Unpacking the "European approach" to tackling challenges of disinformation and political manipulation

Iva Nenadić

Faculty of Political Science, University of Zagreb, Croatia, iva.nenadic@fpzg.hr

Abstract: The European Commission (EC) has recognised the exposure of citizens to online disinformation and micro-targeting of voters based on the unlawful processing of personal data as one of the major challenges for European democracies. In a response, the EC has put in place several measures creating a "European approach". This paper analyses the approach to identify which are the key principles upon which it is based; and the extent to which it takes into account the complexities of the challenges identified. The initial conclusions are that, while being a significant step in the creation of a common EU answer to disinformation and political manipulation, the "European approach" requires further elaboration, primarily to include additional layers of transparency and public oversight.

This paper is part of Data-driven elections, a special issue of Internet Policy Review *guest-edited by Colin J. Bennett and David Lyon.*

INTRODUCTION

In recent years, the spread of disinformation on online platforms and micro-targeted data-driven political advertising has become a serious concern in many countries around the world, in particular as regards the impact this practice may have on informed citizenship and

democratic systems. In April 2019, for the first time in the country's modern history, Switzerland's supreme court has overturned a nationwide referendum on the grounds that the voters were not given complete information and that it "violated the freedom of the vote". While in this case it was the government that had failed to provide correct information, the decision still comes as another warning of the conditions under which elections nowadays are being held and as a confirmation of the role that accurate information plays in this process. There is limited and sometimes even conflicting scholarly evidence as to whether today people are exposed to more diverse political information or trapped in echo chambers, and whether they are more vulnerable to political disinformation and propaganda than before (see, for example: Bruns, 2017, and Dubois & Blank, 2018). Yet, many claim so, and cases of misuse of technological affordances and personal data for political goals have been reported globally.

The decision of Switzerland's supreme court has particularly resonated in Brexit Britain where the campaign ahead of the European Union (EU) membership referendum left too many people feeling "ill-informed" (Brett, 2016, p. 8). Even before the Brexit referendum took place, the House of Commons Treasury Select Committee complained about "*the absence of 'facts' about the case for and against the UK's membership on which the electorate can base their vote*" (2016, p. 3). According to this, the voters in the United Kingdom were not receiving complete or even truthful information, and there are also concerns that they might have been manipulated by the use of bots (Howard & Kollanyi, 2016) and by the unlawful processing of personal data (ICO, 2018a, 2018b).

The same concerns were raised in the United States during and after the presidential elections in 2016. Several studies have shown evidence of the exposure of US citizens to social media disinformation in the period around elections (see: Guess et al., 2018, and Allcott & Gentzkow, 2017). In other parts of the world, such as in Brazil and in several Asian countries, the means and platforms for transmission of disinformation were somewhat different but the associated risks have been deemed even higher. The most prominent world media, fact checkers and researchers systematically reported about the scope and spread of disinformation on the Facebook-owned and widely used messaging application WhatsApp in the 2018 presidential elections in Brazil. Freedom House warned that elections in some Asian countries, such as India, Indonesia, and Thailand, were also afflicted by falsified content.

Clearly, online disinformation and unlawful political micro-targeting represent a threat to elections around the globe. The extent to which certain societies are more resilient or more vulnerable to the impact of these phenomena depends on different factors, including, among other things, the status of journalism and legacy media, levels of media literacy, the political context and legal safeguards (CMPF, forthcoming). Different political and regulatory traditions play a role in shaping the responses to online disinformation and data-driven political manipulation. Accordingly, these range from doing nothing to criminalising the spread of disinformation, as is the case with the Singapore's law 1 which came into effect in October 2019. While there seems to be more agreement that regulatory intervention is needed to protect democracy, the concerns over the negative impact of inadequate or overly restrictive regulation on freedom of expression remain. In his recent reports (2018, 2019), UN Special Rapporteur on Freedom of Expression David Kaye warned against regulation that entrusts platforms with even more powers to decide on content removals in very short time frames and without public oversight. Whether certain content is illegal or problematic on other grounds is not always a straightforward decision and often depends on the context in which it is presented. Therefore, as highlighted by the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression (2019), to require platforms to make these content moderation decisions

in an automated way, without built-in transparency, and without notice or timely recourse for appeal, contains risks for freedom of expression.

The European Commission (EC) has recognised *the exposure of citizens to large scale online disinformation* (2018a) and *micro-targeting of voters based on the unlawful processing of personal data* (2018b) as major challenges for European democracies. In a response to these challenges, and to ensure citizens' access to a variety of credible information and sources, the EC has put in place several measures which aim to create an overarching "European approach". This paper provides an analysis of this approach to identify the key principles upon which it builds, and to what extent, if at all, they differ from the principles of "traditional" political advertising and media campaign regulation during the electoral period. The analysis further looks at how these principles are elaborated and whether they reflect the complexity of the challenges identified. The focus is on the EU as it is "*articulating a more interventionist approach*" to the relations with the online platform companies (Flew et al., 2019, p. 45). Furthermore, due to the size of the European market, any relevant regulation can set the global standard, as is the case with the General Data Protection Regulation (GDPR) in the area of data protection and privacy (Flew et al., 2019).

THE ROLE OF (SOCIAL) MEDIA IN ELECTIONS

The paper starts from the notion that a healthy democracy is dependent on pluralism and that the role of (social) media in elections and the transparency of data-driven political advertising are among the crucial components of any assessment of the state of pluralism in a given country. In this view, pluralism "implies all measures that ensure citizens' access to a variety of information sources, opinion, voices etc. in order to form their opinion without the undue influence of one dominant opinion forming power" (EC, 2007, p. 5; Valcke et al., 2009, p. 2). Furthermore, it implies the relevance of citizens' access to truthful and accurate information.

The media have long been playing a crucial role in election periods: serving, on one side, as wide-reaching platforms for parties and candidates to deliver their messages, and, on the other, helping voters to make informed choices. They set the agenda by prioritising certain issues over others and by deciding on time and space to be given to candidates; they frame their reporting within a certain field of meaning and considering the characteristics of different types of media; and, if the law allows, they sell time and space for political advertising (Kelley, 1963). A democracy requires the protection of media freedom and editorial autonomy, but asks that the media be socially responsible. This responsibility implies respect of fundamental standards of journalism, such as impartiality and providing citizens with complete and accurate information. As highlighted on several occasions by the European Commission for Democracy through Law (so-called Venice Commission) of the Council of Europe (2013, paras. 48, 49): "The failure of the media to provide impartial information about the election campaign and the candidates is one of the most frequent shortcomings that arise during elections".

Access to the media has been seen as "one of the main resources sought by parties in the campaign period" and to ensure a level playing field "legislation regarding access of parties and candidates to the public media should be non-discriminatory and provide for equal treatment" (Venice Commission, 2010, para. 148). The key principles of media regulation during the electoral period are therefore media impartiality and equality of opportunity for contenders. Public service media are required to abide by higher standards of impartiality compared to private outlets, and audiovisual media are more broadly bound by rules than the printed press

and online media. The latter are justified by the perceived stronger effects of audiovisual media on voters (Schoenbach & Lauf, 2004) and by the fact that television channels benefit from the public and limited resource of the radio frequency spectrum (Venice Commission, 2009, paras. 24-28, 58).

In the Media Pluralism Monitor (MPM) 2, a research tool supported by the European Commission and designed to assess risks to media pluralism in EU member states, the role of media in the democratic electoral process is one out of 20 key indicators. It is seen as an aspect of political pluralism and the variables against which the risks are assessed have been elaborated in accordance with the above-mentioned principles. The indicator assesses the existence and implementation of a regulatory and self-regulatory framework for the fair representation of different political actors and viewpoints on public service media and private channels, especially during election campaigns. The indicator also takes into consideration the regulation of political advertising – whether the restrictions are imposed to allow equal opportunities for all political parties and candidates.

The MPM results (Brogi et al., 2018) showed that the rules to ensure the fair representation of political viewpoints in news and informative programmes on public service media channels and services are imposed by law in all EU countries. It is, however, less common for such regulation and/or self-regulatory measures to exist for private channels. A similar approach is observed in relation to political advertising rules, which are more often and more strictly defined for public service than for commercial media. Most countries in the EU have a law or another statutory measure that imposes restrictions on political advertising during election campaigns to allow equal opportunities for all candidates. Even though political advertising is "considered as a legitimate instrument for candidates and parties to promote themselves" (Holtz-Bacha & Just, 2017, p. 5), some countries do not allow it at all. In cases when there is a complete ban on political advertising, public service media provide free airtime on principles of equal or proportionate access. In cases when paid political advertising is allowed, it is often restricted only to the campaign period and regulation seeks to set limits on, for example, campaign resources and spending, the amount of airtime that can be purchased and the timeframe in which political advertising can be broadcast. In most countries there is a requirement for transparency – how much was spent for advertising in the campaign, presented through spending on different types of media. For traditional media, the regulatory framework requires that political advertising (as any other advertising) be properly identified and labelled as such.

Television remains the main source of news for citizens in the EU (Eurobarometer, 2018a, 2017). However, the continuous rise of online sources and platforms as resources for (political) news and views (Eurobarometer, 2018a), and as channels for more direct and personalised political communication, call for a deeper examination of the related practice and potential risks to be addressed. The ways people find and interact with (political) news and the ways political messages are being shaped and delivered to people has been changing significantly with the global rise, popularity and features offered by the online platforms. An increasing number of people, and especially young populations, are using them as doors to news (Newman et al., 2018, p. 15; Shearer, 2018). Politicians are increasingly using the same doors to reach potential voters, and the online platforms have become relevant, if not central, to different stages of the whole process. This means that platforms are now increasingly performing functions long attributed to media and much more through, for example, filtering and prioritising certain content offered to users, and selling the time and space for political advertising based on data-driven micro-targeting. At the same time, a majority of EU countries still do not have specific requirements that would ensure transparency and fair play in campaigning, including political

advertising in the online environment. According to the available MPM data (Brogi et al., 2018; and preliminary data collected in 2019), only 11 countries (Belgium, Bulgaria, Denmark, Finland, France, Germany, Italy, Latvia, Lithuania, Portugal and Sweden) have legislation or guidelines to require transparency of online political advertisements. In all cases, it is the general law on political advertising during the electoral period that also applies to the online dimension.

Political advertising and political communication more broadly take on different forms in the environment of online platforms, which may hold both promises and risks for democracy (see, for example, Valeriani & Vaccari, 2016; and Zuiderveen Borgesius et al., 2018). There is still limited evidence on the reach of online disinformation in Europe, but a study conducted by Fletcher et al. (2018) suggests that even if the overall reach of publishers of false news is not high, they achieve significant levels of interaction on social media platforms. Disinformation online comes in many different forms, including false context, imposter, manipulated, fabricated or extreme partisan content (Wardle & Derakhshan, 2017), but always with an intention to deceive (Kumar & Shah, 2018). There are also different motivations for the spread of disinformation, including financial and political (Morgan, 2018), and different platforms' affordances affect whether disinformation spreads better as organic content or as paid-for advertising. Vosoughi et al. (2018) have shown that Twitter disinformation organically travels faster and further than true information pieces due to technological possibilities, but also due to human nature that is more likely to spread something surprising and emotional, which disinformation often does. On Facebook, on the other hand, the success of spread of disinformation may be significantly attributed to advertising, claim Chiou and Tucker (2018). Accordingly, platforms have put in place different policies towards disinformation. Twitter has recently announced a ban on political advertising, while Facebook continues to run it and exempts politician's speech and political advertising from third-party fact-checking programmes.

Further to different types of disinformation, and different affordances of platforms and their policies, there are "*many different actors involved and we're learning much more about the different tactics that are being used to manipulate the online public sphere, particularly around elections*", warns Susan Morgan (2018, p. 40). Young Mie Kim and others (2018) have investigated the groups that stood behind divisive issue campaigns on Facebook in the weeks before the 2016 US elections, and found that most of these campaigns were run by groups which did not file reports to the Federal Election Commission. These groups, clustered by authors as non-profits, astroturf/movement groups, and unidentifiable "suspicious" groups, have sponsored four times more ads than those that did file the reports to the Commission. In addition to the variety of groups playing a role in political advertising and political communication on social media today, a new set of tactics are emerging, including the use of automated accounts, so-called bots, and data-driven micro-targeting of voters (Morgan, 2018).

Bradshaw and Howard (2018) have found that governments and political parties in an increasing number of countries of different political regimes are investing significant resources in using social media to manipulate public opinion. Political bots, as they note, are used to promote or attack particular politicians, to promote certain topics, to fake a follower base, or to get opponents' accounts and content removed by reporting it on a large scale. Micro-targeting, as another tactic, is commonly defined as a political advertising strategy that makes use of data analytics to build individual or small group voter models and to address them with tailored political messages (Bodó et al., 2017). These messages can be drafted with the intention to deceive certain groups and to influence their behaviour, which is particularly problematic in the

election period when the decisions of high importance for democracy are made, the tensions are high and the time for correction or reaction is scarce.

The main fuel of contemporary political micro-targeting is data gathered from citizens' online presentation and behaviour, including from their social media use. Social media has also been used as a channel for distribution of micro-targeted campaign messages. This political advertising tactic came into the spotlight with the Cambridge Analytica case reported by journalist Carole Cadwalladr in 2018. Her investigation, based on the information from whistleblower Christopher Wylie, revealed that the data analytics firm Cambridge Analytica, which worked with Donald Trump's election team and the winning Brexit campaign, harvested the personal data of millions of peoples' Facebook profiles without their knowledge and consent, and used it for political advertising purposes (Cadwalladr, 2018). In the EU, the role of social media in elections came high on the agenda of political institutions after the Brexit referendum in 2016. The focus has been in particular on the issue of 'fake news' or disinformation. The reform of the EU's data protection rules, which resulted in the GDPR, started in 2012. The Regulation was adopted on 14 April 2016, and its scheduled time of enforcement, 25 May 2018, collided with the outbreak of the Cambridge Analytica case.

PERSPECTIVE AND METHODOLOGY

Although, European elections are primarily the responsibility of national governments, the EU has taken several steps to tackle the issue of online disinformation. In the Communication of 26 April 2018 the EC called these steps a "European approach" (EC, 2018a), with one of its key deliverables being the Code of Practice on Disinformation (2018), presented as a self-regulatory instrument that should encourage proactivity of online platforms in ensuring transparency of political advertising and restricting the automated spread of disinformation. The follow up Commission's Communication from September 2018, focused on securing free and fair European elections (EC, 2018f), suggests that, in the context of elections, principles set out in the European approach for tackling online disinformation (EC, 2018a) should be seen as complementary to the GDPR (Regulation, 2016/679). The Commission also prepared specific guidance on the application of GDPR in the electoral context (EC, 2018d). It further suggested considering the Recommendation on election cooperation networks (EC, 2018e), and transparency of political parties, foundations and campaign organisations on financing and practices (Regulation, 2018, p. 673). This paper provides an analysis of the listed legal and policy instruments that form and complement the EU's approach to tackling disinformation and suspicious tactics of political advertising on online platforms. The Commission's initiatives in the area of combating disinformation contain also a cybersecurity aspect. However, this subject is technically and politically too complex to be included in this specific analysis.

The EC considers online platforms as covering a wide range of activities, but the European approach to tackling disinformation is concerned primarily with "online platforms that distribute content, particularly social media, video-sharing services and search engines" (EC, 2018a). This paper employs the same focus and hence the same narrow definition of online platforms. The main research questions are: which are the key principles upon which the European approach to tackling disinformation and political manipulation builds; and to what extent, if at all, do they differ from the principles of "traditional" political advertising and media campaign regulation in the electoral period? The analysis further seeks to understand how these principles are elaborated and whether they reflect the complexity of the challenges identified. For this purpose, the 'European approach' is understood in a broad sense (EC, 2018f). Looking

through the lens of pluralism, this analysis uses a generic inductive approach, a qualitative research approach that allows findings to emerge from the data without having pre-defined coding categories (Liu, 2016). This methodological decision was made as this exploratory research sought not only to analyse the content of the above listed documents, but also the context in which they came into existence and how they relate to one another.

TWO BIRDS WITH ONE STONE: THE EUROPEAN APPROACH IN CREATING FAIR AND PLURAL CAMPAIGNING ONLINE

The actions currently contained in the EU's approach to tackling online disinformation and political manipulation derive from the regulation (GDPR), EC-initiated self-regulation of platforms (Code of Practice on Disinformation), and the non-binding Commission's communications and recommendations to the member states. While some of the measures, such as data protection, have a long tradition and have only been evolving, some represent a new attempt to develop solutions to the problem of platforms (self-regulation). In general, the current European approach can be seen as primarily designed towards (i) preventing unlawful micro-targeting of voters by protecting personal data; and (ii) combating disinformation by increasing the transparency of political and issue-based advertising on online platforms.

PROTECTING PERSONAL DATA

The elections of May 2019 were the first European Parliament (EP) elections after major concerns about legality and legitimacy of the vote in US presidential election and the UK's Brexit referendum. The May 2019 elections were also the first elections for the EP held under the GDPR, which became directly applicable across the EU as of 25 May 2018. As a regulation, the GDPR is directly binding, but does provide flexibility for certain aspects of the regulation to be adjusted by individual member states. For example, to balance the right to data protection with the right to freedom of expression, article 85 of the GDPR provides for the exemption of, or derogation for, the processing of data for "journalistic purposes or the purpose of academic artistic or literary expression", which should be clearly defined by each member state. While the GDPR provides the tools necessary to address instances of unlawful use of personal data, including in the electoral context, its scope is still not fully and properly understood. Since it was the very first time the GDPR was applied in the European electoral context, the European Commission published in September 2018 the Guidance on the application of Union data protection law in the electoral context (EC, 2018d).

The data protection regime in the EU is not new, [3] even though it has not been well harmonised and the data protection authorities (DPAs) have had limited enforcement powers. The GDPR aims to address these shortcomings as it gives DPAs powers to investigate, to correct behaviour and to impose fines up to 20 million Euros or, in the case of a company, up to 4% of its worldwide turnover. In its Communication, the EC (2018d) particularly emphasises the strengthened powers of authorities and calls them to use these sanctioning powers especially in cases of infringement in the electoral context. This is an important shift as the European DPAs have historically been very reluctant to regulate political parties. The GDPR further aims at achieving cooperation and harmonisation of the Regulation's interpretations between the national DPAs by establishing the European Data Protection Board (EDPB). The EDPB is made up of the heads of national data protection authorities and of the European Data Protection

Supervisor (EDPS) or their representatives. The role of the EDPS is to ensure that EU institutions and bodies respect people's right to privacy when processing their personal data. In March 2018, the EDPS published an Opinion on online manipulation and personal data, confirming the growing impact of micro-targeting in the electoral context and a significant shortfall in transparency and provision of fair processing of information (EDPS, 2019).

The Commission guidance on the application of GDPR in the electoral context (EC, 2018d) underlines that it "applies to all actors active in the electoral context", including European and national political parties, European and national political foundations, platforms, data analytics companies and public authorities responsible for the electoral process. Any data processing should comply with the GDPR principles such as fairness and transparency, and for specified purposes only. The guidance provides relevant actors with the additional explanation of the notions of "personal data" and of "sensitive data", be it collected or inferred. Sensitive data may include political opinions, ethnic origin, sexual orientation and similar, and the processing of such data is generally prohibited unless one of the specific justifications provided for by the GDPR applies. This can be in the case where the data subject has given explicit, specific, fully informed consent for processing; when this information is manifestly made public by the data subject; when the data relate to "the members or to former members of the body or to persons who have regular contact with"; or when processing "is necessary for reasons of substantial public interest" (GDPR, Art. 9, para. 2). In a statement adopted in March 2019, the EDPB points out that derogations of special data categories should be interpreted narrowly. In particular, the derogation in the case when a person makes his or her 'political opinion' public cannot be used to legitimate inferred data. Bennett (2016) also warns that vagueness of several terms used to describe exceptions from the application of Article 9(1) might lead to confusion or inconsistencies in interpretation as processing of 'political opinions' becomes increasingly relevant for contemporary political campaigning.

The principles of fairness and transparency require that individuals (data subjects) are informed of the existence of the processing operation and its purposes (GDPR, Art. 5). The Commission's guidance clearly states that data controllers (those who make the decision on and the purpose of processing, like political parties or foundations) have to inform individuals about key aspects related to the processing of their personal data, including why they receive personalised messages from different organisations; which is the source of the data when not collected directly from the person; how are data from different sources combined and used; and whether the automated decision-making has been applied in processing.

Despite the strengthened powers and an explicit call to act more in the political realm (EC, 2018d), to date we have not seen many investigations by DPAs into political parties under the GDPR. An exception is UK Information Commissioner Elizabeth Denham. In May 2017, she announced the launch of a formal investigation into the use of data analytics for political purposes following the wrongdoings exposed by journalists, in particular Carole Cadwalladr, during the EU Referendum, and involving parties, platforms and data analytics companies such as Cambridge Analytica. The report of November 2018 concludes:

> that there are risks in relation to the processing of personal data by many political parties. Particular concerns include the purchasing of marketing lists and lifestyle information from data brokers without sufficient due diligence, a lack of fair processing and the use of third-party data analytics companies, with insufficient checks around consent (ICO, 2018a, p. 8).

As a result of the investigation, the ICO sent 11 letters to the parties with formal warnings about their practices, and in general it became the largest investigation conducted by a DPA on this matter and encompassing different actors, not only political parties but also social media platforms, data brokers and analytics companies.

Several cases have been reported where the national adaptation of the GDPR does not fully meet the requirements of recital 56 GDPR which establishes that personal data on people's political opinions may be processed "for reasons of public interest" if "the operation of the democratic system in a member state requires that political parties compile" such personal data; and "provided that appropriate safeguards are established". In November 2018 a question was raised in the European Parliament on the data protection law adapting Spanish legislation to the GDPR which allows "political parties to use citizens' personal data that has been obtained from web pages and other publicly accessible sources when conducting political activities during election campaigns". As a member of the European Parliament Sophia in 't Veld, who posed the question, highlighted: "Citizens can opt out if they do not wish their data to be processed. However, even if citizens do object to receiving political messages, they could still be profiled on the basis of their political opinions, philosophical beliefs or other special categories of personal data that fall under the GDPR". The European Commission was also urged to investigate the Romanian GDPR implementation for similar concerns. Further to the reported challenges with national adaptation of GDPR, in November 2019 the EDPS has issued the first ever reprimand to an EU institution. The ongoing investigation into the European Parliament was prompted by the Parliament's use of a US-based political campaigning company NationBuilder to process personal data as part of its activities relating to the 2019 EU elections.

COMBATING DISINFORMATION

In contrast to the GDPR, which is sometimes praised as "the most consequential regulatory development in information policy in a generation" (Hoofnagle et al., 2019, p. 66), the EC has decided to tackle fake news and disinformation through self-regulation, at least in the first round. The European Council, a body composed of the leaders of the EU member states, first recognised the threat of online disinformation campaigns in 2015 when it asked the High Representative of the Union for Foreign Affairs and Security Policy to address the disinformation campaigns by Russia (EC, 2018c). The Council is not one of the EU's legislating institutions, but it defines the Union's overall political direction and priorities. So, it comes as no surprise that the issue of disinformation came high on the agenda of the EU, in particular after the UK referendum and US presidential elections in 2016. In April 2018 the EC (2018a) adopted a Communication on Tackling online disinformation: a Europen Approach. This is the central document that set the tone for future actions in this field. In the process of its drafting, the EC carried out consultations with experts and stakeholders, and used citizens' opinions gathered through polling. The consultations included the establishment of a High-Level Expert Group on Fake News and Online Disinformation (HLEG) in early 2018, which two months later produced a Report (HLEG, 2018) advising the EC against simplistic solutions. Broader public consultations and dialogues with relevant stakeholders were also held, and the specific Eurobarometer (2018b) poll was conducted via telephone interviews in all EU member states. The findings indicated a high level of concern among the respondents for the spread of online disinformation in their country (85%) and saw it as a risk for democracy in general (83%). This urged the EC to act and the Communication on tackling online disinformation was a starting point and the key document in understanding the European approach to the pressing challenges. The Communication builds around four overarching principles and objectives: transparency, diversity of information, credibility of information, and cooperation (EC, 2018a).

Transparency, in this view, means that it should be clear to users where the information comes from, who the author is and why they see certain content when an automated recommendation system is being employed. Furthermore, a clearer distinction between sponsored and informative content should be made and it should be clearly indicated who paid for the advertisement. The diversity principle is strongly related to strengthening so-called quality journalism, [4] to rebalancing the disproportionate power relations between media and social media platforms, and to increasing media literacy levels. The credibility, according to the EC, is to be achieved by entrusting platforms to design and implement a system that would provide an indication of the source and information trustworthiness. The fourth principle emphasises cooperation between authorities at national and transnational level and cooperation of broad stakeholders in proposing solutions to the emerging challenges. With an exception of emphasising media literacy and promoting cooperation networks of authorities, the Communication largely recommends that platforms design solutions which would reduce the reach of manipulative content and disinformation, and increase the visibility of trustworthy, diverse and credible content.

The key output of this Communication is a self-regulatory Code of Practice on Online Disinformation (CoP). The document was drafted by the working group composed of online platforms, advertisers and the advertising industry, and was reviewed by the Sounding Board, composed of academics, media and civil society organisations. The CoP was agreed by the online platforms Facebook, Google and Twitter, Mozilla, and by advertisers and the advertising industry, and was presented to the EC in October 2018. The Sounding Board (2018), however, presented a critical view on its content and the commitments laid out by the platforms, stating that it "*contains no clear and meaningful commitments, no measurable objectives*" and "*no compliance or enforcement tool*". The CoP, as explained by the Commission, represents a transitional measure where private actors are entrusted to increase transparency and credibility of the online information environment. Depending on the evaluation of their performance in the first 12 months, the EC is supposed to determine the further steps, including the possibility of self-regulation being replaced with regulation (EC, 2018c). The overall assessment of the Code's effectiveness is expected to be presented in early 2020.

The CoP builds on the principles expressed in the Commission's Communication (2018a) through the actions listed in Table 1. For the purpose of this paper the actions are not presented in the same way as in the CoP. THey are instead slightly reorganised under the following three categories: Disinformation; Political advertising, Issue-based advertising.

Table 1: Commitments of the signatories of the Code of Practice on Online Disinformation selected and grouped under three categories: disinformation, political advertising, issue-based advertising. Source: composed by the author based on the Code of Practice on Online Disinformation

Disinformation	Political advertising	Issue-based advertising
To disrupt advertising and monetisation incentives for accounts and websites which consistently misrepresent information about themselves	To clearly label paid-for communication as such	

Disinformation	Political advertising	Issue-based advertising
Limiting the abuse of platforms by unauthentic users (misuse of automated bots)	To publicly disclose political advertising, including actual sponsor and amounts spent	To publicly disclose, conditioned to developing a working definition of "issue-based advertising" which does not limit freedom of expression and excludes commercial advertising
Implementing rating systems (on trustworthiness), and report system (on false content)	Enabling users to understand why they have been targeted by a given advertisement	
To invest in technology to prioritise "relevant, authentic and authoritative information" in search, feeds and other ranked channels		
Resources for users on how to recognise and limit the spread of false news		

In the statement on the first annual self-assessment reports by the signatories of the CoP, the Commission acknowledged that some progress has been achieved, but warns that it "*varies a lot between signatories and the reports provide little insight on the actual impact of the self-regulatory measures taken over the past year as well as mechanisms for independent scrutiny*". The European Regulators Group for Audiovisual Media Services (ERGA) has been supporting the EC in monitoring the implementation of the commitments made by Google, Facebook and Twitter under the CoP, particularly in the area of political and issue-based advertising. In June 2019 ERGA released an interim Report as a result of the monitoring activities carried out in 13 EU countries, based on the information reported by platforms and on the data available in their online archives of political advertising. While it stated "that Google, Twitter and Facebook made evident progress in the implementation of the Code's commitments by creating an ad hoc procedure for the identification of political ads and of their sponsors and by making their online repository of relevant ads publicly available", it also emphasised that the platforms have not met a request to provide access to the overall database of advertising for the monitored period, which "was a significant constraint on the monitoring process and emerging conclusions" (ERGA, 2019, p. 3). Furthermore, based on the analysis of the information provided in the platforms' repositories of political advertising (e.g., Ad Library), the information was "not complete and that not all the political advertising carried on the platforms was correctly labelled as such" (ERGA, 2019, p. 3).

The EC still needs to provide a comprehensive assessment on the implementation of the commitments under the CoP after an initial 12-month period. However, it is already clear that the issue of the lack of transparency of the platforms' internal operations and decision-making processes remains and represents a risk. If platforms are not amenable to thorough public auditing, then the adequate assessment of the effectiveness of implementation when it comes to self-regulation becomes impossible. The ERGA Report (2019) further warns that at this point it is not clear what options for micro-targeting were offered to political advertisements nor if all options are disclosed in the publicly available repositories of political advertising.

Further to the commitments laid down in the CoP and relying on social media platforms to

increase transparency of political advertising online, the Commission Recommendation of 9 September 2018 (EC, 2018e), "encourages", and asks member states to "encourage" further transparency commitments by European and national political parties and foundations, in particular:

> information on the political party, political campaign or political support group behind paid online political advertisements and communications" [...] "information on any targeting criteria used in the dissemination of such advertisements and communications" [...] "make available on their websites information on their expenditure for online activities, including paid online political advertisements and communications (EC, 2018e, p. 8).

The Recommendation (EC, 2018e) further advises member states to set up a national election network, involving national authorities with competence for electoral matters, including data protection commissioners, electoral authorities and audio-visual media regulators. This recommendation is further elaborated in the Action plan (EC, 2018c) but, because of practical obstacles, national cooperation between authorities has not yet become a reality in many EU countries.

KEY PRINCIPLES AND SHORTCOMINGS OF THE EUROPEAN APPROACH

This analysis has shown that the principles contained in the above mentioned instruments, which form the basis of the European approach to combating disinformation and political manipulation are: data protection; transparency; cooperation; mobilising the private sector; promoting diversity and credibility of information; raising awareness; empowering the research community.

Data protection and transparency principles related to personal data collection, processing and use are contained in the GDPR. The requirement to increase transparency of political and issues-based advertising and of automated communication is currently directed primarily towards platforms that have committed themselves to label and publicly disclose sponsors and content of political and issues-based advertising, as well as to identify and label automated accounts. Unlike with the traditional media landscapes where, in general, on the same territory, media were broadcasting the same political advertising and messages to their audiences, in the digital information environment political messages are being targeted and shown only to specific profiles of voters with limited ability to track them to see which messages were targeted to whom. To increase transparency on this level would require platforms to provide a user-friendly repository of political ads, including searchable information on actual sponsors and amounts spent. At the moment, they struggle with how to identify political and issue-based ads, to distinguish them from other types of advertising, and to verify ad buyers' identities (Leerssen et al., 2019).

Furthermore, the European approach fails to impose similar transparency requirements towards political parties to provide searchable and easy to navigate repositories of the campaign materials used. The research project of campaign monitoring during the 2019 European elections, showed that parties/groups/candidates participating in the elections were largely not

transparent about their campaign materials. Materials were not readily available on their websites or social media accounts nor did they respond to direct requests from researchers (Simunjak et al., 2019). This warns that while it is relevant to require platforms to provide more transparency on political advertising, it is perhaps even more relevant to demand this transparency directly from political parties and candidates in elections.

In the framework of transparency, the European approach also fails to further emphasise the need for political parties to declare officially to authorities and under a specific category the amounts spent for digital (including social media) campaigning. At present, in some EU countries (for example Croatia, see: Klaric, 2019), authorities with competences in electoral matters do not consider social media as media and accordingly do not apply the requirements to report spending on social media and other digital platforms in a transparent manner. This represents a risk, as the monitoring of the latest EP elections has clearly showed that the parties had spent both extensive time and resources on their social media accounts (Novelli & Johansson, 2019).

The diversity and credibility principles stipulated in the Communication on tackling online disinformation and in the Action plan ask from platforms to indicate the information trustworthiness, to label automated accounts, to close down fake accounts, and to prioritise quality journalism. At the same time, clear definition or instructions on criteria to determine whether an information or a source is trustworthy and whether it represents quality journalism is not provided. Entrusting platforms with making these choices without the possibility of auditing their algorithms and decision-making processes represents a potential risk for freedom of expression.

The signatories of the CoP have committed themselves to disrupt advertising and monetisation incentives for accounts and websites, which consistently misrepresent information about themselves. But, what about accounts that provide accurate information about themselves but occasionally engage in campaigns which might also contain disinformation? For example, a political party may use data to profile and target individual voters or a small group of voters with messages that are not completely false but are exaggerated, taken out of context or framed with an intention to deceive and influence voters' behaviour. As already noted, disinformation comes in many different forms, including false context, imposter, manipulated or fabricated content (Wardle & Derakhshan, 2017). While the work of fact-checkers and flagging of false content are not completely useless here, in the current state of play this is far from sufficient to tackle the problems of disinformation, including in political advertising and especially of dark ads [5]. The efficiency of online micro-targeting depends largely on data and profiling. Therefore, if effectively implemented, the GDPR should be of use here by preventing the unlawful processing of personal data.

Another important aspect of the European approach are stronger sanctions in cases when the rules are not respected. This entails increased powers of authorities, first and foremost of DPAs and increased fines under the GDPR. Data protection in the electoral context is difficult to ensure if the cooperation between different authorities with competence for electoral matters (such as data protection commissioners, electoral authorities and audio-visual media regulators) is not established and operational. While the European approach strongly recommends cooperation, it is not easily achievable at a member state level, as it requires significant investments in capacity building and providing channels for cooperation. In some cases, it may even require amendments to the legislative framework. The cooperation of regulators of the same type at the EU level is sometimes hampered by the fact that their competences differ in

different member states.

The CoP also contains a commitment on "empowering the research community". This means that the CoP signatories commit themselves to support research on disinformation and political advertising by providing researchers access to data sets, or collaborating with academics and civil society organisations in other ways. However, the CoP does not specify how this cooperation should work, the procedures for granting access and for what kind of data, or which measures should researchers put in place to ensure appropriate data storage, security and protection. In the reflection on the platform's progress under the Code, three Commissioners warned that the "*access to data provided so far still does not correspond to the needs of independent researchers*".

CONCLUSIONS

This paper has given an overview of the developing European approach to combating disinformation and political manipulation during an electoral period. It provided an analysis of the key instruments contained in the approach and drew out the key principles upon which it builds: data protection; transparency; cooperation; mobilising the private sector; promoting diversity and credibility of information; raising awareness; empowering the research community.

The principles of legacy media regulation in the electoral period are impartiality and equality of opportunity for contenders. This entails balanced and non-partisan reporting as well as equal or proportionate access to media for political parties (be it free or paid-for). If political advertising is allowed, it is usually subject to transparency and equal conditions requirements: how much was spent on advertising in the campaign needs to be presented through spending on different types of media and reported to the competent authorities. The regulatory framework requires that political advertising be properly labelled as such.

In the online environment, the principles applied to legacy media require further elaboration as the problem of electoral disinformation cuts across a number of different policy areas, involving a range of public and private actors. Political disinformation is not a problem that can easily be compartmentalised into existing legal and policy categories. It is a complex and multi-layered issue that requires a more comprehensive and collaborative approach when designing potential solutions. The emerging EU approach reflects the necessity for that overall policy coordination.

The main fuel of online political campaigning is data. Therefore, the protection of personal data and especially of "sensitive" data from abuse becomes a priority of any action that aims to ensure free, fair and plural elections. The European approach further highlights the importance of transparency. It calls on platforms to clearly identify political advertisements and who paid for them, but it fails to emphasise the importance of having a repository of all the material used in the campaign provided by candidates and political parties. Furthermore, a stronger requirement for political parties to report on the amounts spent on different types of communication channels (including legacy, digital and social media) is lacking in this approach, as well as the requirement for platforms to provide more comprehensive and workable data on sponsors and spending in political advertising.

The European Commission's communication of the European approach claims that it aims to address all actors active in the electoral context, including European and national political

parties and foundations, online platforms, data analytics companies and public authorities responsible for the electoral process. However, it seems that the current focus is primarily on the platforms and in a way that enables them to shape the future direction of actions in the fight against disinformation and political manipulation.

As regards the principle of cooperation, many obstacles, such as differences in competences and capacities of the relevant national authorities, have not been fully taken into account. The elections are primarily a national matter so the protection of the electoral process, as well as the protection of media pluralism, falls primarily within the competence of member states. Yet, if the approach to tackling disinformation and political manipulation is to be truly European, there should be more harmonisation between authorities and approaches taken at national levels.

While being a significant step in the creation of a common EU answer to the challenges of disinformation and political manipulation, especially during elections, the European approach requires further elaboration, primarily to include additional layers of transparency. This entails transparency of political parties and of other actors on their actions in the election campaigns, as well as more transparency about internal processes and decision-making by platforms especially on actions of relevance to pluralism, elections and democracy. Furthermore, the attempt to propose solutions and relevant actions at the European level faces two constraints. On the one hand, it faces the power of global platforms shaped in the US tradition, which to a significant extent differs from the European approach in balancing freedom of expression and data protection. On the other hand, the EU approach confronts the resilience of national political traditions in member states, in particular if the measures are based on recommendations and other soft instruments.

REFERENCES

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. J*ournal of Economic Perspectives, 31*(2), 211–236. https://doi.org/10.1257/jep.31.2.211

Bennett, C. J. (2016). Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America? *International Data Privacy Law*, *6*(4), 261–275. https://doi.org/10.1093/idpl/ipw021

Bodó, B., Helberger, N. & de Vreese, C. H. (2017). Political micro-targeting: a Manchurian candidate or just a dark horse?. *Internet Policy Review*, 6(4). https://doi.org/10.14763/2017.4.776

Bradshaw, S. & Howard, P. N. (2018). *Challenging Truth and Trust: A Global Inventory of Organised Social Media Manipulation* [Report]. Computational Propaganda Research Project, Oxford Internet Institute. Retrieved from https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Brett, W. (2016). It's Good to Talk: Doing Referendums Differently. The Electoral Reform Society's report. Retrieved from https://www.electoral-reform.org.uk/wp-content/uploads/2017/06/2016-EU-Referendum-its-good-to-talk.pdf

Brogi, E., Nenadic, I., Parcu, P. L., & Viola de Azevedo Cunha, M. (2018). *Monitoring Media Pluralism in Europe: Application of the Media Pluralism Monitor 2017 in the European Union, FYROM, Serbia and Turkey* [Report]. Centre for Media Pluralism and Media Freedom, European University Institute. Retrieved from https://cmpf.eui.eu/wp-content/uploads/2018/12/Media-Pluralism-Monitor_CMPF-report_MPM2017_A.pdf

Bruns, A. (2017, September 15). *Echo chamber? What echo chamber? Reviewing the evidence.* 6th Biennial Future of Journalism Conference (FOJ17), Cardiff, UK. Retrieved from https://eprints.qut.edu.au/113937/1/Echo%20Chamber.pdf

Cadwalladr, C. & Graham-Harrison, E. (2018, March 17) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Chiou, L. & Tucker, C. E. (2018). *Fake News and Advertising on Social Media: A Study of the Anti-Vaccination Movement* [Working Paper No. 25223]. Cambridge, MA: The National Bureau of Economic Research. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3209929 https://doi.org/10.3386/w25223

Centre for Media Pluralism and Media Freedom (CMPF). (forthcoming, 2020). *Independent Study on Indicators to Assess Risks to Information Pluralism in the Digital Age*. Florence: Media Pluralism Monitor Project.

Code of Practice on Disinformation (September 2018). Retrieved from https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

Council Decision (EU, Euratom) 2018/994 of 13 July 2018 amending the Act concerning the election of the members of the European Parliament by direct universal suffrage, annexed to

Council Decision 76/787/ECSC, EEC, Euratom of 20 September 1976. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018D0994&qid=1531826494620

Commission Recommendation (EU) 2018/234 of 14 February 2018 on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament (OJ L 45, 17.2.2018, p. 40)

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) (OJ L 201, 31.7.2002, p. 37)

Dubois, E., & Blank, G. (2018). The echo chamber is overstated: the moderating effect of political interest and diverse media. *Information, Communication & Society*, *21*(5), 729–745. https://doi.org/10.1080/1369118X.2018.1428656

Eurobarometer (2018a). *Standard 90: Media use in the EU*. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2215

Eurobarometer (2018b). *Flash 464: Fake news and disinformation online*. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183

Eurobarometer (2017). *Standard 88:. Media use in the EU*. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2143

European Commission (EC). (2018a). *Tackling online disinformation: a European Approach*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM/2018/236. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN

European Commission (EC). (2018b). *Free and fair European elections – Factsheet, State of the Union*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681

European Commission (EC). (2018c, December 5). *Action Plan against Disinformation. European Commission contribution to the European Council* (5 December). Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf

European Commission (EC). (2018d, September 12). 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. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf

European Commission (EC). (2018e, September 12). Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting

disinformation campaigns in the context of elections to the European Parliament. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

European Commission (EC). (2018f). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Securing free and fair European elections. COM(2018)637. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-free-fair-elections-communication-637_en.pdf

European Commission (EC). (2007). *Media pluralism in the Member States of the European Union* [Commission Staff Working Document No. SEC(2007)32]. Retrieved from https://ec.europa.eu/information_society/media_taskforce/doc/pluralism/media_pluralism_swp_en.pdf

European Data Protection Board (EDPB). (2019). Statement 2/2019 on the use of personal data in the course of political campaigns. Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/ostalo/statement-22019-use-personal-data-course-political-campaigns_en

European Data Protection Supervisor (EDPS). (2018). Opinion 372018 on online manipulation and personal data. Retrieved from https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

European Regulators Group for Audiovisual Media Services (ERGA). (2019, June). *Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation* [Report]. Slovakia: European Regulators Group for Audiovisual Media Services. Retrieved from http://erga-online.eu/wp-content/uploads/2019/06/ERGA-2019-06_Report-intermediate-monitoring-Code-of-Practice-on-disinformation.pdf?fbclid=IwAR1BZV2xYlJv9nOzYAghxA8AA5q70vYx0VUNnh080WvDD2BfFfWFM3js4wg

Fletcher, R., Cornia, A., Graves, L., & Nielsen, R. K. (2018). Measuring the reach of "fake news" and online disinformation in Europe. Retrieved from https://www.press.is/static/files/frettamyndir/reuterfake.pdf

Flew, T., Martin, F., Suzor, N. P. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media and Policy*, *10*(1), 33–50. https://doi.org/10.1386/jdtv.10.1.33_1

Guess, A., Nyhan, B., & Reifler, J. (2018). *Selective exposure to misinformation: evidence from the consumption of fake news during the 2016 US presidential campaign* [Working Paper]. Retrieved from https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf

High Level Expert Group on Fake News and Online Disinformation (HLEG). (2018). *Final report* [Report]. Retrieved from https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

Hoofnagle, C.J. & van der Sloot, B., & Zuiderveen Borgesius, F. J. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98.

https://doi.org/10.1080/13600834.2019.1573501

Holtz-Bacha, C. & Just, M. R. (Eds.). (2018). *Routledge Handbook of Political Advertising*. New York: Routledge.

House of Commons Treasury Committee. (2016, May 27). The economic and financial costs and benefits of the UK's EU membership. First Report of Session 2016–17. Retrieved from https://publications.parliament.uk/pa/cm201617/cmselect/cmtreasy/122/122.pdf

Howard, P. N. & Kollanyi, B. (2016). Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum. *ArXiv160606356 Phys*. Retrieved from https://arxiv.org/abs/1606.06356

Information Commissioner's Office (ICO). (2018a, July 11). *Investigation into the use of data analytics in political campaigns* [Report to Parliament]. Retrieved from https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

Information Commissioner's Office (ICO). (2018b, July 11). Democracy disrupted? Personal information and political influence. Retrieved from https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

Kim, Y. M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S. Y., Heinrich, R., Baragwanath, R., & Raskutti, G. (2018). The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook. *Political Communication*, *35*(4), 515–541. https://doi.org/10.1080/10584609.2018.1476425

Kelley, S. Jr. (1962). Elections and the Mass Media. *Law and Contemporary Problems*, *27*(2), 307–326. Retrieved from https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2926&context=lcp

Klaric, J. (2019, March 28) Ovo je Hrvatska 2019.: za Državno izborno povjerenstvo teletekst je medij, Facebook nije. *Telegram*. Retrieved from https://www.telegram.hr/politika-kriminal/ovo-je-hrvatska-2019-za-drzavno-izborno-povjerenstvo-teletekst-je-medij-facebook-nije/

Kreiss, D. l., & McGregor, S. C. (2018). Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google with Campaigns During the 2016 U.S. Presidential Cycle. *Political Communication*, *35*(2), 155–177. https://doi.org/10.1080/10584609.2017.1364814

Valcke, P., Lefever, K., Kerremans, R., Kuczerawy, A., Sükosd, M., Gálik, M., … Füg, O. (2009). *Independent Study on Indicators for Media Pluralism in the Member States – Towards a Risk-Based Approach* [Report]. ICRI, K.U. Leuven; CMCS, Central European University, MMTC, Jönköping Business School; Ernst & Young Consultancy Belgium. Retrieved from https://ec.europa.eu/information_society/media_taskforce/doc/pluralism/pfr_report.pdf

Kumar, S., & Shah, N. (2018, April). False information on web and social media: A survey. *arXiv:1804.08559 [cs]*. Retrieved from https://arxiv.org/pdf/1804.08559.pdf

Leerssen, P., Ausloos, J., Zarouali, B., Helberger, N., & de Vreese, C. H. (2019). Platform ad archives: promises and pitfalls. *Internet Policy Review*, *8*(4).

https://doi.org/10.14763/2019.4.1421

Liu, L. (2016). Using Generic Inductive Approach in Qualitative Educational Research: A Case Study Analysis. *Journal of Education and Learning*, *5*(2), 129–135. https://doi.org/10.5539/jel.v5n2p129

Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*, *3*(1), 39–43. https://doi.org/10.1080/23738871.2018.1462395

Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D. A. L., & Nielsen, R. K. (2018). *Digital News Report 2018*. Oxford: Reuters Institute for the Study of Journalism. Retrieved from https://reutersinstitute.politics.ox.ac.uk/sites/default/files/digital-news-report-2018.pdf

Novelli, E. & Johansson, B. (Eds.) (2019). *2019 European Elections Campaign: Images,Topics, Media in the 28 Member States* [Research Report]. Directorate-General of Communication of the European Parliament. Retrieved from https://op.europa.eu/hr/publication-detail/-/publication/e6767a95-a386-11e9-9d01-01aa75ed71a1/language-en?fbclid=IwAR0C9R6MwoGd5aggB7wZx6KGWt3is84M21oq3rvog9LbXJqJpXuha1H6yeQ

Regulation (EU, Euratom). 2018/673 amending Regulation (EU, Euratom) No 1141/2014 on the statute and funding of European political parties and European political foundations. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0673

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) (OJ L 119, 4.5.2016, p. 1)

Regulation (EU, Euratom). No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations, (OJ L 317, 4.11.2014, p.1).

Report of the Special Rapporteur to the General Assembly on online hate speech. (2019). (A/74/486). Retrieved from https://www.ohchr.org/Documents/Issues/Opinion/A_74_486.pdf

Report of the Special Rapporteur to the Human Rights Council on online content regulation. (2018). (A/HRC/38/35). Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement

Schoenbach, K., & Lauf, E. (2004). Another Look at the 'Trap' Effect of Television—and Beyond. *International Journal of Public Opinion Research*, *16*(2), 169–182. https://doi.org/10.1093/ijpor/16.2.169

Shearer, E. (2018, December 10). Social media outpaces print newspapers in the U.S. as a news source. *Pew Research Center*. Retrieved from https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/

Šimunjak, M., Nenadić, I., & Žuvela, L. (2019). National report: Croatia. In E. Novelli & B. Johansson (Eds.), *2019 European Elections Campaign: Images, topics, media in the 28 Member States* (pp. 59–66). Brussels: European Parliament.

Sounding Board. (2018). The Sounding Board's Unanimous Final Opinion on the so-called Code of Practice on 24 September 2018. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

The Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression. (2019). *How governments and platforms have fallen short in trying to moderate content online* (Co-Chairs Report No. 1 and Working Papers). Retrieved from https://www.ivir.nl/publicaties/download/TWG_Ditchley_intro_and_papers_June_2019.pdf

Valeriani, A., & Vaccari, C. (2016). Accidental exposure to politics on social media as online participation equalizer in Germany, Italy, and the United Kingdom. *New Media & Society*, *18*(9). https://doi.org/10.1177/1461444815616223

Venice Commission. (2013). CDL-AD(2013)021 Opinion on the electoral legislation of Mexico, adopted by the Council for Democratic Elections at its 45th meeting (Venice, 13 June 2013) and by the Venice Commission at its 95th Plenary Session (Venice, 14-15 June 2013).

Venice Commission. (2010). CDL-AD(2010)024 Guidelines on political party regulation, by the OSCE/ODIHR and the Venice Commission, adopted by the Venice Commission at its 84th Plenary Session (Venice, 15-16 October 2010).

Venice Commission. (2009). CDL-AD(2009)031 Guidelines on media analysis during election observation missions, by the OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR) and the Venice Commission, adopted by the Council for Democratic Elections at its 29th meeting (Venice, 11 June 2009) and the Venice Commission at its 79th Plenary Session (Venice, 12- 13 June 2009).

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Wakefield, J. (2019, February 18). Facebook needs regulation as Zuckerberg 'fails' - UK MPs. *BBC*. Retrieved from https://www.bbc.com/news/technology-47255380

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* [Report No. DGI(2017)09]. Strasbourg: Council of Europe. Retrieved from https://firstdraftnews.org/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-de%CC%81sinformation-1.pdf?x56713

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S. Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., de Vreese, C. H. (2018). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review*, *14*(1), 82–96. https://doi.org/10.18352/ulr.420

FOOTNOTES

1. The so-called 'fake news' law was passed in May 2019 allowing ministers to issue orders to platforms like Facebook to put up warnings next to disputed posts or, in extreme cases, to take the content down. The law also allows for fines of up to SG$ 1 million (665,000 €) for companies that fail to comply, and the individual offenders could face up to ten years in prison. Many have raised the voice against this law, including the International Political Science Association (IPSA), but it came into effect and is being used.

2. To which the author is affiliated.

3. The GDPR supplanted the Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (PII (US)) and on the free movement of such data).

4. The Council of Europe also uses the term 'quality journalism' but it is not fully clear what is entailed in 'quality' and who decides on what 'quality journalism' is, and what is not. The aim could be (and most likely is) to distinguish journalism that respects professional standards from less reliable, less structured and less ethical and professional standards bound forms of content production and delivery. Many argue that journalism already entails the request for quality so this attribute adjective is not necessary and, in fact, may be problematic.

5. Dark advertising is a type of online advertising visible only to the advert's publisher and the intended target group.