practice' (4 May 2020) 3 <https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf> accessed 5 Feb 2021.

[202] Commission, 'Commission Staff Working Document: Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement' SWD(2020) 180 final, 19.

[203] Commission, 'On the European democracy action plan' COM(2020) 790 final, 23–24.

[204] Commission, 'European Commission Guidance on Strengthening the Code of Practice on Disinformation' COM(2021) 262 final.

[205] ibid 24.

banned political advertising on its micro-blogging service[206] and Google has limited the targeting of 'election ads' to the factors of geographic location, age, gender and certain contextual targeting options.[207] As noted in the Introduction, while drawing the line of political/non-political is relatively straightforward in terms of the messages of candidates or parties, the differentiation as regards public issue adverts is trickier. Other notable caveats may exist as well. For instance, in Google's case 'election ads don't include ads for products or services, including promotional political merchandise like t-shirts'.[208]

[206] Twitter for Business, 'Political Content' (2021) <https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html> accessed 19 Apr 2021.

[207] Google, 'Advertising Policies Help: Political content' (2021) <https://support.google.com/adspolicy/answer/6014595?hl=en> accessed 5 Feb 2021.

[208] ibid.

PART III: Member State Law – Electoral and media regulation

The third part of the report concerns the electoral law of Member States. As mentioned in the Introduction, I have selected five Member States as case studies of Member State law. The chosen states are Germany, France, Spain, Ireland, and Poland. Many different objective and subjective factors, taken together as the context of a comparative project, could be referred to when making the selection.[209] While in principle any Member State would be eligible for a case study here, the selection of legal systems is influenced by two cumulative criteria, the first being the anticipated existence of some relevant regulation for the topic in question, that is, for the regulation of online political advertising especially in the context of elections.[210] As Oderkerk has noted, '[t]he selection should include systems in which one reasonably expects to find something about the subject matter under analysis'.[211]

The first criterion of expected findings firstly informed the choice of Germany and France, which have been vocal in their willingness to regulate online services.[212] In addition, this criterion backed the inclusion of Ireland. This is because the EU regulatory framework of digital services follows, to a varying extent, the so-called 'country of origin principle' that vests regulatory authority, especially concerning enforcement, with the 'home' Member State of the regulated entity.[213] In practice, for many online service providers this Member State is Ireland and thus one may expect some regulatory attention paid to online political advertising there as well. The second criterion has been the aim of roughly equal geographical representation of Member States combined with the size of Member State as an indication of its capacity to influence policy also on the EU level. This not only backed again the inclusion of Germany and France, but also informed the selection of Poland and Spain. Hence, the selection should

[209] Marieke Oderkerk, 'The Importance of Context: Selecting Legal Systems in Comparative Research' (2001) XLVIII Netherlands International Law Review 298, 311.

[210] Siems notes that 'at the stage of choosing the legal systems, the comparatist already needs to anticipate what type of differences and similarities she may be able to identify'. Mathias M Siems, *Comparative Law* (2nd edn, CUP 2018) 18.

[211] Oderkerk, 'The Importance of Context: Selecting Legal Systems in Comparative Research' 312.

[212] On these regulatory efforts, see below 'Germany' and 'France'.

[213] Paul Przemysław Polanski, 'Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union' (2018) 34 Computer Law & Security Review 562, 563. On the country of origin principle more generally, see Karsten Engsig Sørensen, 'Enforcement of Harmonization Relying on the Country of Origin Principle' (2019) 25 European Public Law 381.

guarantee a roughly equal representation of Member States on the axes of North-South Europe and East-West Europe.

In addition to electoral processes, Member States' retain some competence to regulate online services within the broader EU law framework and especially concerning media pluralism.[214] This part of the report accounts for such media law too insofar it is connected to elections and online media. Therefore, even though media law in Europe generally contains quite extensive regulation of broadcast media during election periods, neither that nor the regulation of printed media is covered here, unless such regulation is relevant from the perspective of online media too. That said, some parts of that national media and election law may implicate the right to freedom of expression and information under the ECHR, even if such law might be outside the jurisdiction of EU and thus also beyond the remit of the rights of the Charter.[215] Indeed, as I will soon outline further, the national limitations to political advertising have been challenged several times before the ECtHR on the basis of freedom of expression and information. While the Strasbourg Court has not for the time being considered a case involving political micro-targeting,[216] one might nevertheless be able to infer a few, at least to some extent generalizable, insights from its case law concerning the regulation of political advertising on broadcast media. Thus, before turning to Member State law, I first address briefly how political micro-targeting relates to freedom of expression under the ECtHR jurisprudence.

Media pluralism and freedom of expression under the ECHR

As stated, freedom of expression and information is guaranteed in Article 10 of the ECHR. According to Dobber and others, online political advertising implicates several actors' freedom of expression and/or information:

[214] For instance, e-Commerce Directive Art 1(6) provides a specific caveat for Member State measures taken in the defense of pluralism, and as mentioned, in accordance with AVMSD Art 4, the directive provides only minimum harmonization of relevant Member State media law.

[215] The Charter in itself does not confer legal competence but is applicable only in conjunction with EU law. See, Charter Art 51(2).

[216] Dobber, Ó Fathaigh and Borgesius, 'The regulation of online political micro-targeting in Europe' 8. Bayer makes the same observation in Bayer, 'Double harm to voters: data-driven microtargeting and democratic public discourse' 6.

> an election candidate's freedom of expression, a political party's freedom of expression, an online platform's freedom of expression, and, indeed, the public's (voters') right to receive information.[217] (References omitted)

Of course, other actors than political parties or candidates who disseminate advertising on a public issue enjoy freedom of expression as well. Moreover, Bayer argues that micro-targeting of political advert only to specific audiences also implicates the right to information of all those other people that are *not* targeted by that advert. In that sense, micro-targeting messages potentially produces 'a mass violation of human rights'.[218]

When assessing the protection of the right, it should first be noted that political advertising is a somewhat liminal activity between commercial expression and political expression. The ECtHR (also 'the Court' in this sub-chapter) has long drawn a line between the two and awarded political expression with highest degree of protection even though for-profit speech is certainly not out of protection either.[219] Political advertising as a form of expression has been ruled to fall within the highest protection category of political expression.[220] At the same time, it is clear that even political expression can be regulated and the ECtHR has decided a few cases which have been about bans on political advertising on broadcast media, perhaps most notably in *VgT Verein Gegen Tierfabriken v Switzerland*,[221] *TV Vest v Norway*,[222] and *Animal Defenders v the United Kingdom*.[223]

In *TV Vest*, the Court accepted that in principle the aim to guarantee pluralistic and undistorted debate in society could provide a legitimate basis for the regulation of political advertising.[224] Here, financial power, as translated into political advertising, may distort public debate for the benefit of the interests of the wealthy. Moreover, states even have a *positive obligation* to guarantee pluralism during and outside election periods, which may require an appropriate

---

[217] Dobber, Ó Fathaigh and Borgesius, 'The regulation of online political micro-targeting in Europe' 8.

[218] Bayer, 'Double harm to voters: data-driven microtargeting and democratic public discourse' 2–3.

[219] Lorna Woods, 'Digital freedom of expression in the EU' in Sionaidh Douglas-Scott and Nicholas Hatzis (eds), *Research Handbook on EU Law and Human Rights* (Edward Elgar Publishing 2017) 394, 400. According to Woods, there is also a third category of expression, artistic speech, whose protection in rank is between commercial and political expression.

[220] Dobber, Ó Fathaigh and Borgesius, 'The regulation of online political micro-targeting in Europe' 8.

[221] *VgT Verein Gegen Tierfabriken v Switzerland* ECHR 2001–VI 243.

[222] *TV Vest AS & Rogaland Pensjonistparti v Norway* ECHR 2008-V 265.

[223] *Animal Defenders International v the United Kingdom* ECHR 2013–II 203.

[224] *TV Vest AS & Rogaland Pensjonistparti v Norway* ECHR 2008-V 265, para 70.

regulatory framework.[225] However, in *TV Vest* a complete ban of political advertising on TV as a general measure for guaranteeing undistorted political debate against powerful financial interests still produced a violation of Article 10. This was because the applicant of the case, a small pensioners' party, was not financially powerful and thus the ban, as applicable indiscriminately to all advertisers, was contrary to its stated aim.[226] Therefore, the acceptability of general measures appears to pin down to their proportionality.

Arguably, the Court's stance shifted further in favor of regulation in *Animal Defenders*. In that case, a general ban on political advertising on broadcast media, which prohibited an NGO from broadcasting its public issue advert on animal treatment, did not lead to a violation of Article 10.[227] The ECtHR ruled that 'the more convincing the general justifications for the general measure are, the less importance the Court will attach to its impact in the particular case', i.e. to the fact that a specific advertiser may not be financially powerful and thus hardly able to distort public debate even absent a general ban.[228]

From the Court's reasoning in *Animal Defenders*, Bayer has abstracted the criteria for a permissible general prohibition on political adverts. Four conditions must be met:

- their dissemination would impose a risk of unequal access based on wealth;
- the legitimate aim is protection of the democratic process from distortion;
- the lurking distortion would cause competitive advantages and thereby curtail a free and pluralist debate;
- the restriction has strict limits by being confined to certain media only, and other media is available.[229]

As regards other available media, in *Animal Defenders* the ECtHR stated: 'Even if it has not been shown that the internet, with its social media, is more influential than the broadcast media in the respondent State […], those new media remain powerful communication tools which can be of significant assistance to the applicant NGO in achieving its own objectives'.[230] For instance in case of video hosting, the Court has stated that 'political content ignored by the

[225] *Centro Europa 7 Srl and Di Stefano v Italy* ECHR 2012–III 339, para 134; and *Animal Defenders International v the United Kingdom* ECHR 2013–II 203, para 111.

[226] *TV Vest AS & Rogaland Pensjonistparti v Norway* ECHR 2008-V 265, paras 71–73.

[227] *Animal Defenders International v the United Kingdom* ECHR 2013–II 203, para 125.

[228] ibid para 109.

[229] Bayer, 'Double harm to voters: data-driven microtargeting and democratic public discourse' 8.

[230] *Animal Defenders International v the United Kingdom* ECHR 2013–II 203, para 124.

traditional media is often shared via YouTube, thus fostering the emergence of citizen journalism. From that perspective, the Court accepts that YouTube is a unique platform on account of its characteristics, its accessibility and above all its potential impact, and that no alternatives were available'.[231]

To conclude, generally attention around restrictions to political advertising is drawn to the value of pluralistic debate and media environment that fosters pluralism.[232] While the jurisprudence on Article 10 of the ECHR imposes a number of limitations for the regulation of political advertising, it is equally clear that European governments have some room to maneuver. As mentioned, the line is however yet to be drawn by the Court in the specific context of online political advertising. I now turn to the case studies into Member State law to explore the relevant regulation more closely.

Germany

The primary pieces of German electoral law, in addition to the 1994 *Grundgesetz* (Basic Law), are the 1993 Federal Elections Act, the 2002 Federal Electoral Regulations, the Law on the Scrutiny of Elections, and the 1994 Act on Political Parties.[233] However, there are no detailed provisions on election campaigns in federal legislation but instead they are largely regulated at *Länder* (State) level.[234]

The Political Parties Act is the main piece of legislation on campaign financing in Germany. In the connection of Federal Parliamentary Elections in 2017, the OSCE report stated that '[t]here are no limits set to campaign expenditures for parties and candidates. According to OSCE/ODIHR EET interlocutors, the bulk of campaign expenses were allotted to media

[231] *Cengiz and Others v Turkey* ECHR 2015–VIII 177, paras 52.

[232] van Hoboken and others, 'The legal framework on the dissemination of disinformation' 38.

[233] Federal Elections Act, version as promulgated on 23 July 1993 (Federal Law Gazette I pp. 1288, 1594), last amended by Article 1 of the Act of 28 October 2020 (Federal Law Gazette I p. 2264); Federal Electoral Regulations, version as promulgated on 19 Apr 2002 (Federal Law Gazette I p. 1376), last amended by Article 10 of the Ordinance of 19 June 2020 (Federal Law Gazette I p. 1328); Law on the Scrutiny of Elections (*WahlPrG*), revised version as promulgated in the Federal Law Gazette, Section III, classification number 111-2, last amended by Article 11 of the Ordiance of 19 June 2020 (Federal Law Gazette I, page 1328); and Act on Political Parties (Parteiengesetz – PartG) version published on 31 January 1994 (Federal Law Gazette I 1994, p. 149), last amended by the Ninth Act amending the Political Parties Act, of 22 December 2004 (Federal Law Gazette I 2004, p. 3673). All acts are available on the website of the Federal Returning Officer <www.bundeswahlleiter.de/en/bundestagswahlen/2021/rechtsgrundlagen.html#0d5e276a-6a3e-4437-b357-be4764eff500> accessed 18 Mar 2021.

[234] OSCE Office for Democratic Institutions and Human Rights, 'Elections to the Federal Parliament (Bundestag) 24 September 2017: OSCE/ODIHR Election Expert Team Final Report' (Warsaw, 27 Nov 2017) 4.

advertising, including on social media. The legislation lacks provisions regulating campaign activities by third-parties'.[235] However, under the Basic Law, 'political parties must publicly account for assets and sources of income, and use of their funds'.[236] The annual financial reports of political parties are submitted to the President of *Bundestag* (Federal Parliament) and donations exceeding EUR 50.000 must be reported immediately and not only in annual reporting.[237] In addition, some parties may have stricter internal requirements for their candidates.[238] There are no restrictions on the campaign period and parties and candidates are allowed to campaign at any time before the elections.[239]

As regards the regulation of election advertising or media reporting on elections, there are big differences between broadcasters, printed media, and online media.[240] In the online sector, a further distinction should be made between (online) broadcasting and telemedia such as on-demand services and social media platforms.[241] As regards on-demand services, '[e]lection advertising via on-demand audiovisual media services is prohibited under Article 58(3)(1), in conjunction with Article 7(9) of the *Rundfunkstaatsvertrag* (Inter-State Broadcasting Agreement)'.[242] However, as many other internet intermediary services do not exert editorial control over the content as on-demand services do, a lot of regulation does not apply to those services. In addition, the German Unfair Competition Act, which is considered the most important instrument for the regulation of online advertising in Germany, does not apply to political advertising.[243] Etteldorf concludes that in comparison to somewhat extensively regulated broadcasting and printed media, Germany has maintained 'a "hands-off" approach in the online sector, where it relies entirely on voluntary self-regulation'.[244]

While not regulating online political advertising specifically, the recent Act to Improve Enforcement of the Law in Social Networks, *Netzwerkdurchsetzungsgesetz* (Network

[235] ibid 4. See also Bayer and others, 'Disinformation and propaganda', 196.

[236] OSCE Office for Democratic Institutions and Human Rights, 'Elections to the Federal Parliament (Bundestag) 24 September 2017' 5.

[237] ibid 6–7.

[238] ibid 6.

[239] ibid 4.

[240] Christina Etteldorf, 'DE – Germany' in Maja Cappello (ed), *Media coverage of elections: The legal framework in Europe* (European Audiovisual Observatory 2017) 30, 37.

[241] ibid 34.

[242] ibid 30.

[243] ibid 34, 36.

[244] ibid 37.

Enforcement Act or 'NetzDG') can be seen as a possible break from the 'hands-off' approach.[245] The widely debated law came into force in October 2017 and in 2020 the German government already introduced amendments to it.[246] NetzDG is applicable to 'telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public (social networks)'.[247] However, the requirements apply only if the social network has more than 2 million users in Germany.[248] As it regulates social media platforms specifically, it is worth a brief visit.

In relation to EU law, NetzDG falls within the regulatory leeway provided for Member States in the loose framework of the e-Commerce Directive, even though its compatibility with the directive has been questioned in scholarship.[249] As its name suggests, the aim of the law is not to impose new substantive restrictions on online behavior but to enhance the enforcement against illegal speech, as provided in the German 1998 Criminal Code,[250] in the online context. Tworek and Leerssen underscore that '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'.[251]

In terms of disinformation, in Germany, disseminating false information is not illegal *per se* and the Network Enforcement Act does not contain specific provisions on disinformation or fake news. However, as we saw in Part I, disinformation is connected also to illegal speech, which in Germany contains for instance defamation, incitement to hatred, or the dissemination

---

[245] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) <www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2> accessed 18 Feb 2021.

[246] Madeline Earp, 'Germany revisits influential internet law as amendment raises privacy implications' *CPJ* (7 Oct 2020) <https://cpj.org/2020/10/germany-revisits-influential-internet-law-as-amendment-raises-privacy-implications/> accessed 18 Feb 2021.

[247] Network Enforcement Act Section 1(1).

[248] ibid Section 1(2).

[249] Thomas Wischmeyer, '"What is illegal offline is also illegal online": The German Network Enforcement Act 2017' in Bilyana Petkova and Tuomas Ojanen (eds), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries* (Edward Elgar Publishing 2020) 28, 43–46. On the e-Commerce Directive, see Part II: Electronic commerce.

[250] German Criminal Code (*Strafgesetzbuch – StGB*) <www.gesetze-im-internet.de/englisch_stgb/> accessed 16 Mar 2021.

[251] Heidi Tworek and Paddy Leerssen, 'An Analysis of Germany's NetzDG Law' (15 Apr 2019) Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2 <www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf> accessed 18 Feb 2021.

of propaganda of unconstitutional organizations.[252] Basically, the law mandates a social media service provider to remove illegal information generally within 7 days and manifestly illegal information within 24 hours from the receipt of a notice.[253] In addition, it contains transparency reporting obligations and other procedural requirements regarding the handling of reports on illegal content.[254]

France

France has been active in the field of disinformation and online advertising regulation, especially regarding elections.[255] The French legal framework regulates both political parties and online media providers, the latter regulation naturally within the limits of EU law. One notable principle of the French regulatory approach to online media is to challenge the country-of-origin principle fostered in the EU legal framework in favor of regulatory competence of the destination country of the service.[256]

As regards French electoral law, the Electoral Code (*Code électoral*) imposes limits on donations and loans to candidates from individuals while donations from legal persons or foreigners are prohibited altogether.[257] Moreover, campaign expenditure is capped, the amount in the 2017 presidential election being 16.8 million euros per candidate for the first round and 22.5 million for the second. According to the OSCE report on the 2017 presidential elections, the restrictions may be circumvented, as there is no explicit prohibition on making a donation in the name of another.[258] In addition, the Electoral Code does not cap or otherwise regulate the expenses of third parties unaffiliated with parties or candidates. However, according to the OSCE interlocutors, third party campaigning was insignificant in the 2017 presidential

[252] German Criminal Code, Sections 186–187, 130 and 86 respectively.

[253] Network Enforcement Act Section 3(2).

[254] Network Enforcement Act Section 2.

[255] See e.g. Mission report submitted to the 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' (May 2019) <www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf> accessed 2 Mar 2021.

[256] ibid 2.

[257] Code électoral, Article L52-7-1 and L52-8, <www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/2021-03-18/> accessed 22 Feb 2021.

[258] OSCE Office for Democratic Institutions and Human Rights, 'Republic of France: Presidential Election 23 April and 7 May 2017: OSCE/ODIHR Election Expert Team Final Report' (Warsaw, 30 Aug 2017) 4–5.

elections.[259] In terms of reporting of campaign funding, there are no disclosure requirements prior to an election. Afterwards, a campaign account must be filed with the overseeing regulator, *Commission nationale des comptes de campagneet des financements politiques* (CNCCFP). The regulator later publishes a general summary of the financial data of the campaign but not detailed information.[260]

In terms of online media regulation during election period, the French legal framework is somewhat extensive. Firstly, the Electoral Code prohibits political advertising through press and audiovisual means in the election period, that is, during six months prior to an election.[261] This prohibition extends to referendum campaigns and covers online communication.[262] In addition, publication of any election propaganda, such as opinion polls, is prohibited one day prior to an election and on the day of election.[263]

Secondly, during three months before an election, there is specific regulation concerning the dissemination of inaccurate or misleading allegations or imputations of a fact (*des allégations ou imputations inexactes ou trompeuses d'un fait*) on platforms in accordance with the 2018 law on the fight against information manipulation.[264] In connection with the law, the Electoral Code was also amended to include new Articles 163-1 and 163-2. The Electoral Code now prescribes that during three months prior to elections, a specified French court may take action against the dissemination of inaccurate or misleading allegations or imputations of a fact likely to alter the sincerity of the forthcoming ballot, and which are disseminated in a deliberate, artificial or automated and massive manner by means of an online public communication service.[265] A court ruling on the measures to be taken against dissemination must be given

[259] OSCE Office for Democratic Institutions and Human Rights, 'Republic of France: Presidential Election 23 April and 7 May 2017' 5.

[260] ibid 6.

[261] Code électoral, Article L52-1. The article prescribes that: '*Pendant les six mois précédant le premier jour du mois d'une élection et jusqu'à la date du tour de scrutin où celle-ci est acquise, l'utilisation à des fins de propagande électorale de tout procédé de publicité commerciale par la voie de la presse ou par tout moyen de communication audiovisuelle est interdite.*'

[262] Agnès Granchet, 'FR – France' in Maja Cappello (ed), *Media coverage of elections: The legal framework in Europe* (European Audiovisual Observatory 2017) 48.

[263] Code électoral, Article L49.

[264] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information <www.legifrance.gouv.fr/loda/id/JORFTEXT000037847559/?isSuggest=true> accessed 22 Feb 2021. For a detailed analysis of the law, see Kamel Ajji, 'Protecting liberal democracy from artificial information: The French proposal' in Bilyana Petkova and Tuomas Ojanen (eds), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries* (Edward Elgar Publishing 2020).

[265] Code électoral, Article L163-2.

within 48 hours from the referral by, for instance, a political party or another actor having an interest in the matter.[266]

Moreover, platform operators must provide users some basic transparency on any adverts concerning public matters. This includes firstly fair, clear and transparent information about the identity of the person or company, which pays the platform remuneration in return for the promotion of information related to a debate of general interest. Secondly, it includes information on the use of their personal data in the context of the promotion of information related to a debate of general interest. Thirdly, transparency mandates information on the amount of remuneration received for the promotion of such information when the amount exceeds a certain threshold. The required information shall be aggregated in a publicly available register.[267]

In turn, Article 11 of the law on the fight against information manipulation specifies that platform operators must 'take measures to fight the dissemination of false information that is likely to disturb public order or to alter the sincerity of one of the elections'.[268] Elections here refer to the elections of the President of the Republic, general elections of Members of the National Assembly, elections of senators, elections of representatives to the European Parliament and referenda. The due diligence obligations apply to online platform operators, as defined in Article L111-7 of the French Consumer Code, 'whose activity exceeds five million unique visitors per month, per platform, calculated on the basis of the last calendar year'.[269] The overseeing regulator of the law on information manipulation is the French media regulator (*Conseil Supérieur de l'Audiovisuel*, CSA). Article 12 of the law provides that the CSA may issue recommendations to these online platform operators on the required measures. In 2019, the CSA provided a recommendation which included detailed information on how platform operators should provide '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'.[270] In addition, the CSA recommended transparency of algorithms, 'fact-checking' content,

[266] Code électoral, Article L163-2.

[267] Code électoral, Article L163-1.

[268] CSA, 'Recommendation no. 2019-03 of 15 May 2019' 2.

[269] Conseil Supérieur de l'Audiovisuel (CSA), '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' 1 <www.csa.fr/Informer/Espace-presse/Communiques-de-presse/Adoption-de-la-recommandation-relative-a-la-lutte-contre-la-manipulation-de-l-information-un-pas-de-plus-vers-une-nouvelle-regulation> accessed 25 Feb 2021.

[270] ibid 2–3.

detection of accounts set up to disseminate disinformation on scale, and reinforcement of media literacy efforts.[271]

Thirdly, France has criminalized the dissemination of fake news (*de nouvelles fausses*) in its 1881 Freedom of Press Act.[272] It is also worth a mention that in July 2019 France adopted the Law aimed at combating hate content on the Internet, in popular discourse often dubbed as 'Avia law'.[273] It was inspired by the German NetzDG and introduced similar obligations on social media platform operators as its German counterpart. However, Constitutional Council (*Conseil Constitutionnel*) judged the main provisions of the law, including the obligation to remove 'manifestly illegal hate speech' within 24 hours from the receipt of a report, unconstitutional due to their unjustified encroachment upon freedom of expression.[274]

By contrast to Germany, one can remark both similarities and differences. While both countries have introduced specific laws concerning online intermediary services, the French legal framework seems to aim somewhat more specifically to maintain election integrity whereas the German law is more concerned with hate speech and other illegal information. In France, the dissemination of fake news has been illegal for long and the law on the fight against information manipulation expressly seeks to enhance transparency of adverts and prevent undue informational influence around elections. Thus, in terms of election law and media regulation around election, the French legal framework seems to be stricter and more complex than in Germany. This holds concerning both political parties and candidates and online services facilitating adverts and other information around elections. Moreover, the French attempt for Avia law, similar to the NetzDG, testifies that in France there is indeed interest in further regulatory action regarding other issues in the online context as well. Moreover, in both countries the general election law that regulates the financing and transparency of political parties and candidates may provide certain base level protection against undue distortion of public discourse around elections. Nevertheless, it should be noted that neither country has

[271] Conseil Supérieur de l'Audiovisuel (CSA), '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' 3–6.

[272] Loi du 29 juillet 1881 sur la liberté de la presse, Article 27 <www.legifrance.gouv.fr/loda/id/JORFTEXT000000877119/?isSuggest=true> accessed 22 Feb 2021.

[273] Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet <www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970/> accessed 16 Mar 2021.

[274] Conseil Constitutionnel, Décision n° 2020-801 DC du 18 juin 2020 <www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm> accessed 16 Mar 2021. See also, EDRi, 'French Avia law declared unconstitutional: What does this teach us at EU level?' (24 June 2020) <https://edri.org/our-work/french-avia-law-declared-unconstitutional-what-does-this-teach-us-at-eu-level/> accessed 16 Mar 2021.

undertaken wide-scale reforms of existing electoral or media law frameworks to systematically incorporate the use of online services. In addition, both countries lack extensive regulation of third party campaigning.

Spain

In Spain, the most important piece of legislation in terms of electoral law in general, and media regulation during elections as well, is the Spanish Law on the General Electoral System (*Ley Orgánica 5/1985, del Régimen Electoral General*, LOREG).[275] While the authority over election management is to some extent delegated to Autonomous Communities (*Comunidad Autónoma*) and provincial levels, the primary oversight entity nationally is the Central Electoral Board (*Junta Electoral Central*), which has the competence to issue authoritative interpretations ('*instrucción*') of LOREG. Generally, LOREG differentiates between traditional electoral campaigns and 'institutional campaigns' that are executed by the government to inform the public, for instance, about issues of public health or security.[276] Electoral campaigning is allowed during the specific election period of 15 days prior to an election with silence period on the election day.[277] Political parties, candidates, federations, coalitions, or groups are allowed to engage in political advertising only during such election period.[278] Also, it is prohibited to publish opinion polls five days before an election.[279]

In terms of campaign financing, there is emphasis on public funding. During the last two decades, substantial limitations to private campaign contributions have been added to the Spanish Law on Political Campaign Financing.[280] The recent reforms include prohibitions on anonymous contributions and contributions by legal persons.[281] Private donations by

[275] Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General <www.boe.es/buscar/act.php?id=BOE-A-1985-11672> accessed 1 Mar 2021. Hereafter in footnotes LOREG.

[276] LOREG, Artículo 50. See also, Junta Electoral Central, 'Instrucción 2/2011, de 24 de marzo, de la Junta Electoral Central, sobre interpretación del artículo 50 de la Ley Orgánica del Régimen Electoral General, en relación al objeto y los límites de las campañas institucionales y de los actos de inauguración realizados por los poderes públicos en periodo electoral', BOE-A-2011-5522 <www.boe.es/buscar/pdf/2011/BOE-A-2011-5522-consolidado.pdf> accessed 1 Mar 2021.

[277] LOREG, Artículo 51.

[278] LOREG, Artículo 53.

[279] LOREG, Artículo 69(7).

[280] Ley Orgánica 8/2007, de 4 de julio, sobre financiación de los partidos politicos <https://boe.es/buscar/act.php?id=BOE-A-2007-13022> accessed 2 Mar 2021.

[281] Ley Orgánica 8/2007, Articulo 5.

individuals are capped to EUR 10.000 per party, federation, coalition or group per election.[282] In addition, there is a yearly cap of EUR 50.000 for donations from the same individual.[283] Oversight powers regarding party financing have been conferred to the Court of Accounts (*Tribunal de Cuentas*).[284]

As regards media law, to guarantee equality and pluralism in the media during election time, LOREG places some limitations to political advertising as well. Firstly, political advertising on television is forbidden. Instead, political parties are allotted free advertising slots on public service television and radio.[285] Advertising expenditure on radio and print media is also capped to 20% of the planned campaign expenditure.[286] Secondly and importantly, the Central Electoral Board has clarified that while LOREG itself is silent on electoral campaigning online, the limitations imposed by it nevertheless apply also to electoral propaganda disseminated through electronic means.[287] Despite the interpretation, some uncertainties around digital media appear to persist and the adequacy of LOREG to meet the challenges of online electoral coverage has been questioned.[288] For instance, it has been stated that some provisions, such as the limitation on the release of opinion polls or the silence period of the election day, can be easily circumvented through foreign/transnational online media.[289]

Thirdly, LOREG was amended in 2018 in the connection of introduction of the Spanish Law on Data Protection and Digital Rights to contain rules on the use of personal data in political campaigning.[290] The amendment inserted new Article 58 bis which concerns specifically the use of personal data in political campaigning and certain other questions related to new information technologies. Broadly in line with the GDPR, the article provides that political

[282] LOREG, Artículo 129.

[283] Ley Orgánica 8/2007, Articulo 5.

[284] Ley Orgánica 8/2007, Articulo 16.

[285] Francisco Javier Cabrera Blázquez, 'ES – Spain' in Maja Cappello (ed), *Media coverage of elections: The legal framework in Europe* (European Audiovisual Observatory 2017) 40.

[286] LOREG, Artículo 58.

[287] Junta Electoral Central, 'Instrucción 4/2007, de 12 de abril, de la Junta Electoral Central, sobre la utilización de las nuevas tecnologías de la información y de la comunicación electrónicas como instrumento de propaganda electoral', BOE-A-2007-8181 <www.boe.es/buscar/pdf/2007/BOE-A-2007-8181-consolidado.pdf> accessed 1 Mar 2021.

[288] María Holgado González, 'Publicidad e información sobre elecciones en los medios de comunicación durante la campaña electoral' (2017) UNED. Teoría y Realidad Constitucional, no. 40, 457–485, 484.

[289] ibid 482–484.

[290] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales <www.boe.es/buscar/doc.php?id=BOE-A-2018-16673> accessed 2 Mar 2021.

parties may utilize personal data collected from publicly accessible sources in their campaigns during the election period. In addition, the article specifies that contracting electoral propaganda on social networks or through equivalent means does not count as commercial communication. However, it is required that the electoral nature of such communications is disclosed and recipients are allowed to oppose the communications.[291]

Yet, it should be pointed out that in May 2019 Section 1 of Article 58 bis was annulled by the Constitutional Court (*Tribunal Constitucional*) due to its undue restrictions on fundamental rights, primarily data protection.[292] While the role of new information technologies remains a debated matter in Spain, it has been pointed out that political campaigns are still mainly done in 'traditional ways', especially if compared to the US, with television seen as the most important medium for electoral messages.[293]

When compared with France and Germany, the Spanish regulatory strategy has been to extend the scope of the existing framework to cover also the online context through the authoritative interpretation of the Central Electoral Board. However, while the regulation on political advertising has traditionally been strict with a complete ban on political advertising on television, and also other campaigning is limited to the specific election period, the amendment to LOREG sought to allow certain leeway for electoral communications through online means with specific safeguards. In that sense, the regulation seems to be somewhat more lenient than in France but more stringent than in Germany. Also similarly to France, there are time restrictions to the release of polls, and the effectiveness of such limitations becoming questionable with the transnational nature of online media. Yet unlike to France or Germany, Spain has not so far taken comprehensive legislative effort to regulate online disinformation around elections (like the French law against information manipulation) or illegal speech disseminated through online intermediaries (like the German NetzDG).

---

[291] Ley Orgánica 3/2018, Articulo 58 bis.

[292] Sentencia del Tribunal Constitucional n.º 76/2019, de 22 de mayo de 2019 (Judgment 76/2019, of 22 May 2019), Recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo respecto del apartado primero del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (BOE n.º 151 de 25-VI-2019) <http://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2019-9548.pdf> accessed 2 Mar 2021. See also, Diego Ramos, 'Spain: New Data Protection Act (partly) nullified by the Constitutional Court' *Privacy Matters: DLA Piper's Global Privacy and Data Protection Resource* (23 May 2019) <https://blogs.dlapiper.com/privacymatters/spain-new-data-protection-act-partly-nullified-by-the-constitutional-court/> accessed 2 Mar 2021.

[293] Laura Cervi, Nuria Roca, 'La modernización de la campaña electoral para las elecciones generales de España en 2015. ¿Hacia la americanización?' (2017) Comunicación y Hombre, no. 13, 133.

Ireland

The most important piece of Irish electoral law is the Electoral Act from 1997, which has been subsequently amended several times.[294] While the Irish electoral law framework lacks a central election management body, to some extent the Standards in Public Office Commission (SIPO) serves similar functions, complemented with emphasis on judicial oversight over electoral law.[295] SIPO is the overseeing administrative body especially in terms of campaign financing and transparency. However, it does not have oversight role in the practical management of elections.[296]

Firstly, the Irish electoral law framework regulates campaign financing both with substantive limitations and transparency requirements. Anonymous donations exceeding EUR 100 are prohibited. Under the Electoral Act, donations and financial records of political parties and candidates in general are subject to reporting requirements, the reports of which being filed with the SIPO. Third parties that accept donations must register with the SIPO and corporate donors that seek to donate more than 200 euros need to register as corporate donors as well.[297] In addition, there are both campaign spending and donation limits, including a prohibition to donations by foreign actors.[298] Spending limits for candidate campaigns in the lower house of the Oireachtas, *Dáil*, and the European Parliament depend on the size of the constituency of the candidate, while the limit for candidates in the presidential election is the same.[299]

Secondly, under the 2009 Broadcasting Act there is a statutory prohibition on advertising 'directed towards a political end' on broadcast media that concerns both elections and referenda.[300] The Broadcasting Authority of Ireland (BAI) is responsible for the oversight of broadcasters. However, Ireland lacks a proper regulatory framework on data-driven campaigning and online political advertising and the current regulation relies mainly on data

[294] Electoral Act, 1997, Law No. 25 of 1997 <www.irishstatutebook.ie/eli/1997/act/25/enacted/en/html> accessed 10 Mar 2021.

[295] Jennifer Kavanagh, 'Electoral Law in Ireland: Sustaining Electoral Integrity from Process, Procedures, and Precedent?' (2015) 30 *Irish Political Studies* 510, 525–526.

[296] Standards in Public Office Commission, 'Electoral' <www.sipo.ie/acts-and-codes/legislation/electoral/> accessed 10 Mar 2021.

[297] ibid. See, Electoral Act, Sections 22–26.

[298] Standards in Public Office Commission, 'Electoral'.

[299] Electoral Act, Sections 31, 32, 33, 53.

[300] Broadcasting Act, 2009, Law No. 18 of 2009, <www.irishstatutebook.ie/eli/2009/act/18/enacted/en/html?q=Broadcasting+Act> accessed 10 Mar 2021.

protection law. The Irish Data Protection Commission has issued a brief guidance on the application of GDPR in electoral context.[301] Nevertheless, concerns have been raised regarding the use of online media. For instance, prior to the referendum on the extension of the right to abortion, there were reports on third party campaigning from the US done via Facebook advertisements, which prompted a warning on undue influence from the Irish Data Protection Commissioner.[302] Practically, such campaign activities were able to circumvent the regulatory limitations outlined above and were halted only after the company took self-regulatory action.[303]

However, the Irish regulatory framework is in the process of being overhauled both in terms of electoral and media law. In early 2021, the Irish government published its General Scheme of the Electoral Reform Bill that would contain major revisions of electoral law.[304] As the lack of a central election management body has been seen as a notable regulatory flaw,[305] the Electoral Reform Bill would introduce 'a statutory, independent Electoral Commission for Ireland' which would 'have responsibility for the regulation of online political advertising during electoral periods, oversight of the Electoral Register, and a new public information, research and advisory role in relation to electoral matters'.[306] In addition, the bill would include comprehensive rules on online political advertising in election times and would impose obligations both on online platforms/other online facilitators and advert buyers.[307] In summary, these rules would require that:

---

[301] Data Protection Commission, 'DPC publishes guidance on data protection and electoral and canvassing activities' (9 Oct 2018) <www.dataprotection.ie/en/news-media/latest-news/dpc-publishes-guidance-data-protection-and-electoral-and-canvassing-activities> accessed 10 Mar 2021.

[302] Cormac McQuinn, 'Warning that foreign ads "could influence referendum on Eighth Amendment"' *Independent.ie* (18 Apr 2018) <www.independent.ie/irish-news/abortion-referendum/warning-that-foreign-ads-could-influence-referendum-on-eighth-amendment-36817674.html> accessed 10 Mar 2021. See also, Calara Provost and Lara Whyte, 'Foreign and 'alt-right' activists target Irish voters on Facebook ahead of abortion referendum' *OpenDemocracy* (25 Apr 2018) <www.opendemocracy.net/en/5050/north-american-anti-abortion-facebook-ireland-referendum/> accessed 10 Mar 2021.

[303] Facebook, 'Facebook will not be accepting referendum related ads from advertisers based outside of Ireland' (8 May 2018) <www.facebook.com/notes/facebook-dublin/facebook-will-not-be-accepting-referendum-related-ads-from-advertisers-based-out/10156398786998011/> accessed 10 Mar 2021.

[304] Department of Housing, Local Government and Heritage, 'Ministers O'Brien and Noonan publish the General Scheme of the Electoral Reform Bill' *gov.ie* (8 Jan 2021) <www.gov.ie/en/press-release/0dfe8-ministers-obrien-and-noonan-publish-the-general-scheme-of-the-electoral-reform-bill/> accessed 11 Mar 2021.

[305] Kavanagh, 'Electoral Law in Ireland' 526.

[306] ibid. See General Scheme of the Electoral Reform Bill 2020, Chapters 1 and 4 <https://assets.gov.ie/118345/15ac22d0-1d73-438a-a1f8-4958bdacafa6.pdf> accessed 11 Mar 2021.

[307] General Scheme of the Electoral Reform Bill 2020, Part 4.

> Online paid-for political advertisements commissioned for use during electoral periods will be required to be clearly labelled as such. The advertisements will display specified information by way of a transparency notice, linked to the advertisement in a transparent and conspicuous manner. The transparency notice will include information on who paid for the advertising, details of any micro-targeting which was applied and the total cost of the advertising.[308]

As regards the reform of Irish media law, the General Scheme of the Online Safety Media Regulation Bill was announced in early 2020 and during the writing of this report, the reform is still in process with new additions introduced by the government in December 2020. The reform would also implement the revised AVMSD.[309] Since the directive follows the country of origin principle, it entrusts significant regulatory authority over the largest online platforms to Ireland, thus making the reform important European-wide.[310] Basically, the reform would renew the Irish media law framework to clearly cover also online media and respond to the challenges it may pose. It would replace BAI with a new Media Commission which would include an Online Safety Commissioner.[311] The General Scheme would provide 'a framework for the regulation of online safety to address the proliferation of harmful online content to be administered by an Online Safety Commissioner'.[312] The aim was not 'to define harmful online content as a singular concept (…) [but] it is proposed to enumerate definitions of categories of material that are considered to be harmful online content'.[313] While disinformation or 'false statements' are not included as such a category, one cannot rule out overlaps between disinformation and other 'harmful content'.[314]

---

[308] Department of Housing, Local Government and Heritage, 'Ministers O'Brien and Noonan publish the General Scheme of the Electoral Reform Bill'.

[309] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Online Safety and Media Regulation Bill' *gov.ie* (10 Jan 2020) <www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/> accessed 11 Mar 2021; and Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Minister Martin presents additions to new law proposed for online safety and media regulation' *gov.ie* (9 Dec 2020) <www.gov.ie/en/press-release/1e05a-minister-martin-presents-additions-to-new-law-proposed-for-online-safety-and-media-regulation/> accessed 11 Mar 2021.

[310] AVMSD Art 28a(1). On the requirements in the revised AVMSD, see above Part II: Media Regulation.

[311] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Online Safety and Media Regulation Bill'.

[312] ibid. See General Scheme of the Online Safety Media Regulation Bill, Part 4 <https://assets.gov.ie/126000/b174bdcd-e017-47d9-bb48-07b29671330c.pdf> accessed 11 Mar 2021.

[313] General Scheme of the Online Safety Media Regulation Bill, 83.

[314] On disinformation and its connections with different legal contexts, see above Part I: Disinformation in different contexts.

When compared, the Irish electoral law framework includes many standard substantive limitations and procedural requirements similar to the ones in Germany, France and Spain, such as caps to campaign financing, prohibitions and limitations to certain types of donations, and financial reporting requirements. While such regulation undoubtedly serves an important role also in the context of online political advertising, especially when advertisers are parties or candidates, at the same time Ireland lacks a proper regulation tailored to the challenges of the online media around elections. As mentioned, so far in Ireland there is reliance on the data protection framework that flows from EU law. In that sense, the regulation in some other Member States, such as in France, seems more extensive and thus stricter. However, when compared with the other countries, Ireland has also started perhaps the most comprehensive overhaul of its regulation both in terms of electoral law (Electoral Reform Bill) and in terms of media law (Online Safety Media Regulation Bill). These laws could together cover many of the issues now regulated under the law against information manipulation in France and NetzDG in Germany. Especially the Electoral Reform Bill would incorporate online political advertising within the regulatory framework in a systematic way, clearly placing obligations on both political advertisers and online service providers. Yet, it should be noted that the final nature of the obligations is still unclear.

Poland

In Poland, the most important piece of election law is the 2011 Electoral Code.[315] In addition, there is a separate Act on Nationwide Referenda.[316] The oversight of election regulation is primarily trusted with the National Election Commission (NEC), which 'has the authority to issue binding instructions for election commissions and officials, as well as clarifications pertaining to election regulations for broadcasters, governmental authorities, and electoral committees'.[317] According to OSCE interlocutors, the role of the NEC is important and during the 2019 parliamentary elections for the lower and upper houses, *Sejm* and *Senat*, it 'supplemented the regulatory framework with a number of regulations, guidance and clarifications

[315] Ustawa z dnia 5 stycznia 2011 r. - Kodeks wyborczy, Dz.U. 2011 nr 21 poz. 112 <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20110210112> accessed 8 Mar 2021.

[316] Ustawa z dnia 14 marca 2003 r. o referendum ogólnokrajowym, Dz.U. 2003 nr 57 poz. 507 <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20030570507> accessed 8 Mar 2021.

[317] OSCE Office for Democratic Institutions and Human Rights, 'Republic of Poland: Parliamentary Elections 13 October 2019: ODIHR Limited Election Observation Mission Final Report' (Warsaw, 14 Feb 2020) 4.

on various aspects of the process'.[318] After the 2019 elections, the composition of the NEC was changed with new political appointments that prompted alarm for the erosion of the body's independence.[319]

The Electoral Code was comprehensively revised in 2018.[320] The relevant regulation includes, firstly, Article 107(1) that prevents campaigning on the election day. Thus, an electoral campaign starts from the date of announcement of the election day and it lasts until 24 hours before the election day. Article 115 provides that the release of opinion polls is also prohibited from 24 hours before the start of the vote to the end of voting. The same limitation is found in the Act on Nationwide Referenda.[321]

Secondly, in terms of campaign financing, all campaigns must be financed through election committees. Election committees of political parties and coalitions can be financed only through the designated party funds. Voters' election committees may in turn accept private donations.[322] However, indirectly private donations to party/coalition election committees are possible since parties and coalitions themselves may accept private donations that are not under disclosure requirements.[323] In addition, Articles 99 and 134 provide a donation cap for individuals and a spending cap for each election committee respectively and the criteria for calculating the exact limits.[324]

Anonymous donations from foreign actors and legal entities are prohibited.[325] Additionally, an electoral committee must publish on their websites loans and private donations exceeding one minimum monthly salary. However, in the 2018 revision of the Electoral Code, the sanction for third party campaigning without the consent of the candidate, party or coalition was repealed, resulting in unclear regulatory framework for third party campaigning.[326] The NEC has a prominent oversight role, as '[e]lectoral committees must submit financial reports on campaign

[318] ibid 5.

[319] ibid 6.

[320] ibid 5.

[321] Beata Klimkiewicz, 'PL – Poland' in Maja Cappello (ed), *Media coverage of elections: The legal framework in Europe* (European Audiovisual Observatory 2017) 90–91.

[322] OSCE, 'Republic of Poland: ODIHR Limited Election Observation Mission Final Report' 14.

[323] ibid 15.

[324] Vít Šimral and others, 'The Funding and Oversight of Political Parties and Election Campaigns in East Central Europe' *Frank Bold* (May 2015) 14–15 <https://en.frankbold.org/sites/default/files/publikace/the-funding-and-oversight-of-political-parties-and-election-campaigns-in-east-central-europe.pdf> accessed 8 Mar 2021.

[325] OSCE, 'Republic of Poland: ODIHR Limited Election Observation Mission Final Report' 15.

[326] ibid.

income and expenditures, together with an external audit of the financial report, to the NEC within three months of the elections'.[327]

Thirdly, as regards the dissemination of false information, Article 111 of the Electoral Code is of importance. It states that 'election material disseminated in the press' meaning 'posters, leaflets and slogans, as well as speeches or other forms of election propaganda' is subject to specific court procedure in case the correctness of information in the material is disputed.[328] Klimkiewicz summarizes the procedure as follows:

> [T]he relevant district court shall rule within twenty-four hours on a request for untrue information to be corrected, and its judgment shall be executed immediately (Article 111(2)). Any appeal against the decision of the district court must be lodged within twenty-four hours, and the appellate court must review the case within a further twenty-four hours – its judgment must then be executed immediately (Article 111(3)). The publication of a correction, reply or an apology must take place at the latest within forty-eight hours of the issuance of such a judgment; the court ruling must specify the media in which such a correction, reply or apology is to be published (Article 111(4)).[329]

In the context of local elections, a similar provision in the Polish Local Elections Act was challenged before the ECtHR and in 2019 the Strasbourg Court ruled that a restriction on the dissemination of election propaganda by the applicant was not corresponding to any pressing need and thus found a violation of Article 10 of the ECHR.[330]

Finally, the Electoral Code includes regulation of political advertising, including regulated prices, primarily on broadcast media.[331] While there are no specific provisions concerning online media, certain online news sites and portals have been considered to fall within the definition of 'the press' within the meaning of Article 7(2) of the 1984 Press Law Act. The regulations of print media apply to those online operators as well, even though there are

---

[327] OSCE, 'Republic of Poland: ODIHR Limited Election Observation Mission Final Report' 15.

[328] Klimkiewicz, 'PL – Poland' 94.

[329] ibid.

[330] *Brzeziński v Poland* App no 47542/07 (ECtHR, 25 July 2019). For a comment, see Ronan Ó Fathaigh, 'Brzeziński v. Poland: Fine over 'false' information during election campaign violated Article 10' *Strasbourg Observers* (8 Aug 2019) <https://strasbourgobservers.com/2019/08/08/brzezinski-v-poland-fine-over-false-information-during-election-campaign-violated-article-10/> accessed 9 Mar 2021.

[331] Klimkiewicz, 'PL – Poland' 91.

uncertainties regarding the specific sphere of online actors that are included.[332] Recently, however, Poland has expressed growing interest in regulating social media specifically as well.[333]

In terms of electoral law, the Polish regulation shares many features with the other Member States' electoral law, including financial reporting requirements like in all the other Member States, and limitations to the campaign time like in Spain. An important regulatory role is assigned to the central election administration both in Spain (*Junta Electoral Central*) and Poland (NEC). Again, similarly to Spain and also to Ireland, there is a ban on anonymous donations in Poland. Moreover, it is notable that the rules on third party campaigning have been pointed to be somewhat unclear and a similar lack of proper regulation on third party campaigning has been expressed in relation to Germany and France as well. Finally, Article 111 of the Electoral Code, which contains the court procedure on the removal of incorrect election information, appears to share some similarities with the French court procedure established to intervene into the dissemination of inaccurate and misleading information around elections. However, it should be noted that the French law also places additional conditions compared to the Polish law, since the misleading or inaccurate information must also be 'disseminated in a deliberate, artificial or automated and massive manner'.

[332] Klimkiewicz, 'PL – Poland' 95.

[333] See, Adam Easton, 'Poland proposes social media 'free speech' law' *BBC News* (15 Jan 2021) <www.bbc.com/news/technology-55678502> accessed 9 Mar 2021.

Conclusive Summary

The goal of this report has been to lay out a map of the intricate regulatory field of online political advertising in Europe. The first of part of the report addressed the target and function of regulation. It was stated that disinformation as a policy formulation could be translated into crisper legal understandings by thinking it in different contexts. Disinformation in the context of advertising, and then even more specifically online political advertising, was chosen as a proper delineation for guiding the mapping of relevant regulation in the subsequent parts of the report.

The second part of the report mapped regulation on the higher European level that mostly focuses on the regulation of different services and technologies facilitating information online. The most relevant legal areas include data protection law and the regulation of electronic commerce. In addition, the more complementary regulation of EU media law, unfair commercial practices, and self-regulatory efforts were outlined. It was found out that in general the state of relevant EU law is in flux with new laws and other regulatory initiatives being processed in the fields of data protection, e-commerce, and artificial intelligence. The EU has considerable interest to introduce further regulation on online services. There are also uncertainties concerning the interpretation of existing laws, for instance, on data protection obligations and intermediary liability.

The third part of the report delved into the regulation of elections and online media in Germany, France, Spain, Ireland, and Poland. It was found out that Member States have developed intricate and frequently amended regulatory frameworks regarding elections and political parties and candidates. However, some parts of the regulation have to some extent been disrupted by emergent online services that afford new ways of influencing for candidates and other politically motivated actors. For instance, restrictions on campaign times, electoral coverage, and political advertising may lose some of their effectiveness due to the increasing use of online information services. In addition, third party campaigning may become more prominent in the future as online services bring new campaigning and advertising possibilities to a much larger group of actors than before. These technologies also afford campaigning outside transnationally and therefore beyond the jurisdiction of national election laws. So far, the addressed Member States lack electoral/media law that would comprehensively and systematically take into account the deployment of online services in the dissemination of election propaganda. However, there is increasing attention paid to online services that circles

heavily around the utilization of the largest social networking platforms. While laws on disinformation or illegal speech have been put in place in France and Germany, Ireland is probably processing the most comprehensive legal overhaul covering both electoral and media law. One may expect considerable regulatory developments both on the EU and Member State level in the upcoming years.

References

Legislation

International

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended)

European Union

Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L149/22

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending 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) in view of changing market realities [2018] OJ L303/69

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Germany

Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) <www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2> accessed 18 Feb 2021

Criminal Code (*Strafgesetzbuch – StGB*) <www.gesetze-im-internet.de/englisch_stgb/> accessed 16 Mar 2021

Federal Elections Act, version as promulgated on 23 July 1993 (Federal Law Gazette I pp. 1288, 1594), last amended by Article 1 of the Act of 28 October 2020 (Federal Law Gazette I p. 2264)

Federal Electoral Regulations, version as promulgated on 19 Apr 2002 (Federal Law Gazette I p. 1376), last amended by Article 10 of the Ordinance of 19 June 2020 (Federal Law Gazette I p. 1328)

Law on the Scrutiny of Elections (*WahlPrG*), revised version as promulgated in the Federal Law Gazette, Section III, classification number 111-2, last amended by Article 11 of the Ordiance of 19 June 2020 (Federal Law Gazette I, p. 1328)

Act on Political Parties (*Parteiengesetz – PartG*) version published on 31 January 1994 (Federal Law Gazette I 1994, p. 149), last amended by the Ninth Act amending the Political Parties Act, of 22 December 2004 (Federal Law Gazette I 2004, p. 3673)

France

Code électoral (Electoral Code) <www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/2021-03-18/> accessed 22 Feb 2021

Loi du 29 juillet 1881 sur la liberté de la presse (Freedom of Press Act) <www.legifrance.gouv.fr/loda/id/JORFTEXT000000877119/?isSuggest=true> accessed 22 Feb 2021

Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (Law on the fight against information manipulation) <www.legifrance.gouv.fr/loda/id/JORFTEXT000037847559/?isSuggest=true> accessed 22 Feb 2021

Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (Law to combat hateful content on Internet) <www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970/> accessed 16 Mar 2021

Spain

Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (Organic Law on the General Electoral System) <www.boe.es/buscar/act.php?id=BOE-A-1985-11672> accessed 1 Mar 2021

Ley Orgánica 8/2007, de 4 de julio, sobre financiación de los partidos politicos (Organic Law on the Financing of Political Parties) <https://boe.es/buscar/act.php?id=BOE-A-2007-13022> accessed 2 Mar 2021

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (Organic Law on the Protection of Personal Data and Guarantee of Digital Rights) <www.boe.es/buscar/doc.php?id=BOE-A-2018-16673> accessed 2 Mar 2021

Ireland

Electoral Act, 1997, Law No. 25 of 1997 <www.irishstatutebook.ie/eli/1997/act/25/enacted/en/html> accessed 10 Mar 2021

Broadcasting Act, 2009, Law No. 18 of 2009, <www.irishstatutebook.ie/eli/2009/act/18/enacted/en/html?q=Broadcasting+Act> accessed 10 Mar 2021

General Scheme of the Electoral Reform Bill 2020 <https://assets.gov.ie/118345/15ac22d0-1d73-438a-a1f8-4958bdacafa6.pdf> accessed 11 Mar 2021

General Scheme of the Online Safety Media Regulation Bill <https://assets.gov.ie/126000/b174bdcd-e017-47d9-bb48-07b29671330c.pdf> accessed 11 Mar 2021

Poland

Ustawa z dnia 5 stycznia 2011 r. - Kodeks wyborczy (Electoral Code), Dz.U. 2011 nr 21 poz. 112 <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20110210112> accessed 8 Mar 2021

Ustawa z dnia 14 marca 2003 r. o referendum ogólnokrajowym (Law on National Referendum), Dz.U. 2003 nr 57 poz. 507 <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20030570507> accessed 8 Mar 2021

Case law

CJEU

Joined Cases C-236/08–C-238/08, *Google France and Google Inc. v Louis Vuitton Malletier and others* [2010] ECR I–2417

Case C-324/09, *L'Oréal SA and Others v eBay International AG and Others* [2011] ECR I–6011

Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, EU:C:2016:779

Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, EU:C:2018:388

Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, EU:C:2019:458

Case C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, EU:C:2019:629

Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH,* EU:C:2019:801

Case C-61/19, *Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP),* EU:C:2020:901

ECtHR

VgT Verein Gegen Tierfabriken v Switzerland ECHR 2001–VI 243

TV Vest AS & Rogaland Pensjonistparti v Norway ECHR 2008-V 265

Centro Europa 7 Srl and Di Stefano v Italy ECHR 2012–III 339

Animal Defenders International v the United Kingdom ECHR 2013–II 203

Delfi v Estonia ECHR 2015–II 319

Cengiz and Others v Turkey ECHR 2015–VIII 177

Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary App no 22947/13 (ECtHR, 2 Feb 2016)

Brzeziński v Poland App no 47542/07 (ECtHR, 25 July 2019)

France

Conseil Constitutionnel, Décision n° 2020-801 DC du 18 juin 2020 <www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm> accessed 16 Mar 2021

Spain

Sentencia del Tribunal Constitucional n.º 76/2019, de 22 de mayo de 2019 (Judgment 76/2019, of 22 May 2019), Recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo respecto del apartado primero del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (BOE n.º 151 de 25-VI-

2019) <http://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2019-9548.pdf> accessed 2 Mar 2021

European Commission and Council of the European Union documents

Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses' SWD(2016) 163 final

Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life 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

Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final

Commission, 'Code of Practice on Disinformation' (Apr 2018) <https://ec.europa.eu/digital-single-market/en/code-practice-disinformation> accessed 1 Feb 2021

Commission, 'Code of Practice on Disinformation: Annex II: Current best practices from Signatories of the Code of Practice' (Apr 2018) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54455> accessed 18 Mar 2021

Commission, 'Commission guidance on the application of Union data protection law in the electoral context' COM(2018) 638 final

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

Commission, 'Digital Single Market: Updated audiovisual rules' MEMO/18/4093

Commission, 'Commission Staff Working Document: Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement' SWD(2020) 180 final

Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' COM(2020) 264 final

Commission, 'On the European democracy action plan' COM(2020) 790 final

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)' COM(2020) 767 final

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final

Commission, 'Audiovisual Media: Commission opens infringement procedures against 23 Member States for failing to transpose the Directive on audiovisual content' IP/20/2165 <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2165> accessed 1 Feb 2021

Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM(2021) 206 final

Commission, 'European Commission Guidance on Strengthening the Code of Practice on Disinformation' COM(2021) 262 final

Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP' (10 Feb 2021) 6087/21

Other secondary sources

Ajji, Kamel, 'Protecting liberal democracy from artificial information: The French proposal' in Petkova, Bilyana and Ojanen, Tuomas (eds), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries* (Edward Elgar Publishing 2020).

Ananny, Mike, 'Making up Political People: How Social Media Create the Ideals, Definitions and Probabilities of Political Speech' (2020) 4(1) Georgetown Law Technology Review 1

Article 29 Data Protection Working Party (WP29), 'Opinion 03/2013 on purpose limitation' (WP 203, 2 Apr 2013)

—— 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (last revised and adopted on 6 Feb 2018)

Baldwin-Philippi, Jessica, 'Data campaigning: Between empirics and assumptions' (2019) 8(4) Internet Policy Review 1

Bayer, Judit, 'Double harm to voters: data-driven microtargeting and democratic public discourse' (2020) 9(1) Internet Policy Review 1

—— and others, 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States' (Feb 2019) Study commissioned by European Parliament's LIBE Committee, PE 608.864

Blázquez, Francisco Javier Cabrera, 'ES – Spain' in Cappello, Maja (ed), *Media coverage of elections: The legal framework in Europe* (European Audiovisual Observatory 2017)

Boerman, SC and others, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46 Journal of Advertising 363

Borgesius, Frederik J Zuiderveen, 'Personal data processing for behavioural targeting: Which legal basis?' (2015) 5 International Data Privacy Law 163

—— and others, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14(1) Utrecht Law Review 82

Brkan, Maja and Bonnet, Grégory, 'Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas' (2020) 11 European Journal of Risk Regulation 18

Cadwalladr, Carole and Graham-Harrison, Emma, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' *The Guardian* (17 Mar 2018) <www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 6 Apr 2021

Cervi, Laura, Roca, Nuria 'La modernización de la campaña electoral para las elecciones generales de España en 2015. ¿Hacia la americanización?' (2017) Comunicación y Hombre, no. 13

Cohen, Julie E, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP 2019)

Conseil Supérieur de l'Audiovisuel (CSA), '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' <www.csa.fr/Informer/Espace-presse/Communiques-de-presse/Adoption-de-la-recommandation-relative-a-la-lutte-contre-la-manipulation-de-l-information-un-pas-de-plus-vers-une-nouvelle-regulation> accessed 25 Feb 2021

Data Protection Commission, 'DPC publishes guidance on data protection and electoral and canvassing activities' (9 Oct 2018) <www.dataprotection.ie/en/news-media/latest-news/dpc-publishes-guidance-data-protection-and-electoral-and-canvassing-activities> accessed 10 Mar 2021

Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, 'Online Safety and Media Regulation Bill' *gov.ie* (10 Jan 2020) <www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/> accessed 11 Mar 2021

—— 'Minister Martin presents additions to new law proposed for online safety and media regulation' *gov.ie* (9 Dec 2020) <www.gov.ie/en/press-release/1e05a-minister-martin-presents-additions-to-new-law-proposed-for-online-safety-and-media-regulation/> accessed 11 Mar 2021

Department of Housing, Local Government and Heritage, 'Ministers O'Brien and Noonan publish the General Scheme of the Electoral Reform Bill' *gov.ie* (8 Jan 2021) <www.gov.ie/en/press-release/0dfe8-ministers-obrien-and-noonan-publish-the-general-scheme-of-the-electoral-reform-bill/> accessed 11 Mar 2021

Dobber, Tom, Ó Fathaigh, Ronan and Borgesius, Frederik J. Zuiderveen, 'The regulation of online political micro-targeting in Europe' (2019) 8(4) Internet Policy Review 1

Dommett, Katharine, 'Data-driven political campaigns in practice: Understanding and regulating diverse data-driven campaigns' (2019) 8(4) Internet Policy Review 1

Earp, Madeline, 'Germany revisits influential internet law as amendment raises privacy implications' *CPJ* (7 Oct 2020) <https://cpj.org/2020/10/germany-revisits-influential-internet-law-as-amendment-raises-privacy-implications/> accessed 18 Feb 2021

Easton, Adam, 'Poland proposes social media 'free speech' law' *BBC News* (15 Jan 2021) <www.bbc.com/news/technology-55678502> accessed 9 Mar 2021

Edelman, Gilad, 'Ad Tech Could Be the Next Internet Bubble' *WIRED* (10 May 2020) <www.wired.com/story/ad-tech-could-be-the-next-internet-bubble/> accessed 3 Feb 2021

EDRi, 'French Avia law declared unconstitutional: What does this teach us at EU level?' (24 June 2020) <https://edri.org/our-work/french-avia-law-declared-unconstitutional-what-does-this-teach-us-at-eu-level/> accessed 16 Mar 2021

Edwards, Lilian and Veale, Michael, 'Slave to the Algorithm: Why a Right to an Explanation is Probably Not the Remedy You are Looking for' (2017) 16 Duke Law & Technology Review 18

Edwards, Lilian and Veale, Michael, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018) 16 IEEE Security & Privacy 46

Etteldorf, Christina, 'DE – Germany' in Cappello, Maja (ed), *Media coverage of elections: The legal framework in Europe* (European Audiovisual Observatory 2017)

European Data Protection Board (EDPB), 'Statement 2/2019 on the use of personal data in the course of political campaigns' (adopted 13 Mar 2019)

—— 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020)

—— 'Guidelines 8/2020 on the targeting of social media users' (adopted 2 Sep 2020)

—— 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (version 2.0, 20 Oct 2020)

—— 'Register of certification mechanisms, seals and marks' <https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en> accessed 15 Apr 2021

European Data Protection Supervisor (EDPS), 'Opinion 3/2018: EDPS Opinion on online manipulation and personal data' (19 Mar 2018)

European Regulators Group for Audiovisual Media Services (ERGA), 'ERGA Report on disinformation: Assessment of the implementation of the Code of Practice' (4 May 2020) <https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf> accessed 5 Feb 2021

Facebook, 'Facebook will not be accepting referendum related ads from advertisers based outside of Ireland' (8 May 2018) <www.facebook.com/notes/facebook-dublin/facebook-will-not-be-accepting-referendum-related-ads-from-advertisers-based-out/10156398786998011/> accessed 10 Mar 2021

Facebook for Business, 'About ad auctions' <https://en-gb.facebook.com/business/help/430291176997542?id=561906377587030> accessed 19 Mar 2021

François, Camille, 'Actors, Behaviors, Content: A Disinformation ABC Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses' (20 Sep 2019) Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression Working Paper <www.ivir.nl/twg/publications-transatlantic-working-group/> accessed 6 Apr 2021

Frederik, Jesse and Martijn, Maurits, 'The new dot com bubble is here: It's called online advertising' *The Correspondent* (6 Nov 2019) <https://thecorrespondent.com/100/the-new-dot-com-bubble-is-here-its-called-online-advertising/13228924500-22d5fd24> accessed 3 Feb 2021

Ghosh, Dipayan and Scott, Ben, '#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet' (23 Jan 2018) New America Policy Paper <www.newamerica.org/pit/policy-papers/digitaldeceit/> accessed 6 Apr 2021

Gillespie, Tarleton, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018)

González, María Holgado, 'Publicidad e información sobre elecciones en los medios de comunicación durante la campaña electoral' (2017) UNED. Teoría y Realidad Constitucional, no. 40, 457–485

Google, 'Advertising Policies Help: Political content' (2021) <https://support.google.com/adspolicy/answer/6014595?hl=en> accessed 5 Feb 2021

Granchet, Agnès, 'FR – France' in Cappello, Maja (ed), *Media coverage of elections: The legal framework in Europe* (European Audiovisual Observatory 2017)

High Level Expert Group, 'A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation' (Mar 2018) <https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en> accessed 23 Mar 2021

Hochmann, Thomas, 'Shedding Light or Shooting in the Dark – How to define Fake News?' *Verfassungsblog* (5 Sep 2018) <https://verfassungsblog.de/shedding-light-or-shooting-in-the-dark-how-to-define-fake-news/> accessed 16 Mar 2021

Hoofnagle, Chris Jay, van der Sloot, Bart and Borgesius, Frederik Zuiderveen, 'The European Union general data protection regulation: what it is and what it means' (2019) 28 Information & Communications Technology Law 68

Hwang, Tim, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet* (FSG Originals 2020)

Junta Electoral Central, 'Instrucción 4/2007, de 12 de abril, de la Junta Electoral Central, sobre la utilización de las nuevas tecnologías de la información y de la comunicación electrónicas como instrumento de propaganda electoral', BOE-A-2007-8181 <www.boe.es/buscar/pdf/2007/BOE-A-2007-8181-consolidado.pdf> accessed 1 Mar 2021

—— 'Instrucción 2/2011, de 24 de marzo, de la Junta Electoral Central, sobre interpretación del artículo 50 de la Ley Orgánica del Régimen Electoral General, en relación al objeto y los límites de las campañas institucionales y de los actos de inauguración realizados por los poderes públicos en periodo electoral', BOE-A-2011-5522 <www.boe.es/buscar/pdf/2011/BOE-A-2011-5522-consolidado.pdf> accessed 1 Mar 2021

Kavanagh, Jennifer, 'Electoral Law in Ireland: Sustaining Electoral Integrity from Process, Procedures, and Precedent?' (2015) 30 Irish Political Studies 510

Klimkiewicz, Beata, 'PL – Poland' in Cappello, Maja (ed), *Media coverage of elections: The legal framework in Europe* (European Audiovisual Observatory 2017)

Kruschinski, Simon and Haller, André, 'Restrictions on data-driven political micro-targeting in Germany' (2017) 6(4) Internet Policy Review 1

Kuczerawy, Aleksandra, 'The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act' *Verfassungsblog* (12 Jan 2021) <https://verfassungsblog.de/good-samaritan-dsa/> accessed 20 Jan 2021

Laux, Johann, Wachter, Sandra and Mittelstadt, Brent, 'Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice' (2021) 58(3) Common Market Law Review 719

Leiser, Mark, 'AstroTurfing, 'CyberTurfing' and other online persuasion campaigns' (2016) 7(1) European Journal of Law and Technology 1

Marwick, Alice and Lewis, Rebecca, 'Media Manipulation and Disinformation Online' (15 May 2017) Data & Society Report <https://datasociety.net/library/media-manipulation-and-disinfo-online/> accessed 6 Apr 2021

—— and others, 'Critical Disinformation Studies: A Syllabus' (2021) Center for Information, Technology, & Public Life (CITAP), University of North Carolina at Chapel Hill <https://citap.unc.edu/critical-disinfo> accessed 6 Apr 2021

McQuinn, Cormac, 'Warning that foreign ads "could influence referendum on Eighth Amendment"' *Independent.ie* (18 Apr 2018) <www.independent.ie/irish-news/abortion-referendum/warning-that-foreign-ads-could-influence-referendum-on-eighth-amendment-36817674.html> accessed 10 Mar 2021

Merrill, Jeremy B, 'Facebook Charged Biden a Higher Price Than Trump for Campaign Ads' *The Markup* (29 Oct 2020) <https://themarkup.org/election-2020/2020/10/29/facebook-political-ad-targeting-algorithm-prices-trump-biden> accessed 19 Mar 2021

Mission report submitted to the 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' (May 2019) <www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf> accessed 2 Mar 2021

Neudert, Lisa-Maria N, 'Computational Propaganda in Germany: A Cautionary Tale' (2017) University of Oxford Computational Propaganda Research Project Working Paper No. 2017.7 <www.oii.ox.ac.uk/blog/computational-propaganda-in-germany-a-cautionary-tale/> accessed 6 Apr 2021

Oderkerk, Marieke, 'The Importance of Context: Selecting Legal Systems in Comparative Research' (2001) XLVIII Netherlands International Law Review 298

Ó Fathaigh, Ronan, 'Brzeziński v. Poland: Fine over 'false' information during election campaign violated Article 10' *Strasbourg Observers* (8 Aug 2019) <https://strasbourgobservers.com/2019/08/08/brzezinski-v-poland-fine-over-false-information-during-election-campaign-violated-article-10/> accessed 9 Mar 2021

OSCE Office for Democratic Institutions and Human Rights, 'Republic of France: Presidential Election 23 April and 7 May 2017: OSCE/ODIHR Election Expert Team Final Report' (Warsaw, 30 Aug 2017)

—— 'Elections to the Federal Parliament (Bundestag) 24 September 2017: OSCE/ODIHR Election Expert Team Final Report' (Warsaw, 27 Nov 2017)

—— 'Republic of Poland: Parliamentary Elections 13 October 2019: ODIHR Limited Election Observation Mission Final Report' (Warsaw, 14 Feb 2020)

Peinado, Fernando, 'The business of digital manipulation in Spain' *El País* (24 May 2018) <https://english.elpais.com/elpais/2018/05/24/inenglish/1527147309_000141.html> accessed 16 Mar 2021

Polanski, Paul Przemysław, 'Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union' (2018) 34 Computer Law & Security Review 562

Provost, Calara and Whyte, Lara, 'Foreign and 'alt-right' activists target Irish voters on Facebook ahead of abortion referendum' *OpenDemocracy* (25 Apr 2018) <www.opendemocracy.net/en/5050/north-american-anti-abortion-facebook-ireland-referendum/> accessed 10 Mar 2021

Ramos, Diego, 'Spain: New Data Protection Act (partly) nullified by the Constitutional Court' *Privacy Matters: DLA Piper's Global Privacy and Data Protection Resource* (23 May 2019) <https://blogs.dlapiper.com/privacymatters/spain-new-data-protection-act-partly-nullified-by-the-constitutional-court/> accessed 2 Mar 2021

Sankin, Aaron, 'Want to Find a Misinformed Public? Facebook's Already Done It' *The Markup* (23 Apr 2020) <https://themarkup.org/coronavirus/2020/04/23/want-to-find-a-misinformed-public-facebooks-already-done-it> accessed 14 Dec 2020

Sørensen, Karsten Engsig, 'Enforcement of Harmonization Relying on the Country of Origin Principle' (2019) 25 European Public Law 381

Siems, Mathias M, *Comparative Law* (2nd edn, CUP 2018)

Šimral, Vít and others, 'The Funding and Oversight of Political Parties and Election Campaigns in East Central Europe' *Frank Bold* (May 2015) 14–15

<https://en.frankbold.org/sites/default/files/publikace/the-funding-and-oversight-of-political-parties-and-election-campaigns-in-east-central-europe.pdf> accessed 8 Mar 2021

Standards in Public Office Commission, 'Electoral' <www.sipo.ie/acts-and-codes/legislation/electoral/> accessed 10 Mar 2021

Subramanian, Samanth, 'Inside the Macedonian Fake-News Complex' *WIRED* (15 Feb 2017) <www.wired.com/2017/02/veles-macedonia-fake-news/> accessed 16 Mar 2021

Tambini, Damian, 'Internet and electoral campaigns: Study on the use of internet in electoral campaigns' (Apr 2018) Council of Europe study DGI(2017)11

—— 'Media Freedom, Regulation and Trust: A Systemic Approach to Information Disorder' Council of Europe Background Paper, Ministerial Conference (Cyprus, 28-29 May 2020)

Tucker, Joshua A and others, 'Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature' *Hewlett Foundation* (Mar 2018)

Twitter for Business, 'Political Content' (2021) <https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html> accessed 19 Apr 2021

Tworek, Heidi and Leerssen, Paddy, 'An Analysis of Germany's NetzDG Law' (15 Apr 2019) Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2 <www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf> accessed 18 Feb 2021

UK Digital, Culture, Media and Sport select committee, 'Disinformation and 'fake news': Final Report' (18 Feb 2019) <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179104.htm> accessed 6 Apr 2021

van Eijk, Nico and others, 'Unfair Commercial Practices: A Complementary Approach to Privacy Protection' (2017) 3(3) European Data Protection Law Review 325

van Hoboken and others, 'The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising' (Dec 2019) Final Report, Institute for Information Law (IViR), University of Amsterdam

Veale, Michael and Edwards, Lilian, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34 Computer Law & Security Review 398.

—— and Borgesius, Frederik Zuiderveen, 'Adtech and Real-Time Bidding under European Data Protection Law' (2021) German Law Journal (forthcoming) 3–4 <https://osf.io/preprints/socarxiv/wg8fq/> accessed 11 June 2021

Vilmer, Jean-Baptiste Jeangène and others, 'Information manipulation: A challenge for our democracies' (Aug 2018) Report to the Minister for Europe and Foreign Affairs

Wachter, Sandra, Mittelstadt, Ben and Floridi, Luciano, 'Why a Right to Explanation of Automated Decision-Making does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76

Wardle, Claire and Derakhshan, Hossein, 'Information Disorder: Toward an interdisciplinary framework for research and policymaking' (Sep 2017) Council of Europe report DGI(2017)09

Wischmeyer, Thomas, ''What is illegal offline is also illegal online': The German Network Enforcement Act 2017' in Petkova, Bilyana and Ojanen, Tuomas (eds), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries* (Edward Elgar Publishing 2020) 28

Woods, Lorna, 'Digital freedom of expression in the EU' in Douglas-Scott, Sionaidh and Hatzis, Nicholas (eds), *Research Handbook on EU law and Human Rights* (Edward Elgar Publishing 2017) 394

Zittrain, Jonathan, 'Engineering an Election' (2014) 127 Harvard Law Review Forum 335