Strasbourg, 24 June 2019 **CDL-AD(2019)016**

Opinion No. 925 / 2018 Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

JOINT REPORT

OF THE VENICE COMMISSION

AND OF THE DIRECTORATE OF INFORMATION SOCIETY AND ACTION AGAINST CRIME OF THE DIRECTORATE GENERAL OF HUMAN RIGHTS AND RULE OF LAW (DGI)

ON DIGITAL TECHNOLOGIES AND ELECTIONS

Adopted by the Council of Democratic Elections
at its 65th meeting
(Venice, 20 June 2019)

Adopted by the Venice Commission
at its 119th Plenary Session
(Venice, 21-22 June 2019)

On the basis of comments by

Mr Richard BARRETT (Member, Ireland)
Ms Herdís KJERULF THORGEIRSDOTTIR
(Member, Iceland)
Mr Rafael RUBIO NUÑEZ (Substitute Member, Spain)
Mr José Luis VARGAS VALDEZ (Substitute Member, Mexico)
Ms Krisztina ROZGONYI
(DGI Expert, Media and Internet Governance Division)
Ms Nevena RUZIC (DGI Expert, Data Protection Division)

Table of Contents

I. Introduction

1. At its 59th meeting (15 June 2017), the Council for Democratic Elections, upon an initiative by Mr José Luis Vargas Valdez and on the basis of his "Study on the role of social media and the internet in democratic development" (CDL-LA(2018)001), decided to undertake a study on the use of digital technologies during electoral processes, jointly with the Council of Europe's Information Society Department.

2. In addition to Mr Vargas Valdez, Ms Herdis Kjerulf Thorgeirsdóttir, Mr Richard Barrett and Mr Rafael Rubio Nuñez acted as rapporteurs. Ms Krisztina Rozgonyi and Ms Nevena Ružić acted as experts on behalf of the Information Society and Action against Crime Directorate, Media and Internet Governance Division and of the Data Protection Division respectively. Mr Alexander Seger, head of the Cybercrime Division, also contributed to the relevant parts of this joint report.

3. This joint report was prepared on the basis of Mr Vargas Valdez's original study and of the comments submitted by the rapporteurs and experts above; it was examined at the meeting of the Sub-Commission on Latin America on 30 November 2018, adopted by the Council for Democratic Elections at its 65th meeting (Venice, 20 June 2019) and subsequently adopted by the Venice Commission at its 119th plenary session (Venice, 21-22 June 2019).

II. Background

4. Digital (or "new") technologies and social media – the latter being understood as "internet platforms that allow for bidirectional interaction through users-generated content"[1] – have revolutionised the way people interact and exercise their freedom of expression and information, as well as other related - and sometimes conflicting - fundamental rights.[2] People who engage in social media may use the internet to organise and demand better services, more transparency and meaningful participation in the political arena.[3] Individuals all over the globe are now able to shape global perceptions, position topics in their national agendas and foster political activism.[4] This digital transformation is recasting the relation between states and citizens.

5. According to the Global Digital Report 2018, more than half of the world's web traffic now comes from mobile phones. From a total of 7.6 billion inhabitants of the world, roughly 4 billion are internet users (which represents 53% of the total population), and 3.2 billion are social media active users (which represents 42% of the total population).

6. Between 2017 and 2018, the number of internet users increased by 7% and active social media users increased by 13%. The average internet user spends around 6 hours online each

[1] This study adopts a definition of social media as "web or mobile-based platforms that allow for two-way interactions through user-generated content (UGC) and communication. Social media are therefore not media that originate only from one source or are broadcast from a static website. Rather, they are media on specific platforms designed to allow users to create ('generate') content and to interact with the information and its source (International IDEA 2014: 11). While social media rely on the internet as a medium, it is important to note that not all internet sites or platforms meet the definition of social media. Some websites make no provision for interactivity with the audience, while others allow users only to post comments as a reaction to particular published content as discussions posts (or 'threads') which are moderated and controlled" (International IDEA 2014: 11).

[2] Parliamentary Assembly of the Council of Europe, Resolution 1987 [2014] on the right to internet access.

[3] Santiso, 2018.

[4] There are notable examples of this: from the Egyptian teenagers who used Facebook to rally protesters to Tahrir Square, to the influence of disinformation on the outcome of the Kenyan Presidential Election, to the Chileans who campaigned online to make overseas voting a key election issue with "Haz tu voto volar" or the fact-checking project "Verificado2018" in Mexico.

day. Much of this time will be spent in social media platforms like Facebook (with 2,167 million users), Youtube (1,500 millions), Instagram (800 millions) or Twitter (330 millions).

7. Today approximately two billion internet users are using social networks[5] on a daily basis, and social media have become an indispensable part of modern political campaigning, their effects on the public being dependent on multiple factors such as channel-variables (e.g. Twitter vs. Instagram), specific audience characteristics and predispositions, user motivations and the political campaign context overall.[6]

8. Even though everyone seems to use the internet and social media, different age groups use them for different purposes. According to the *Reuters Institute Digital News Report 2017*, social media tends to be the main source of news for people between 18 and 34 years old, whereas television is more important for people above 55.

9. According to the same study of the Reuters Institute, more than half of the respondents (54%) prefer paths that use algorithms to select stories (search engines, social media, and many aggregators) rather than editors or journalists (44%). This means that young citizens might be making political decisions based on the information filtered by the algorithms of such digital environments, instead of on strict journalistic standards. At the same time, it should be noted that according to recent research,[7] personalised recommendations through algorithmic selection may provide just as diverse news offers as human editorial selection.

10. According to the *Reuters Institute Digital News Report 2018*, the use of social media for accessing news decreased in 2017. People seemed to have less trust in the social media sources. It has also been observed that "[t]he internet has quickly moved from primarily being used for information access to become a participatory environment more closely mimicking the democratic participation traditional in the physical world".[8] As a consequence, the massive use of the internet and social media platforms around the world is changing many aspects of our social and political life. The social mechanisms of knowledge and opinion making are becoming more collaborative and self-regulated (e.g. Wikipedia, Facebook) and political activism has found new and efficient ways of organisation and expression.[9]

11. In its beginnings, the internet was hailed as a promise of equality and liberty. It was seen as a potential *new public sphere*, the platform of democratic public discourse, empowering individuals to be active participants in the public discourse and hence contributing to a more efficient political democracy with an enlightened public due to the active discourse on social media. The public sphere used to be hierarchically organised with set and established functions of various players such as the State, the media, the church or educational institutions, all of which have today lost control over the horizontal interchange of news and views among the users. The social media promised to give everyone a voice. In contrast with the traditional mass media, the internet has an open-ended multidirectional architecture, and the access costs are relatively low. These traits make the internet a particularly effective media for common citizens to become active speakers instead of just receivers of information and have created a "networked public sphere", where individuals can "monitor and disrupt the use of mass media power" thanks to the immediate access to several sources of information and data distribution.

---

[5] Statista – Most popular social networks worldwide as of October 2018. Available at: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[6] Dimitrova & Matthes, 2018.

[7] See https://www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1444076 and https://www.thatseemsimportant.com/content/blame-the-algorithm/ .

[8] Laidlaw 2015, p. 7.

[9] Castells 2011; Cohen et al. 2012.

12. In the past, journalists with their editorial practices and ethical obligations held the gatekeeper role in communication, not only deciding what was fit to print or publish, but also in charge of adherence to the statutory requirements, such as a fair and balanced coverage with regard to the public service media, respecting silence periods where relevant, and/or the right of reply and equivalent remedies for candidates and political parties. Now this gatekeeping function is increasingly taken over by new intermediaries. Such companies include internet service providers (ISPs), search engines and social media platforms. The *Internet intermediaries*[10] are organizations (primarily, for-profit companies) that "bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties". These have hence acquired control over the flow, availability, findability and accessibility of information and other content online.[11]

13. The internet's great promise was that it operated outside the purview of existing communications monopolies but in reality large multinational corporations[12] have global control over the flow of information and are thus in a position to shape the political discourse and opinion formation. The same forces are at work as in the traditional media landscape but now their voices are amplified by social media and they are able to reach every corner of the world and transform societies and lives. The notion that the internet should afford at least a minimally competitive landscape for new entrants seems no longer relevant. The few private actors who own the information superhighways are powerful and deregulated enough to dictate conditions on social, individual and political freedoms, thus becoming a third actor in the democratic arena; and content production has become so "democratic" and anonymous that it is extremely difficult to identify trustworthy information and attribute responsibilities for illegal behaviours online.

14. The social media, like Facebook, is no less than the traditional media controlled by market forces. The stock price of Facebook like any big media corporations depends on its advertisement revenues; to grow financially and sustain its market value. Advertising on Facebook works by determining its users' interests, based on data it collects from their browsing, likes and so on, through a very hi-tech operation. The sites make money from clicks, and through algorithmic regulation create echo chambers and filter bubbles where individuals receive the kinds of information that they have either preselected, or, more ominously, that algorithms have figured out they want to hear. This allows for political advertising to be increasingly individually tailored and targeted. Instead of being a public square featuring many voices people are becoming more isolated and out of touch with the whole spectrum of the public.

15. The "democratisation" of content production and the centralisation of online distribution channels have had as unintended consequence the proliferation of false information, private and public disinformation tactics. The advent of every means of communication (1) expands the dissemination of and the access to information (freedom of communication); (2) implies the risk of abuses (malicious content); (3) opens the way to censorship and (4) to manipulation by the powerful public and private actors.

---

[10] The term 'internet intermediaries' refers to the operators of online media platforms, of search engines, social networks and app stores (van der Noll, Helberger, & Kleinen-von Königslöw, 2015). According to the Council of Europe's Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries, these players facilitate interactions on the internet between natural and legal persons by offering and performing a variety of functions and services. Some connect users to the internet, enable the processing of information and data, or host web-based services, including for user-generated content. Others aggregate information and enable searches; they give access to, host and index content and services designed and/or operated by third parties. Some facilitate the sale of goods and services, including audio-visual services, and enable other commercial transactions, including payments.

[11] https://www-cdn.law.stanford.edu/wp-content/uploads/2017/04/07_28.2_Persily-web.pdf

[12] See e.g. https://www.forbes.com/sites/steveandriole/2018/09/26/apple-google-microsoft-amazon-and-facebook-own-huge-market-shares-technology-oligarchy/#372d73d92318

16. The development of internet and of social media has brought mass communication and the imparting and receiving process to a scale of dimensions unkown since the creation of the printing press. The proliferation of false information, private and public disinformation tactics has therefore become significantly more widespread and technically sophisticated over the last few years, with bots, propaganda producers, disinformation outlets exploiting social media and search algorithms that ensure high visibility and seamless integration with trusted content, misleading large audiences of news consumers, and more importantly, voters. While disinformation has always been a strategy to discredit opponents and to sway political support to one side or the other, digital technologies have increased the threats of false information to democracy for different reasons: the speed of dissemination of (false) information through the internet;[13] the fact that they are actually facilitated by the current architecture of search-engines and social media; the lack of tools (either legal, social or technical) to identify them and stop their spread; and the difficulty of investigating and prosecuting such online behaviour.

17. In recent years, foreign intervention in elections through the use of social media has also become a concern for democracies. Technological resources such as low-cost digital espionage campaigns, paid users and bots, selective disclosure of information or creation of false information has changed the rules of the game during electoral campaigns. As a side effect, this has eroded confidence in democratic governments.

18. At a global scale, the above-mentioned practices – which are facilitated by digital technologies – may pose a threat to democracy and question the idea of the internet as a technological means for more democratic governance.

19. The existence of digital technology, and its application to nearly all aspects of life including elections, is a fact which cannot be put into question. This study is not intended at assessing its positive and negative aspects, but at meeting the challenges it presents in the electoral field. It will therefore mainly focus more on the problems the innovation raises and on their possible solutions than on its advantages.

20. The present report does not intend to provide concrete and universal solutions for all problems that the use of the internet and social media might entail in all electoral processes. The particularities of each nation and each democracy would make it an impossible task.[14] Instead, its purpose is to identify the most relevant legal problems caused by the use of those technologies, describe their logic and possible solution parameters, point out the shortcomings identified so far, and suggest a general set of principles and guidelines that might help to adapt democracy and its laws to the new technological realities. In this sense, the conclusion of this work resembles a roadmap to existing and future regulation and cooperation principles, rather than a handbook to solve all problems.

21. This study is to be seen as a complement to previous Council of Europe documents on this topic, notably the 2017 Council of Europe report on “Information Disorder”[15] (hereafter CoE Information Disorder Report 2017) and the “Study on the use of internet in electoral campaigns” (hereafter CoE Election Study 2017). [16]

[13] Evidence is also now available that people are more likely to share untrue news. Moreover, according to the largest ever-made study of this phenomenon in digital media done by the MIT, false information is more prone to circulate through digital means. It would furthermore appear that it takes true stories about six times as long as false stories to reach people (Vosoughi, Roy and Aral, 2018). According to the Edelman Trust Barometer 2018 Global Report nearly 70% of the global internet users worry about “fake news” being used as a weapon.
[14] See the Reference document CDL-AD(2019)016 for examples of different criteria to solve similar problems.
[15] Council of Europe report, DGI(2017)09.
[16] Council of Europe study, DGI(2017)11.

III. New technologies and information

22. In online society, information is the prime commodity not only of economic production but also of social interaction and governance. The impact of the internet on reality is universal, and affects even those who have never used the technology. It directly affects public opinion wherever people are located, and has already changed the way that people think and behave in the world around them. It gives voice to each and everyone interested and enables them to contribute to the public discourse, whether negatively or positively. It paves the way for 'PR-troops' to rush to the forum when much is at stake to try to influence the turn of events. At times fiction intervenes into this equation with the virtual and the physical.[17] Public figures may discover that their fictional characters are even more influential "actors" than their physical selves.[18] Humor can have a similar effect: Internet users may build different perceptions, by creating fake satirical accounts for public figures for example, which directly affect the image of the person imitated and can sometimes end up confusing the public and the mass media.[19]

23. Information is transmitted mainly through images, which, unlike words, are processed automatically: man risks being converted into a passive receptor, submerged in colours, shapes, sequences and background noises and incapable, in the absence of written culture and verbal language, of transforming information into knowledge, and images into judgments and ideas. This risks resulting in a progressive dilution of the capacity for abstraction. *Homo sapiens*[20] is increasingly turning into *homo videns*: a creature that looks but does not think, that sees but does not understand. Images are surrounded by written texts, either positive or negative, which are also converted into images and, like other information, are processed in an immediate way, instead of being reflected on.[21]

24. When information is reduced to simple stimuli that affect the recipient,[22] man responds more to persuasion and less to information. The prominence of the image also leads to a difficulty in explaining complex concepts that require a certain level of abstraction. The stimuli to which people respond are almost exclusively audiovisual, with the presumption of truth, and they only react to images that manage to create a reaction. The emotional content in rumors becomes more important than the factual and thus provokes emotional reactions, normally hatred or slander. This is increasingly taken advantage of by PR-agencies paid by political actors to mobilize the ground where hatred and slander have gained foothold.

---

[17] A clear example of the breakdown of the lines of fiction and reality can be observed in DAESH´s communications strategy. By consciously imitating video games and blockbusters, they generate attention, creating a humanized image of the terrorist and a depersonalized image of victims: Lesaca, Javier. *Armas de seducción masiva*. Peninsula, Atalaya, 2017. By contrast, traditional media do not reflect the consequences of their barbarism in all its harshness.

[18] Support for Kevin Spacey, or his incarnation of the President of the United States of America in the series, House of Cards, created a lot of controversy. The case of the wrestler, Hulk Hogan, went to North American courts, and eventually achieved a favourable sentence, based on the distinction between the acts of the fictional character, inside and outside the ring, and the person that represented it.

[19] In different social media platforms false accounts are rife, and whether or not they warn of their parodic nature, they create a stereotype of the character that they are imitating, using humour. Some of them end up having more of a following than the real accounts of the person that they are parodying. In Spanish politics, notable examples include @EspeonzaAguirre and @NanianoRajoy

[20] Sartori, Giovanni. Homovidens, Taurus, 1989

[21] In this regard it is important to reconsider the famous phrase by E.M. Foster which said that "*Books are facts to be read (which is annoying as that takes a long time); it is the only way of knowing what they contain. Some wild tribes eat them, but in the West reading is the only technique known".*

[22] Schwartz, Tony. La respuesta emocional. Ed. Liderazgo democrático 2. Quito, 2001. p. 37.

25. The phenomenon called “fake news”[23] captured popular attention in the wake of the 2016 US presidential elections. ‘Fake news’ describes various distinct phenomena. It usually combines elements of traditional news with features that are exogenous to professional journalism.[24] Fake news is characteristic of the collapse of traditional news (not that disinformation, misinformation or sensationalism are new phenomenons) and the prevailing chaos of social media communication. This is a new version of the old struggle over the definition of truth, political and financial forces waging propaganda wars with ‘fake news’ as the main weapon.

26. The mass distribution of images has decisively contributed to the success of ´fake news´, by giving information the appearance of infallibility. Communication ends up being converted into a spectacle, rewarding simple concepts, misleading headlines, anything that draws the reader’s attention (click bait), although it can end up being reductionist. Form reigns over substance, and images over ideas; there is a search for simple answers that divide the world into black and white, yes and no, and in which there are no nuances. The brevity, the importance of the image and the ease of re-sharing content, typical of social networks, all favor the spread of the techniques that distort reality.

27. Today’s expectation for constant updates and even predictions[25] results in information being developed as soon as it is produced, without being checked or reflected upon. This dynamic rewards speed over quality, creating informative cycles that often do not even last twenty-four hours, exhausting information before it has time to be published in the written press the following day. The infinity of storage capacity and its availability means that statements can be recalled in seconds from the respective website months or even years afterwards. These contradictions are also subject to mass diffusion and sometimes, when seen out of context, can be subject to “fake news”.

28. Thousands of analyses, opinions and data on each event accumulate in a chaotic way on social networks and are distributed with an almost infinite capillarity through various terminals to which citizens are connected. The overload of information hinders communication, because certain realities manage to go unnoticed, benefitting from the simpler and more eye-catching aspects of others. The process of showing facts to correct errors in information is an insufficient means of correcting these errors.

29. Individuals create their own informative ecosystem or personal world, which is formed of auto-referential pieces of information that do not require any type of consistency with earlier texts, nor with reality. The result is a heavily biased perception of those who do not share the same informative ecosystem. The new and varied sources of information allow for the reinforcement of individual ideas and thus give force to confirmation bias, in which attention and credibility are given to information that fuels one´s own beliefs. The algorithms used by personal communication tools and other social networks detect the preferences of users, displaying them more often and thus further reinforcing the knowledge and support of related topics. As such, despite the mass of information available, the majority of it is either not accessed, or accessed by those already convinced of its limited credibility. Undesirable or unwelcome facts can be ignored, in favor of personalized narratives. Information and corrections are selected in order to prove that a particular opinion is correct and that

[23] The Council of Europe Information Disorder report 2017 deliberately refrains from using the term “fake news” on the ground that it is inadequate to capture the complexity of information pollution and has become increasingly politicised.

[24] Mourao, R.R. and Robertson, C.T.: Fake News as Discursive Integration: An Analysis of Sites that Publish False, Misleading, Hyperpartisan and Sensational Information, published online: 13 Januar 2019

[25] In Spain, especially on Wikipedia, a current trend involves suggesting that people are dead when they are actually in good health. For example, the nurse who contracted Ebola was cremated and then miraculously came back to life again.

alternative ones are wrong.[26] This can even happen with verified information, as it is shared much more when it reinforces previous ideas than when it questions them.[27]

30. Social environments also determine how information is received, in particular when it allows people to identify with a group and hide what may damage, or not coincide with, the group´s position. The bandwagon effect, for example, is based on the need to belong and the shame of being different. Hence, people trust the opinion of the majority, creating an echo-chamber where opinions are mutually reinforced.

31. The confirmation bias triggers fragmentation between informative bubbles[28] of parallel informative worlds, which makes it difficult for common spaces for debate to exist. The general public sphere is currently being reduced to small highly mobilized blocks isolated from one another. The possibility of communicating and being informed in a selective, almost personalized way, which is principally facilitated through technology and social networks, creates self-referential micro-communities within which the possibility of knowing and putting oneself in the place of the other encourages more radical positions and a lack of dialogue, hindering empathy.[29] Together these two elements promote polarization and allow for the establishment of a single system of values, at least within closed groups that end up silencing and expelling dissidents. As different informative ecosystems interact they often clash, which in itself feeds this polarization, as the credibility of each radical position decreases according to their opposite´s views, again fuelling the radical discourse of the other.[30]

32. Technology does not just affect the way that information is distributed, it affects the entire communicative process of collecting, storing, organizing and distributing information. Citizens are not mere recipients of information, they become major players in the communicative process. They create they own information sources, in the absence of the traditional gatekeepers and regulators. As a result of this abundance and diversity of information, the media loses its referential character and authority. Moreover, the errors made by traditional media sources because of the aforementioned immediacy of the informative process, coupled with the confusion of sources, have furthered the decline of the credibility of the media.[31] In this way individuals join the media, often on equal terms. Personal information spaces are created in which citizens take shelter; faced with floods of content, they have a reduced and manageable, reliable and secure informative universe dominated by relationships with those who are closest to them in their personal and professional lives, and ideological views.

33. As they share information, citizens become the protagonists of communication, questioning the added value of the mass media. The internet is increasingly used by citizens as a source of information,[32] and when they do so, they do not distinguish between the

---

[26] Sunstein, C., Scala, A., Quattrociocchi, W. Echo Chambers on Facebook. 2016. Available at: https://ssrn.com/abstract=2795110 (consulted 25/01/2018)

[27] Shin, Jieun, Thorson, Kjerstin. Partisan Selective Sharing: The Biased Diffusion of Fact-Checking Messages on Social Media. Journal of Communication. Vol 67, 2017. Available : http://onlinelibrary.wiley.com/doi/10.1111/jcom.12284/full (consulted 25/01/2018)

[28] Parisier, Eli. The filter bubble. The Penguin Press. New York. 2011.

[29] Sunstein, C. R. The law of group polarization. Journal of political philosophy 10, 175–195 (2002).

[30] https://www.buzzfeed.com/charliewarzel/2017-year-the-internet-destroyed-shared-reality (consulted 25/01/2018)

[31] President Trump has used some of these real or apparent failures to award prizes to fake news https://www.elconfidencial.com/mundo/2018-01-18/trump-fake-news-awards-noticias-falsas-premios_1508101 (consulted 25/01/2018)
An example can be consulted at: https://theintercept.com/2017/12/09/the-u-s-media-yesterday-suffered-its-most-humiliating-debacle-in-ages-now-refuses-all-transparency-over-what-happened (consulted 25/01/2018)

[32] 46% of European Union citizens followed the news on social networks in 2016: Reuters Institute Digital News Report 2016, available at:

original, more credible, sources of information and the rest of the content from family and friends.[33] In fact 79% view the latter as a credible source of information, followed by the views of academic experts (72%), employees of businesses (60%), and businesses whose services they use (59%). Information from journalists (48%), CEOs (43%), well-known online figures (42%) and celebrities (29%) are at the bottom of the list.[34]

34. The weight that interpersonal communication gains through social networks has led to the mass creation of bots, anonymous, automated and sometimes fake accounts that act as individuals online and increase the massive distribution of specific information, aiming to create currents of public opinion, acceptance or rejection of people or ideas, in an artificial way.[35] By giving off the impression that they have widespread support, these features create a bandwagon effect, and others accept the ideas shared by this apparent majority. This generates herd behavior, by which individuals neglect personal responsibility and submit themselves to the will of the collective; they imitate one another and deny discrepancy. The redundancy of misinformation, especially when it is found in the mass media, is set up as a "belief", an unquestionable basis whose denial implies the risk of being disqualified.

IV. The impact of social media and the internet on democracy and electoral processes

35. The internet has given people unprecedented access to information about elections and enabled them to express their opinions, interact with candidates and get actively involved in electoral campaigns.[36] Social media in particular constitute the predominant platform of political debate and, as such, they are sources of political information.[37] Studies suggest that the increasing flux of information fostered by social media strengthen the critical capacity of citizens towards their governments[38] and that there is a strong positive correlation (0.71) between the use of the internet and social media, on one side, and the support to democracy as a desirable form of government, on the other.[39] Moreover, many authors argue that the generalised use of internet and social media provides a more accurate knowledge of the citizens' interests and facilitates the organisation of large scale social movements.[40]

36. Nonetheless, even if "[t]he internet has the power to be a tool of democracy… its potential in this respect is at risk… [because the] same technology that facilitates discourse creates opportunities for censorship of information, monitoring of online practices and the subtle shaping and manipulation of behaviour",[41] hence threatening the authenticity of suffrage, the equity of the electoral competition and, ultimately, the capacity to translate the *will of the people* into institutional representation and governmental decisions.[42] It should be noted that any undue influence over the authenticity and freedom of suffrage might affect not only the translation of the popular will into concrete actions, but also the protection of minorities, the balance among basic human rights and the possibility to hold political parties and elected officials accountable. Even if such threats already existed in the past, they have increased through the more sophisticated methods facilitated by digital technologies.

---

http://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Digital%2520News%2520Report%25202016.pdf(consulted 25/01/2018)

[33] According to the report "I saw the news on Facebook" by the Reuters Institute for the Study of Journalism at the University of Oxford, in 2017 over half of British people obtained information from social networks. And of this half, over 50% do not remember the correct information source.

[34] Edelman Trust Barometer 2016

[35] http://agendapublica.elperiodico.com/desde-rusia-bots/

[36] CoE Election Study 2017, p. 7.

[37] Democracy Reporting International 2017.

[38] Gainous *et al.* 2016.

[39] Basco 2018.

[40] Castells 2011; Metaxas and Mustafaraj 2012; Cohen *et al*. 2012; European Union 2015.

[41] Laidlaw 2015, p. 1.

[42] Cf. CoE Election Study 2017, p. 7-9. See also Tambini 2018, p. 265-293.

37. The constant and simultaneous flux of information in real time across multiple platforms represents a huge challenge for the surveillance of behaviour and resources during political campaigns. Moreover, the scattered and anonymous creation of content seriously hampers the identification and attribution of responsibilities for illegal online behaviours. The growing use of *bots* and *trolls* to set agenda in the social media, as well as the massive distribution of false information, seriously damage the equity in the electoral competition and allow for external actors to manipulate the discourse and the voting preferences.[43] Furthermore, the algorithms that govern search engines and social media may foster a partial and sometimes illusory comprehension of politics and democracy.[44]

38. The impact of the digital environment on elections was highlighted in the controversies following the United Kingdom Brexit referendum and the United States presidential elections in 2016. The enforcement of rules and regulations on paid advertising was limited; voters' personal data were collected and processed for election purposes without their consent and in lack of legal entitlement; political communication was channeled to unregulated social media platforms without safeguards in place on fair media coverage. These implications challenged the established institutions and principles of regulation of election communications such as freedom of association, spending limits and regulation of political advertising,[45] and undermined the ability of the current regulatory regimes to maintain a level playing field in electoral communication. They posed threats to elections and unleashed a potential for corrupt practices to emerge.

39. The transformed communicative spheres on the internet and the changed way of transmitting political messages to voters making it possible for false and/or harmful information to "spread among potential voters on an unprecedented scale without any oversight or rebuttal".[46] This has led to a degree of *information disorder*, which may take three different forms:

- Mis-information, that is sharing false information, but without the intent of causing harm;
- Dis-information, which stands for knowingly sharing false information with the intent to harm; and
- Mal-information, which describes genuine information shared with the intent to cause harm, often by disclosing information from the private sphere into the public sphere. [47]

40. In certain cases untrue information has been *strategically* disseminated with the intent to *influence election results*. It has been documented that *cyber troops* on the internet are often *government, military or political party teams committed to manipulating public opinion* over social media. Organised *social media manipulation first emerged* in 2010, and by 2017 there are details on such organisations in 28 countries.[48]

41. Not only the social media, but also search engine providers can manipulate information with or without the intent to skew the election results in favour of a particular political option. Recent research shows that manipulations of search results by those providers can produce a

[43] Quintana 2016; Fidler 2017.
[44] Van Dijck 2013; McChesney 2013.
[45] CoE Election Study 2017, p. 13.
[46] CoE Election Study 2017, p. 15.
[47] CoE Information Disorder Report 2017
[48] Bradshaw & Howard, 2017. See also the Freedom House 2017 report, according to which manipulation and disinformation tactics played an important role in elections in at least 17 other countries over the year. According to the Communications Security Establishment (CSE) of the Government of Canada, in 2017 alone, 13% of countries holding federal elections have had their democratic process targeted by hacktivist, cybercriminals, and even public or private political actors, all of them with the intent to manipulate information, sway public opinion or even destabilise democratic institutions.

so-called *search engine manipulation effect* which can shift the voting preferences of undecided voters by 20% or even more in some demographic groups.[49]

42. There are cases where state agencies have employed armies of "opinion shapers" to spread government views and counter critics on social media, or the case of Cambridge Analytica, the company that is being investigated for its alleged role in the 2017 US presidential elections and in the Brexit referendum for accessing and using private data of 50 million Facebook users.[50] Unlike other direct methods of censorship, such as website blocking or arrests for internet activity, online content manipulation is difficult to detect and even more difficult to defeat, given its dispersed nature and the sheer number of people and bots employed for this purpose.

43. As targeted messages do not reach the public, but only selected groups or individuals, and are not subject to any oversight or journalistic scrutiny, political candidates and parties can make different promises to different people, dispersing their political objectives into separate, not necessarily reconcilable messages. Indeed, some research shows increased digital campaigning on the so-called wedge issues, those that are highly divisive but have the ability to mobilise voters (immigration policies, welfare, same-sex marriages, etc.). Lastly, message targeting seeks to optimise the electoral campaigns' resources and thus focuses largely on swing or undecided voters. Those who are not singled out by political party messages are deprived of an entire spectrum of political stances, which in turn creates inequalities in terms of the available information on which the voters base their political choices.

44. Finally, states and private actors all over the world can use the digital technologies to violate human rights or even as a military instrument to attack countries and their institutions through malware, ransom ware, spyware and other sophisticated programmes.[51] This is known as "*cyber warfare*" and has been previously and successfully used to undermine state projects and systems, for instance the Stuxnet attack on the Natanz (Iran) nuclear plant.[52]

45. Along with their accessibility, sophistication and public appeal, cybernetic tools are embedded in a borderless environment. What was legally created under national laws, could now be illegally allocated in a different jurisdiction or vice versa. Moreover, with the increasing use of *cloud computing*, the online information has become even more fragmented, thus making it extremely difficult to identify its origin or authorship. Cybercrime and cyber-threats operate beyond the limits of any national jurisdiction. This situation presents several difficulties to criminal investigation and prosecution; hence, the urge to attend this phenomenon from a transnational perspective.[53]

46. To conclude, today we are witnessing the parallel proliferation of information and its pollution at a global scale. The internet-based services have enriched and diversified news sources, facilitating individuals' access to information and their decisions on the most crucial matters in democracy, notably on the choice of their legislature. However, at the same time, a new era of information disorder distorted the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their votes. This environment potentially undermines the exercise of the right to free elections and creates considerable risks to the functioning of a democratic system.

[49] Epstein & Robertson, 2015.
[50] Mccausland, P. and Schecter, A., 2018, BBC, 2018.
[51] Quintana 2016.
[52] Quintana 2016; Mecinas Montiel 2016, p. 404, 418-419.
[53] Davara 2003; Salt 2017 p. 520-521.

47. Digital technologies have reshaped the ways in which societies translate the will of the people into votes and representation, and they have to a large extent changed political campaigning. Even though the internet fosters some aspects of the democratic contest, it also hampers them. The worldwide pervasiveness of digital technologies has moved the arena of democratic debate to the virtual world, raising many questions about their influence on voter turnout and the need to survey and regulate online social behaviour. Moreover, adequate protection against cyber warfare needs to be ensured.

V. Relevant European and international standards and instruments

48. The aforementioned phenomena interfere with a number of fundamental rights protected at European and universal level by several international declarations and conventions, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the American Declaration of the Rights and Duties of Man, the American Convention on Human Rights, the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights (hereafter ECHR).

A. Right to free elections and freedom of expression

1. Basic principles

49. Under the ECHR, as interpreted by the European Court of Human Rights (hereafter the ECtHR), the Council of Europe member states have an obligation to secure the rights and freedoms for everyone within their jurisdiction. The *right to free elections* enshrined in Article 3 of Protocol No. 1 to the ECHR is not only an objective and essential principle in any democratic society, but also a fundamental individual right on which every citizen can rely, one that most effectively promotes "true democracy".[54]

50. The right to free elections incorporates the right to vote and the right to stand for election.[55] Moreover, it also entails a positive obligation on the member states to ensure conditions under which people can freely form and express their opinions and choose their representatives. This obligation is of utmost importance with regard to the (un)disrupted communicative context of elections. The right to free elections provides that member states "undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature", which indicates that the rights to freedom of expression and to free elections are prerequisites of each other.[56] This interpretation was reaffirmed by the ECtHR in stating that "free elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system".[57]

51. The ECtHR further stated that the two rights are inter-related and operate to reinforce each other, freedom of expression being one of the conditions necessary to ensure free elections. In order for the rights guaranteed by Article 3 of Protocol No. 1 to be effective, their protection extends to the election campaign. For this reason, it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate

---

[54] Thorgeirsdóttir, Herdis (2005), *Journalism Worthy of the Name: the Affirmative Side of Article 10 of the ECHR*, Kluwer Law International. Lécuyer, 2014. See *Mathieu-Mohin and Clerfayt v. Belgium*, Application no. 9267/81 (ECtHR, 2 March 1987); *Ždanoka v. Latvia*, Application no. 58278/00 (ECtHR, 16 March 2006). See also ECtHR, 2018, "Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights – Right to free elections", available at: https://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_ENG.pdf

[55] *Mathieu-Mohin and Clerfayt v. Belgium*; *Ždanoka v. Latvia*.

[56] Plaizier, 2018.

[57] *Bowman v the United Kingdom,* Application no. 24839/94 (ECtHR, 19 February 1998), para 42.

freely.[58] According to the ECtHR, member states have a positive obligation to ensure the effectiveness of freedom of expression: they are required to create a favourable environment for participation in public debate by all persons concerned, enabling them to express their opinions and ideas without fear. The state must not just refrain from any interference in the individual's freedom of expression, but is also under a positive obligation to protect his or her right to freedom of expression against attack, including by private individuals.[59]

52. The ECtHR recognised however that in certain circumstances the rights under Article 10 ECHR and Article 3 of Protocol No. 1 may conflict and it may be considered necessary, in the period preceding or during an election, to place certain restrictions on freedom of expression, of a type which would not usually be acceptable, in order to secure the "free expression of the opinion of the people in the choice of the legislature".[60] The Court recognised that, in striking the balance between these two rights, member states have a margin of appreciation, as they do generally with regard to the organisation of their electoral systems. At the same time, it stressed that any restrictions on freedom of expression must be proportionate to the legitimate aim pursued and necessary in a democratic society. The Court indicated for example that Article 10 ECtHR as such does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful.[61] On the other hand, attention is drawn to the Court's decision concerning the right of an NGO to make political advertisements on radio and television, in which it balanced the applicant NGO's right to impart information and ideas of general interest which the public is entitled to receive with the authorities' desire to protect the democratic debate and process from distortion by powerful financial groups with advantageous access to influential media.[62] The Court recognised that such groups could obtain competitive advantages in the area of paid advertising and thereby curtail a free and pluralist debate, of which the state remains the ultimate guarantor. As a result, the risk of an imbalance between political forces in competition has to be taken into account to maintain a free and pluralist debate.

53. The rights under Article 3 of Protocol No. 1 are not absolute either: there is room for "implied limitations",[63] and the member states must be given a wide margin of appreciation in this sphere. In examining compliance with Article 3 of Protocol No. 1, the Court has focused mainly on two criteria: whether there has been arbitrariness or a lack of proportionality, and whether the restriction has interfered with the free expression of the opinion of the people.[64]

54. The ECtHR recognised the right of individuals to access the internet, as in its ruling against the wholesale blocking of online content, it asserted that "the internet has now become one of the principal means of exercising the right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest".[65] It stated that Article 10 ECHR guarantees the freedom to express, receive and impart information and ideas regardless of frontiers. Blocking

[58] *Bowman v the United Kingdom,* Application no. 24839/94 (ECtHR, 19 February 1998); *Orlovskaya Iskra v. Russia*, Application no. 42911/08 (ECtHR, 21 February 2017). During the 2019 European elections, Facebook allowed EU-wide political ads for the European Parliament: https://www.politico.eu/article/facebook-allows-eu-wide-political-ads-for-european-parliament/; https://techcrunch.com/2019/04/26/facebook-says-its-open-to-advertising-u-turn-for-the-eu-elections-enabling-cross-border-campaigns/?renderMode=ie11.

[59] *Dink v. Turkey*, Application no. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09 (ECtHR, 14 September 2010).

[60] *Bowman v the United Kingdom,* Application no. 24839/94 (ECtHR, 19 February 1998); *Orlovskaya Iskra v. Russia*, Application no. 42911/08 (ECtHR, 21 February 2017).

[61] *Salov v. Ukraine*, Application no. 655118/01 (ECHR, 6 September 2005).

[62] *Animal Defenders International v. the United Kingdom*, Application no. 48876/08 (ECHR, 2013).

[63] Article 3 is not limited by a specific list of "legitimate aims" such as those enumerated in Articles 8 to 11 ECHR, and the ECtHR does not apply the traditional tests of "necessity" or "pressing social need" which are used in the context of Articles 8 to 11 ECHR.

[64] *Mathieu-Mohin and Clerfayt v. Belgium*; *Ždanoka v. Latvia*.

[65] *Ahmet Yıldırım v. Turkey,* Application no. 3111/10 (ECtHR, 18 December 2012). See also *Cengiz and Others v. Turkey*, Application nos. 48226/10 and 14027/11 (ECtHR, 1 December 2015).

access to host and third-party websites in addition to websites concerned by proceedings renders much information inaccessible, thus restricting the rights of internet users. The Court further clarified that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework, affording the guarantee of judicial review to prevent possible abuses, is in place.

55. Moreover, the ECtHR acknowledged that "given the important role played by the internet in enhancing the public's access to news and facilitating the dissemination of information (see Delfi AS v. Estonia [GC], § 133, ECHR 2015), the function of bloggers and users of the social media may be assimilated to that of 'public watchdog' in so far as the protection of Article 10 is concerned".[66] This protection may extend to access to (publicly held) information if it is instrumental for the exercise of the right to freedom of expression: the information to which access is sought must meet a public-interest test. Nonetheless, as mentioned earlier, Article 10 does not guarantee an unlimited freedom of expression; restrictions may be permitted, for example, in order to protect the right to private life (Article 8 ECHR), if the means used are proportionate to the aim pursued.

56. Fundamental principles relating to elections are furthermore expressed in the Code of Good Practice in Electoral Matters adopted by the Venice Commission in 2002.[67] They include, *inter alia*:

- equality of opportunity for parties and candidates;
- a neutral attitude by state authorities with regard to the election campaign, to coverage by the media, and to public funding of parties and campaigns;
- equality of opportunity can be proportional rather than strict, and applies in particular to "radio and television air-time";
- in conformity with freedom of expression, legal provision should be made to ensure that there is a minimum access to privately owned audio-visual media, with regard to the election campaign and to advertising, for all participants in elections;
- campaign funding must be transparent;
- equality of opportunity can lead to a limitation on political party spending, especially on advertising.

57. The basic principles relating to elections are subject to particular challenges when electronic voting methods are used. The Council of Europe continues to be the only organisation that has set intergovernmental standards in the field of e-voting. The Committee of Ministers Recommendation Rec(2004)11, which has been used in national jurisprudence even in non-member states, as well as by other relevant international actors, has recently been updated: a new recommendation – which consists of the actual Recommendation CM/Rec(2017)5 on standards for e-voting, the guidelines on the implementation of the provisions of the Recommendation with specific requirements and the Explanatory Memorandum – was drafted as an enhancement of Rec(2004)11 and deals with the most critical part of election technology, namely e-voting, which means the use of electronic means to cast and count the vote. This category includes systems such as Direct Recording Electronic (DRE) voting machines, ballot scanners, digital pens and internet voting systems. The Recommendation is aimed at ensuring that e-voting guarantees universal, equal, free and secret suffrage, and it includes provisions on organisational requirements, accountability, reliability and security of the system.

---

[66] *Magyar Helsinki Bizottság v. Hungary*, Application no. 18030/11 (ECtHR, 8 November 2016). See also *Animal Defenders International v. the United Kingdom*, Application no. 48876/08 (ECHR, 2013).

[67] CDL-AD(2002)023rev-cor. See also the Joint Guidelines for Preventing and Responding to the Misuse of Administrative Resources during Electoral Processes (CDL-AD(2016)004), which reaffirm the principles of neutrality and equality of opportunity concerning access to publicly-owned media.

58. In this connection, attention is also drawn to relevant Venice Commission documents. The Code of Good Practice in Electoral Matters makes it clear that "electronic voting should be used only if it is safe and reliable; in particular, voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage; the system must be transparent".[68]

2. Funding of electoral campaigns

59. There is a range of commonly agreed standards against corruption in the funding of political parties and electoral campaigns (which are recommended to also apply to entities related to political parties, such as political foundations). They were set by the Parliamentary Assembly Recommendation 1516 (2001) on the financing of political parties and followed upon by the Committee of Ministers Recommendation Rec(2003)4 on common rules against corruption in the funding of political parties and electoral campaigns. The standards to be applied include (a.) requirements on a *reasonable balance* between public and private funding of political parties; (b.) the use of *fair criteria* for the distribution of state contributions to parties; (c.) imposition of strict rules concerning private donations including *bans on or limitations of contributions* from foreign donors, religious organisations and restrictions on corporations and anonymous donations; (d.) *limitations on parties' expenditures* linked to election campaigns; (e.) provisions on *transparency* of donations and expenses of political parties; and (f.) the establishment of an *independent authority* and meaningful *sanctions* for those who violate the rules.

60. Similarly, in the Guidelines on Political Party Regulation[69], the Venice Commission and OSCE/ODIHR set out that electoral campaigns' regulations should

- prevent improper influence (and ensure the independence of parties) on political decisions through financial donations;
- provide for transparency in expenditure of political parties and
- ensure that all political parties have an opportunity to compete in line with the principle of equal opportunity.

61. In order to achieve these objectives, the "main ways campaign communication has been regulated has been through electoral law including spending limits and campaign finance controls; subsidies for campaigning communications; pre-poll black outs; media regulation in particular broadcast licensing; rules on political advertising including impartiality, subsidies and free air time; and self-regulation and journalism ethics".[70]

62. The applicable standards were set high in order to "protect the integrity of elections, ensure they are free and fair, and not captured by a narrow range of interests."[71] However, the legislative steps taken by the member states and regulations implemented focused on the offline context.[72] Therefore, their *applicability and efficacy in times of digital political advertising* turned out to be *severely limited*. As mentioned earlier, in recent years policy-makers, governments and civil society alike had to face the reality of there being limits to *law enforcement of the current regulation on the internet*, including as regards the applicability of existing regulation on electoral campaigns.

---

[68] Code of Good Practice in Electoral Matters, CDL-AD(2002)023rev-cor, section I.3.2.IV.; see also paragraphs 42-44 of the Explanatory Memorandum. See also the Venice Commission Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe, CDL-AD(2004)12.
[69] CDL-AD(2010)024, p. 35, para. 159.
[70] CoE Election Study 2017, p. 9.
[71] CoE Election Study 2017, p. 9.
[72] In this context, the use of crowd funding campaigns, mainly through the internet, is increasingly important in changing the scope of funding for electoral campaigns.

63. Namely, legislative limits on campaign finance have been challenged by new forms of digital advertising which are inherently less transparent than their analogue predecessors, thus undermining the existing definitions and restrictions based on specific media types. The safeguards against corruption based on methods for calculating spend and categories for reporting spend on traditional media channels have lost their meaning as political campaigning shifted to the internet. As a result, also the absolute spending limits imposed on broadcasting are becoming less meaningful, while transparency regulations ensuring that citizens are aware of campaign finance and spend are difficult, if not impossible to implement across borders in the digital environment.[73]

3. Political speech and media coverage on electoral campaigns

64. While 'freedom of expression is the lifeblood of democracy', all legal systems now have campaign funding rules and limits and transparency obligations. In the individual sphere it may be that the expression deserves protection irrespective of content, but that does not apply to a campaign. The vast majority if not the totality of the constitutional systems contemplate limits on freedom of expression during an election campaign: for instance, the silence period, cordon sanitaire at polling stations, campaign funding rules and transparency obligations. All campaign restrictions, even those promoting transparency, must be seen firstly as an interference which must be justified, in European systems, according to a test of necessity and proportionality. Regulating the publication of political advertising seems legally possible in the principle for a) Regulation on transparency rather than content, b) regulation on political campaigning, c) Regulation which is either aimed at elections or polls or linked to funding mechanisms or aimed to identify an origin outside the political community. While there are difficult concepts to pin down it is clearly possible to design a scheme for traditional press, broadcasting or poster advertising. But in the digital sphere what is publication and who is the publisher? When is a message “advertising” rather than the individual expression of opinion which “goes viral”?

65. The ECtHR has clearly pointed to the responsibility of the state for preventing inequality in media coverage during elections[74] online and offline, however with significant differences as regards the *influence* between traditional media and new media.[75] The issue at stake now is how to define those differences precisely – *whether they have already reached a “sufficiently serious shift in the respective influence”.*[76] The crucial caption of the momentum of this ‘shift’ is to determine whether the positive responsibility of the state in assuring equal exposure of political parties and candidates are to be applied to new information intermediaries and in what manner.

66. The Council of Europe standards and other instruments in this area seek to provide an *enabling communication context for the enjoyment of the right to free elections*. They reflect the positive obligations of the state to ensure that citizens receive necessary and truthful information on political parties to support their democratic choice to elect their representatives.

67. Recommendation CM/Rec(2007)15[77] applies to a broad range of media, irrespective of the means and technology used for the dissemination of their content, providing guidelines for free and independent media coverage of political campaigns, with higher standards applicable to the public service media outlets. The Recommendation includes a number of guidelines aimed at ensuring responsible, accurate and fair coverage of electoral campaigns; however public service media have a particular responsibility to cover elections in a “fair, balanced and

[73] CoE Election Study 2017, p. 20-21.
[74] *Communist Party of Russia and Others v Russia* App. no. 29400/05 (ECtHR, 19 June 2012).
[75] *Animal Defenders International v the United Kingdom* App. no. 48876/08 (ECtHR, 22 April 2013).
[76] *Ibid.,* para 119.
[77] Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of electoral campaigns.

impartial manner, without discriminating a specific political party or a candidate". As regards the overall opportunities for the political parties and candidates to address the electorate, the Recommendation leaves it to the discretion of individual member states whether they will allow for paid political advertising. However, where parties have the possibility of buying advertising space for the purpose of electoral campaigning, they must be able to do so under equal conditions and rates of payment.

68. Furthermore, the Recommendation sets out a few general requirements for ensuring fair and transparent campaigns; for example, the *right of reply* or equivalent remedies should be made available to the candidates and/or political parties, so as to enable them to effectively respond to any statements that might cause them prejudice during the relatively short duration of electoral campaigns. Also, the *modalities of disseminating opinion polls* should provide the public sufficient information to make a judgment on the value of the polls, while the potential impact of electoral messages just before the elections is mitigated by the provision allowing the member states to consider prohibiting their dissemination on the day preceding voting ("day of reflection"). Moreover, the Recommendation spells out *transparency requirements* on *paid advertising content* along with *ownership* of the outlets (these requirements are detailed by Recommendation CM/Rec(2018)1)[78]. The above-mentioned guidelines target, first and foremost, linear broadcast (private and public) media with extensions to non-linear audiovisual services of public service media. However, with the shift of political campaigning to the online social media context in the past decade, their effectiveness is proving to be reduced.

69. This shift is reflected also in Recommendation CM/Rec(2018)1 which clearly points to the potentially disturbing impact that the online platform's control over the flow, availability, findability and accessibility of information can have on *media pluralism*. Selective exposure to media content leading to potential societal fragmentation is identified as one of the major concerns especially during the time of elections. Therefore, the Recommendation calls on the states to fulfill their positive responsibility and to act as the ultimate guarantor of media pluralism by *ensuring pluralism in the entirety of the multimedia ecosystem*.

70. This interpretation is reinforced by Recommendation CM/Rec(2018)2[79] which addresses the roles and responsibilities of internet intermediaries in relation to their users and to the member states, having due regard to their growing power over communication and the dissemination of information. The potential co-responsibility of intermediaries for content that they store - if they do not act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature (in line with the principles of legality, necessity and proportionality) - should be read in this context. Meanwhile, intermediaries should bear no general obligation to monitor content, which they merely give access to, or which they transmit or store. In this connection, attention is also drawn to the Recommendation CM/Rec(2016)1 which calls on member states to safeguard the principle of network neutrality in the development of national legal frameworks, in order to ensure the protection of the right to freedom of expression and to access to information, and the right to privacy.[80]

71. In its Declaration Decl(13/02/2019)1 of 13 February 2019[81] on the manipulative capabilities of algorithmic processes, the Committee of Ministers emphasised "the need to assess the regulatory frameworks related to political communication and electoral processes to safeguard the fairness and integrity of elections offline as well as online in line with established principles. In particular it should be ensured that voters have access to comparable levels of information across the political spectrum, that voters are aware of the dangers of political

[78] Recommendation CM/Rec(2018)1 on media pluralism and transparency of media ownership.
[79] Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries.
[80] Recommendation CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network.
[81] Declaration Decl(13/02/2019)1 on the manipulative capabilities of algorithmic processes, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

redlining, which occurs when political campaigning is limited to those most likely to be influenced, and that voters are protected effectively against unfair practices and manipulation."

72. The Parliamentary Assembly in its Resolution 2254 (2019) on Media freedom as a condition for democratic elections[82] called on member states to implement effective strategies to protect the electoral process from the information manipulation and undue propaganda through social media. It proposed measures such as the development of specific regulatory frameworks for internet content at election times, and the establishment of a clear legal liability for the social media companies that publish illegal content harmful to candidates – while avoiding extreme measures such as the blocking of entire websites. The Parliamentary Assembly further called on organisations in the media sector to develop self-regulation frameworks with professional and ethical standards for their coverage of election campaigns, and on internet intermediaries to co-operate with civil society and organisations of all political affiliations specialising in the verification of content, to ensure that all information is confirmed by an authoritative third-party source.

B. Right to privacy and personal data protection

73. Article 8 ECHR provides for the protection of the right to privacy. On this basis, the ECtHR has developed extensive case law concerning personal data protection.[83]

74. The Council of Europe Convention on the protection of individuals with regard to automatic processing of personal data ETS No. 108 of 1981 sets out principles and rules for personal data processing as well as the rights of individuals. The Additional Protocol to the Convention of 2011 sets standards for the establishment of data protection supervisory authorities. The particular added value of this legal framework in comparison with the European Union General Data Protection Regulation is that, being open to any country in the world, it allows various legal systems to stand under the same umbrella, hence, harmonising different legal regimes.[84]

75. On 10 October 2018 the new protocol modernising this Convention (hereafter the Modernised Convention) was signed by 21 of the Parties to the Convention. Article 5 of the Modernised Convention strengthens the data protection principles by requiring that data shall be processed fairly and in a transparent manner, collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes, while any further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is subject to appropriate safeguards, compatible with those purposes. The Modernised Convention furthermore provides for additional principles and requirements such as privacy by design, personal data impact assessment and privacy by default, as well as the compulsory notification of data breach to, at least, data protection authorities. It introduces additional safeguards, in particular having in mind the omnipresence of information technologies in data processing, and recognises new categories of data as of sensitive nature. The additional safeguards particularly apply to the processing of sensitive data such as political opinions. The Modernised Convention provides for more detailed provisions on transborder data flows, on additional requirements on data controllers and on the follow-up mechanism.

---

[82] Resolution 2254 (2019) on Media freedom as a condition for democratic elections http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=25409&lang=en

[83] Case law of the ECtHR concerning the protection of personal data, available at: https://rm.coe.int/case-law-on-data-protection/1680766992. See also ECtHR, 2018, "Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life", available at: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[84] This concerns both non-European countries (Cabo Verde, Mauritius, Mexico, Senegal, Tunisia and Uruguay) and European countries (e.g. Albania, Russia, Serbia, Turkey, Ukraine).

76. In addition, there are a significant number of Council of Europe legal instruments pertaining to the protection of personal data within the operation of social networks.

77. The 1999 Committee of Ministers Recommendation No. R (99) 5 for the protection of privacy on the internet includes Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways. The 2010 Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling provides for conditions for such processing and sets out a detailed list of information needed to be given to data subjects. It notes that the lack of transparency, or even "invisibility", of profiling and the lack of accuracy that may derive from the automatic application of pre-established rules of inference can pose significant risks for the individual's rights and freedoms. Although initially perceived as a technique used in a business and marketing context, the recent events demonstrate that profiling is also applied in the election processes.

78. The 2010 Ministers of Justice Resolution No. 3 on data protection and privacy in the 3rd millennium, MJU-30 (2010) RESOL, notes probable consequences of the wide use of ICTs enabling observation, storage and analysis of most day-to-day human activities, thereby potentially inducing a chilling effect linked to the feeling of being under surveillance, which may impair the free exercise of human rights and fundamental freedoms unless robust standards of data protection are effectively enforced worldwide. The 2011 Parliamentary Assembly Resolution 1843 (2011) on the protection of privacy and personal data on the internet and online media emphasises that the protection of the right to data protection is a necessary element of human life and of the humane functioning of a democratic society, and that its violation affects a person's dignity, liberty and security.

79. The 2012 Committee of Ministers Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines recognises the challenge caused by the fact that an individual's search history contains a footprint which may reveal the person's beliefs, interests, relations or intentions, and could reveal, *inter alia*, one's political opinions or religious or other beliefs. It calls for action to enforce data protection principles, in particular purpose limitation, data minimisation and limited data storage, while data subjects must be made aware of the processing and provided with all relevant information.

80. Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services notes the increasingly prominent role of such and other social media services, offering great possibilities for enhancing the potential for the participation of individuals in political, social and cultural life. It recommends actions to provide an environment for users of social networks that allows them to further exercise their rights and freedoms, to raise users' awareness of the possible challenges to their human rights and of the negative impact on other people's rights when using these services, as well as to enhance transparency about data processing, and to forbid the illegitimate processing of personal data. These actions may be taken by engaging with social networking providers. The Recommendation also underlines that users should be informed where their personal data is used in the context of profiling.

81. The 2013 Committee of Ministers Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies stresses that member states do not only have the negative obligation to refrain from interference with human rights, but also the positive responsibility to actively protect these rights, which includes the protection of individuals from action by non-state actors. The ubiquitous use of various devices and information gathered through those devices make tracking and surveillance of people possible, thus revealing delicate and/or sensitive personal information, including political or religious preferences, which can be aggregated to provide detailed and intimate profiles of them.

82. The 2014 Committee of Ministers Recommendation CM/Rec(2014)6 provides for a Guide to human rights for internet users, and in 2017 the Committee of Convention ETS 108 adopted Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. In its Declaration Decl(13/02/2019)1 of 13 February 2019 on the manipulative capabilities of algorithmic processes, the Committee of Ministers encouraged member states to "consider the need for additional protective frameworks related to data that go beyond current notions of personal data protection and privacy and address the significant impacts of the targeted use of data on societies and on the exercise of human rights more broadly".

83. Finally, the Council of Europe produced or commissioned different reports and studies in the field, including the Report on "the use of the Internet & related services, private life & data protection: trends & technologies, threats & implications".[85] The latter calls for affirming and protecting the right to anonymity on the internet, regulating and strictly limiting the creation and use of profiles, in all kinds of different contexts, and for the adoption by the Council of Europe of guidelines on the restrictions to be imposed on surveillance technologies, including the international trade in such technologies.

C. Protection against cybercrime

84. The Council of Europe Convention on Cybercrime ETS 185 of 2001 ("Budapest Convention") addresses two types of threats to electoral democracy.[86] Firstly, attacks against the confidentiality, integrity and availability of election computers and data, which represent forms of cybercrime such as illegal access to computer systems (Article 2), illegal interception (Article 3), data and system interference (Articles 4 and 5) and others. Secondly, dis-information operations where rules on the protection of personal data, on political finances, on media coverage or on the broadcasting of elections, that is, rules to ensure free, fair and clean elections, are violated.

85. While the second type of conduct does not constitute cybercrime per se, the evidence that such rules are broken often takes the form of electronic evidence. It is essential, therefore, that states provide their criminal justice authorities with the necessary powers to secure such evidence. Parties to the Budapest Convention are required to do so under Articles 16 to 21 that cover procedural law powers such as the expedited preservation of data, the search and seizure of computer systems and data, production orders and others.

86. A major problem is that data – and thus electronic evidence – is volatile and often held by service providers in foreign jurisdictions or stored in multiple, shifting or unknown jurisdictions, that is, "somewhere on servers in the cloud".[87] Attributing an attack, or simply identifying the user of an Internet Protocol (IP) address or the owner of a social media or email account is often not possible with reasonable effort. This is one of the reasons why cybercrime and other cyber threats to electoral democracy are rarely prosecuted.

87. Effective international cooperation and cooperation with service providers is warranted. The Budapest Convention in its current form includes detailed provisions on international cooperation combining expedited provisional measures to secure data (e.g. Article 29 on expedited preservation and Article 35 on 24/7 points of contact) with provisions on mutual legal assistance. These provisions are routinely used to investigate cybercrime.

---

[85] Korff, 2013, at http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168067f7f4

[86] The following information is based on a presentation by Alexander Seger (Executive Secretary, Cybercrime Convention Committee, Council of Europe) at the 15th European Conference of Electoral Management Bodies, Oslo, Norway, 19-20 April 2018.

[87] For detailed background information see the reports prepared by the Cloud Evidence Group on the Cybercrime Convention Committee, https://www.coe.int/en/web/cybercrime/ceg (last accessed 30 September 2018).

88. However, these do not sufficiently address the problem of cloud computing and related problems of jurisdiction or the fact that service providers in one state offer their services in many others without being legally or physically present or accountable in the latter.

89. For this reason, the Parties to the Budapest Convention have launched the negotiation of a 2nd Additional Protocol to permit added options for enhanced international cooperation and access to data in the cloud. Solutions under consideration include direct cooperation with service providers in other Parties, extending searches to computers in other jurisdictions in limited circumstances, or emergency mutual assistance. Negotiations are expected to last until the end of 2019.[88]

VI. Other international and national legislation, case law and initiatives[89]

A. International level

90. At the level of the United Nations, it was noted in the Joint Declaration on Freedom of Speech and Internet of 1 June 2011[90] that the approaches to regulation developed for other means of communication – such as telephone services or broadcasting – are very different to the ones needed for the internet, and such methods must be specifically designed for it. The more recent Joint Declaration, of 3 March 2017, now includes "fake news", disinformation and propaganda, and underlines the necessity to prioritise the freedom of speech, stating that the prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a)[91], and should be abolished.

91. Growing awareness of the need to prevent false news and to limit their spreading particularly during electoral periods has triggered initiatives ranging from research, education and cooperation to self-regulation and regulatory solutions, including at the international level. The NATO has set up a Stratcom Centre of Excellence, a think tank focusing on the impact of information domination on the internet and cyber defence. As a result of EU-NATO cooperation on hybrid threats, the European Centre of Excellence for Countering Hybrid Threats, was established in 2017.[92]

92. Several networks of people working together to fact-check online information exist, for example the International Fact-Checking Network (IFCN) works as a unit of the Poynter Institute that is dedicated to bringing together fact-checkers worldwide. The IFCN was created in 2015, to support and study the work of 64 fact-checking organisations from around the globe.

---

[88] See https://www.coe.int/en/web/cybercrime/t-cy-drafting-group .
[89] This report does not contain an exhaustive description of national material. See also CDL-AD(2019)016.
[90] Declaration signed by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 1 June 2011.
[91] States may only impose restrictions on the right to freedom of expression in accordance with the test for such restrictions under international law, namely that they be provided for by law, serve one of the legitimate interests recognised under international law, and be necessary and proportionate to protect that interest.
[92] See also the practical guide for the use of social media during elections which has been developed by the International Institute for Democracy and Electoral Assistance (International IDEA) for the benefit of electoral management bodies: Seema Shah, "Guidelines for the Development of a Social Media Code of Conduct for Elections", International IDEA, 2015. The guide is available at: https://www.idea.int/sites/default/files/publications/social-media-guide-for-electoral-management-bodies.pdf.

B. European Union

93. In January 2018, the European Commission set up a high-level group of experts (”HLEG") to advise on policy initiatives to counter “fake news” and disinformation which is spread online. In its Final Report,[93] the HLEG recommended a multi-dimensional approach based on five pillars designed to:

i) enhance transparency of online news;
ii) promote media and information literacy to counter disinformation;
iii) develop tools for empowering users and journalists to tackle disinformation;
iv) safeguard the diversity and sustainability of the European news media ecosystem; and
v) promote continued research on the impact of disinformation in Europe.

94. Building on the output of the HLEG, the European Commission has issued in April 2018 a Communication outlining the Commission’s strategy to tackle the problem of online disinformation.94 Such strategy does not foresee a regulatory intervention and has as main lines of actions: i) the development of an ambitious self-regulatory Code of Practice by leading actors of the market (including social networks, advertisers and other players of the advertising industry); ii) the strengthening of fact checking and monitoring capacity on disinformation; iii) the use of new technologies (e.g. artificial intelligence) for tackling disinformation; iv) the reinforcement of the election processes; and v) the fostering of education and media literacy.

95. The Code of Practice on Disinformation has been adopted in September 2018[95] with the view of protecting the upcoming EU elections. The Code is aimed at:

- ensuring transparency about sponsored content, in particular political advertising, as well as restricting targeting options for political advertising and reducing revenues for purveyors of disinformation;
- providing greater clarity about the functioning of algorithms and enabling third-party verification;
- making it easier for users to discover and access different news sources representing alternative viewpoints;
- introducing measures to identify and close fake accounts and to tackle the issue of automatic bots;
- enabling fact-checkers, researchers and public authorities to continuously monitor online disinformation.

96. The European Commission, through the research and innovation Framework Programme Horizon 2020 has also supported several innovation actions to develop new tools and services to help professionals and citizens in verifying online content (text, image and video). Moreover, it will create an independent European network of fact-checkers, who will be selected from the European members of the IFCN. The network will develop working methods, establish best practices, in order to achieve the broadest coverage for factual corrections. The Commission will give the network the online tools needed, a secure European online platform on disinformation, to help it achieve its goal. Through the Connect Europe Facility (CEF), the Commission will also support the deployment of a European platform on disinformation to increase the capacity to detect and analyse disinformation campaigns across Europe.

---

[93] See https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.
[94] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on “Tackling online disinformation: a European Approach”, COM(2018) 236 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=EN.
[95] Available at: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

97. In September 2018, the European Commission made specific recommendations with the aim to protect Europe's democratic processes from manipulation by third countries or private interests, and proposed new rules on election cooperation networks, online transparency, protection against cybersecurity incidents and steps to counter disinformation campaigns in the context of the European elections.[96] In December 2018, an Action Plan against disinformation[97] was adopted which is aimed at building up capabilities and strengthening cooperation between member states and EU institutions to proactively address the threats posed by disinformation. Attention is also drawn to the March 2018 Opinion by the European Data Protection Supervisor on online manipulation and personal data,[98] which recommends that data protection rules be completed and enforced, that regulators should aim for a collective diagnosis of the problem and cooperate across sectors, that self-regulation and codes of conduct be encouraged, and that individuals be empowered to exercise their rights including collective action.

98. Among already existing EU regulations, the following appear particularly relevant in the present context:

- The General Data Protection Regulation (GDPR)[99] which is directly applicable across the EU since 25 May 2018. Its provisions are mandatory and grant individuals numerous rights, including those to transparent communication, erasure (the right to be forgotten), and data portability (i.e. transfer from one data controller to another). The Regulation provides a general prohibition to process personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" with some exceptions, notably when "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". The rights established by the GDPR may be exercised and enforced not only by individuals but by organisations acting on behalf of individuals. To fill the protection gap from inadequate personal data processing outside of EU, the GDPR extends legal protection to the processing of personal data of EU data subjects "regardless of where the processing activities take place". This makes it applicable also to entities established outside the EU if they offer goods or services to individuals in the Union, or if they monitor their online behaviour. The regulation provides for strict rules on data transferring outside the Union; data processors must keep records of all processing activities. They are held responsible for adopting all necessary measures to guarantee that personal data is processed lawfully, fairly and in a transparent manner. The GDPR thus has the potential to prevent unauthorised personal data processing for electoral purposes, like in the case of Cambridge Analytica.[100]

---

[96] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Securing free and fair European elections", COM(2018) 637 final. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:637:FIN.

[97] See https://ec.europa.eu/digital-single-market/en/news/europe-protects-eu-steps-action-against-disinformation.

[98] Available at: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[99] Available at: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[100] For information on the implementation of the GDPR in different European countries, see: https://www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties/

- Regulation (EU) 2015/2120 laying down measures concerning open internet access,[101] applicable as of 30 April 2016, creates the individual and enforceable right for end-users in the EU to access and distribute internet content and services of their choice, and enshrines the principle of non-discriminatory traffic management. The enforcement of open internet rules within the EU is the task of national regulatory authorities which should respect the guidelines adopted by the body of European Regulators for Electronic Communications (BEREC) in 2016. Accordingly, it is not up to internet service providers to arbitrate the success or failure of the services and content distributed. The rules enshrine the principle of net neutrality into EU law and seek to prevent the blocking or throttling or discrimination of online content, applications and services.[102]

- Directive 2000/31/EC of the European Parliament and of the Council[103] contains liability exemptions available to certain online service providers including providers of 'hosting' services, on the condition that they act expeditiously to remove or disable access to illegal information that they store *upon obtaining actual knowledge thereof*. In this connection, it should be noted that the European Commission in several recent Communications stressed the need for online platforms to act more responsibly and step up EU-wide self-regulatory efforts to remove illegal content; on 1 March 2018, it adopted the Recommendation on measures to effectively tackle illegal online content[104] which is directed at member states and hosting service providers, and which is aimed at enhancing transparency and the accuracy of notice-and-action mechanisms.

C. Examples at the national level

99. Several States have recently adopted – or are planning to adopt – legislation to regulate online content and to counter politically loaded disinformation in their elections. Germany acted first[105] by obliging internet intermediaries (such as Facebook, Instagram, Twitter or YouTube) to promptly remove upon complaint any illegal content designated as such in the Criminal Code; obviously illegal content must be blocked or deleted within 24 hours. Offences range from hate speech and certain defamatory offences to content amounting to a threat to the constitutional order or national security, etc., which can have a direct impact on public debate and opinion especially during times of elections (the law is a general one, it is not specific to electoral campaigns). The Network Enforcement Act which took effect in the beginning of 2018 provides for fines up to € 50 million, which are applicable even if the offence was not committed in Germany.

100. In November 2018, the French Parliament adopted a law to combat manipulation of information[106] during electoral periods, which aims to identify and stop deliberate allegations of a false or misleading fact on an online platform in the three-month period before an election. Under the new legislation, platforms are subject to an obligation of transparency: they must give clear, correct and transparent information on their own identity and quality or of that of the third party for which it sponsors the content; they must also make public the amount received in exchange for sponsoring the content. A prosecutor, any person with legal interest in bringing the case before a judge on the basis of urgency, parties or candidates may complain about an

[101] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120.
[102] See https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality.
[103] Available at: Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031.
[104] Available at: https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.
[105] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) - Network Enforcement Act, https://germanlawarchive.iuscomp.org/?p=1245.
[106] Loi n° 2018 1202 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=EDB587F21F791D8941E5E11E82A0320A.tplgfr22s_1?cidTexte=JORFTEXT000037847559&categorieLien=id.

item of allegedly false or implausible deliberately, artificially and massively disseminated information online; this notion of artificial and widespread dissemination will be a clue for false information. A judge is obliged to rule on a case of this nature within 48 hours, and has the right to block the publication and to force the platform to stop this campaign. Technical intermediaries, who are persons offering access to communication services, have to promptly remove any illicit content brought to their attention and implement an easily accessible and visible mechanism for persons to notify them of any false news. Moreover, the French Regulatory Broadcast Authority has the right to refuse to sign a convention with a foreign country if the latter's activities could seriously upset the life of the nation by the dissemination of false news or violated pluralism of streams of opinion[107].

101. Russia[108], Singapore[109] and the Philippines have directly cited the German law as a positive example as they contemplate or have adopted legislation to remove "illegal" content online.[110]

102. The British Electoral Commission called on increasing transparency for voters with regard to the practice of digital electoral campaigns. It made recommendations about the responsibility of digital campaigns, spending on digital campaigns, transparency on payments for digital campaigns and enforcement of these rules.[111]

103. In the USA, the bipartisan Honest Ads Act presented in October 2017 before the US Congress[112] envisages disclosure and disclaimer rules to online political advertising. While television and radio have long been required to disclose the purchasers and content of all who purchase advertisements on their stations, internet companies have not. The Honest Ads Act would mandate that internet companies reveal the identities and content of advertisements related to elections or campaigns. Specifically, this would be done by amending a decades-old existing campaign finance law from 1971, by adding the phrase "paid internet or paid digital communication" to its list of media forms subject to the law. It would also require any website with at least 50 million monthly viewers - including Facebook, Google, and Twitter - to maintain a public list of any organisation or person who spends at least $500 in election-related advertisements. An exemption is made for "news story, commentary, or editorial" to ensure that the requirements are not levied on legitimate news reporting or opinion pieces.

---

[107] The French law has been the object of harsh criticism, see e.g. https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law. In the case of Germany, see e.g. https://www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590 and https://www.economist.com/europe/2018/01/13/germany-is-silencing-hate-speech-but-cannot-define-it .

[108] Federal Law "On information, information technologies, and protection of information" (of 27 July 2006, no. 149-FZ) was adopted on 18 March 2019. It penalises the spread of "unreliable socially important information" that could endanger lives and public health, raise the threat of massive violation of public security etc. This law permits to block the web-page containing such information. On the same day Federal Law no. 30-FZ(the "disrespect law") was adopted, adding Article 15-1-1 to the Federal Law "On information, information technologies, and protection of information" (of 27 July 2006, no. 149-FZ). It penalizes expression which "shows disrespect towards the society, the State, official State symbols … and organs of State power" and which is expressed in "obscene form". The Code of Administrative Offences was amended to introduce fines for publications containing "obscene disrespect" and "fake news".

[109] https://techcrunch.com/2019/05/09/singapore-fake-news-law/?renderMode=ie11&guccounter=1&guce_referrer_us=aHR0cHM6Ly90ZWNoY3J1bmNoLmNvbS8yMDE5LzA1LzA5L3NpbmdhcG9yZS1mYWtlLW5ld3MtbGF3Lw&guce_referrer_cs=oKT9smcHtaNhdWGcU8VGvg; https://mediawrites.law/fake-news-law-passed-in-singapore-protection-from-online-falsehoods-and-manipulation-act/

[110] See https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law .

[111] See https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf .

[112] https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%2C%22search%22%3A%22Honest%20Ads%20act%22%7D&searchResultViewType=expanded.

104. In some countries, specialised units to combat information disorder have been or are being created, for example:

a) In the United Kingdom it is planned to set up a national security communications unit to tackle "fake news" disinformation.
b) In the Czech Republic, the Centre Against Terrorism and Hybrid Threats, part of the Interior Ministry, it is a specialised analytical and communications unit that monitors threats directly related to internal security, which implies a broad array of threats and potential incidents relative to terrorism, soft target attacks, security aspects of migration, extremism, public gatherings, violation of public order and different crimes, but also disinformation campaigns related to internal security. It also develops proposals for substantive and legislative solutions that it also implements where possible and disseminates information and spread awareness about the given issues among the general and professional public.

105. Cooperation among electoral authorities, academics and practitioners has been fostered in Brazil in order to assess the true impact and efficiency of adopted measures, through the Advisory Council for Internet and Elections that advises the Electoral Tribunal. Panama and Mexico[113] are examples of countries where operators and platforms have been cooperating with electoral authorities in order to detect threats and to spread official information.

106. Fact-checking[114] has been developing in many countries[115] and in some of them, networks of fact-checkers have been set up; an interesting example is "#Verificado2018", a group of journalists, civil society and academic partners that sought to debunk viral misinformation, fact check politicians' claims and combat fake news for the 2018 electoral federal process in Mexico. Spain also established a special fact-checking unit during the last elections.[116]

VII. E-Challenges to democracy and human rights

107. The holding of democratic elections, hence the very existence of democracy are impossible without respect for human rights, particularly the freedom of expression and of the press and the freedom of assembly and association for political purposes, including the creation of political parties. Respect of these freedoms is vital particularly during election campaigns. Restrictions on these fundamental rights must comply with the European Convention on Human Rights and, more generally, with the requirement that they have a basis in law, are in the general interest and respect the principle of proportionality. Clear criteria for balancing the competing rights should be set out in the legislation and effectively implemented through electoral and ordinary justice mechanisms.

108. Several specific notions of democracy are affected by the use of digital technologies. First, new information technologies - the electronic vote and the formation and actualisation of centralised registers of voters for example - make an impact on *electoral democracy*, understood as the institutional activities and infrastructure that make elections possible, and commonly known in the internet context as "e-government". Second, the internet and new information technologies have the potential to allow for greater transparency and accountability, as well as for broader and more efficient forms of political participation, extending the reach of

[113] INE (Instituto Nacional Electoral) of Mexico, during the preparation of the 2018 elections, entered into co-operation agreements with Facebook, Twitter and Google; see INE, Democracia en riesgo, Elecciones en tiempos de desinformación, Estrategia y acciones implementadas para enfrentar la desinformación deliberada en las elecciones mexicanas de 2018.
[114] Cf. Lazer et al., 2018.
[115] See e.g. the Appendix of the CoE Information Disorder Report 2017 which lists European fact-checking and debunking initiatives. See also https://reporterslab.org/fact-checking/.
[116] https://elpais.com/politica/2019/03/10/actualidad/1552243571_703630.html.

the "public sphere"; in this sense, they impact on *deliberative democracy*, which refers to participation by individuals in open debate in the belief that it will lead to better decisions on matters of common concern".[117] Finally, to the extent that these technologies facilitate a process whereby large disorganised groups of people organise and act to address specific social, economic or political issues, they may be seen as having an influence on the so-called "*monitory democracy", defined as "*the public accountability and public control of decision makers, whether they operate in the field of state or interstate institutions or within so-called non-governmental or civil society organisations, such as businesses, trade unions, sports associations and charities".[118] To the extent that the citizens' capacity to survey and self-organise for political purposes depends both on the information they can access and on their possibilities to deliberate and agree on a common agenda, the monitory democracy variables may be considered as embedded in the deliberative democracy category.

A. Challenges to electoral democracy

109. As mentioned earlier, the concept "*electoral democracy"* refers to the institutional activities and infrastructure that make elections possible. From the organisation of the election itself, to the creation and administration of voters' registers or the implementation of electronic ballots and internet voting, the electoral aspect of democracy sets the material and institutional conditions necessary to translate the popular suffrage into the appointment of representatives or the approval of laws and public policies. The proper maintenance of electoral registers, for example, is crucial to the realization of the principle of universal suffrage; the strict observance of the voting and counting procedures is crucial to the realization of the principle of free suffrage.

110. If on the one hand the use of digital technologies may make democratic processes more accessible to all citizens, it may also bring about obstacles to the exercise and development of electoral democracy, entailing new forms of undue interference with the right to vote and the right to stand for election (Article 3 of Protocol 1 ECHR), the right to freedom of expression (Article 10 ECHR) and the right to respect for private life (Article 8 ECHR).

111. According to the Communications Security Establishment (CSE) of the Government of Canada, "[a]dversaries worldwide use cyber capabilities… against elections… to suppress voter turnout, tamper with election results, and steal voter information… against political parties and politicians... to conduct cyberespionage for the purposes of coercion and manipulation, and to publicly discredit individuals… [and] against both traditional and social media… to spread disinformation and propaganda, and to shape the opinions of voters".[119] Furthermore, the CSE

---

[117] Laidlaw 2015, p. 10-11.

[118] John Keane, The Life and Death of Democracy,2009. The definition of "monitory democracy" is given at http://thelifeanddeathofdemocracy.org/glossary/monitorydemocracy/.

[119] CSE 2017. We have seen several examples of these interventions around the world:

- "In June 2016, the US state of Arizona shut down its voter registration system for nearly a week after adversaries attempted to gain access to the system. The next month, in Illinois, the state election agency took down its website for two weeks after discovering tens of thousands of voter records (e.g. names, addresses, and driver's licence numbers) were suspected to have been viewed by the adversaries" (Nakashima, as referred by the CSE).
- "Responding to perceived software vulnerabilities in its vote tabulation machines and warnings that the election may be targeted by Russia, the Netherlands amended voting procedures in their most recent election. To avoid the possibility of adversaries interfering with the election, all votes were hand-counted" (Escritt, as referred by the CSE).
- "In December 2016, adversaries gained access to the website of Ghana's Central Election Commission during the general election as the votes were being counted. An unknown adversary tweeted fake results that the incumbent candidate had lost. The electoral commission then sent out its own tweets claiming these results to be false. While the outcome of the election was not altered, this incident served to sow confusion in the minds of many voters" (BBC News, as referred by the CSE).
- "In the last US presidential election, both major political parties were subjected to cyberespionage attempts by Russia. Russian operatives used cyber capabilities to gain access to the emails of key political staff

estimates that "it is highly probable that cyber threat activity against democratic processes worldwide will increase in quantity and sophistication" over the next years for the following reasons:[120]

- *Many effective cyber capabilities are publicly available, cheap, and easy to use.*
- *The rapid growth of social media, along with the decline in longstanding authoritative sources of information, makes it easier for adversaries to use cyber capabilities and other methods to inject disinformation and propaganda into the media and influence voters.*
- *Election agencies are, increasingly, using the internet to improve services for voters. As these services move online, they become more vulnerable to cyber threats.*
- *Deterring cyber threat activity is challenging because it is often difficult to detect, attribute, and respond to in a timely manner. As a result, the cost/benefit equation tends to favour those who use cyber capabilities rather than those who defend against their use.*
- *Finally, there is a dynamic of success emboldening adversaries to repeat their activity, and to inspire copycat behaviour."*

112. The Council of Europe Convention on Cybercrime ETS 185 of 2001 ("Budapest Convention") and the current work on a 2nd Additional Protocol to this treaty show that many states have understood the risks.[121]

113. From a cybercrime perspective, threats to electoral democracy may involve at least two types of interference. One type is attacks against the confidentiality, integrity and availability of election computers and data, including:

- compromising voter databases or registration systems, for example, through hacking of computer systems or deleting, altering or adding data;
- tampering with voting machines to manipulate results;
- interfering with the functioning of systems (for example, a distributed denial of service attack on election day);
- illegally accessing computers to steal, modify or disseminate sensitive data such as, for example, the theft of data from election campaign computers for use in information operations.

114. Such attacks clearly represent forms of cybercrime as defined in the Budapest Convention on Cybercrime, such as illegal access to computer systems (Article 2), illegal interception (Article 3), data and system interference (Articles 4 and 5) and others. The currently more than sixty Parties to this treaty have transposed these provisions into their domestic law.

115. As mentioned earlier, these attacks amount to an interference with several fundamental rights guaranteed by the ECHR and other international human rights instruments. They may be

---

working on the Democratic Party campaign. The emails were subsequently leaked to embarrass the Democratic Party candidate" (ODNI, as referred by the CSE).

- "According to media reports, French intelligence believes that social botnets were used to influence the presidential election. Certain social media accounts, the same ones that were active during last year's US election, were promoting false and defamatory information against a leading candidate. In the final days of the election, one party was also victimised by the unauthorised release of thousands of campaign-related emails" (Auchard, as referred by the CSE).
- "Cyberwarfare, once a largely hypothetical threat, has become a well-documented reality, and attacks by foreign states are now a credible threat to a national online voting system. As recently as May 2014, attackers linked to Russia targeted election infrastructure in Ukraine and briefly delayed vote counting" (Springall *et al.* 2014).

[120] CSE 2017.

[121] "Cybercrime in the election process: the role of the Budapest Convention", http://www.venice.coe.int/files/15EMB/Alexander_Seger.pptx

carried out by governments, political parties/candidates, foreign powers and private actors. In this respect, it needs to be stressed that under the ECHR states have a positive obligation to ensure free and secure elections and to guarantee human rights such as the right to private life and the freedom of expression.

116. A second type of attack involves (dis-)information operations – which do not constitute cybercrime but violate the rules on the protection of personal data, on political finances, on media coverage or on the broadcasting of elections, that is, rules to ensure free, fair and clean elections. The evidence that such rules are broken often takes the form of electronic evidence, that is, it is evidence found on computer systems. It is essential, therefore, that states provide their criminal justice authorities with the necessary powers to secure such evidence. Parties to the Budapest Convention are required to do so under Articles 16 to 21.

117. International standards indeed point to a responsibility of the States to prevent inequality in media coverage of electoral campaigns and to ensure that citizens are informed on political parties in order to make an informed free political choice of their representatives. In addition to their obligations not to unduly interfere with the enjoyment of fundamental rights, States also have positive obligations to prevent that violations be committed by third parties. A fair balance needs to be provided by conflicting rights. The undue use of the voters' registry data for electoral purposes or the excessive disclosure of a candidate's personal information in the heat of a political campaign are common scenarios of such conflicts. Most democracies would deem the first scenario as a clear violation of the right to privacy and a breach to electoral equity, even if political parties have the right to access such information. It may be argued however that the nature of the democratic debate would allow for an extended permissiveness of the political right of expression over the candidate's right to privacy, provided that those expressions do not clearly constitute defamation or slander. Contemporary democracies are used to these scenarios and have produced a rather abundant set of rulings and national legislation on the matter.

118. For at least two decades, several countries have experimented with internet voting to strengthen political rights. For instance, in the year 2000, Switzerland launched the project "vote électronique" to test its reliability. Since then, the country has conducted more than 150 trials at the federal level and some cantons have made e-voting available for their citizens. In 2008, Norway also started testing internet voting and made some trials during the 2011 municipal elections and the 2013 parliamentary elections. In Canada, internet voting is available in some provinces (Ontario and Nova Scotia) since 2003. Perhaps the most successful experiment has been carried out by Estonia, where discussions about internet voting began in 2001 and since 2005 it has been considered as an additional and legally binding form of voting.[122]

119. Notwithstanding the success of some trials, the use of the internet for casting votes has raised several security concerns. "Estonia was the first country in the world to use internet voting nationally, and today more than 30% of its ballots are cast online", but researchers from the University of Michigan and the Open Rights Group have found "that the [Estonian] I-voting system has serious architectural limitations and procedural gaps that potentially jeopardise the integrity of elections" to the extent that "attackers could target the election servers or voters' clients to alter election results or undermine the legitimacy of the system." Their concerns were such that they concluded that "[s]omeday, if there are fundamental advances in computer security, the risk profile may be more favorable for internet voting, but we do not believe that the I-voting system can be made safe today".[123]

120. In this context, it should be stressed that it may be that misinformation and blanket digital interference with political discourse is aimed not a subverting the mechanics of the

[122] ACE Project 2018.
[123] Springall *et al.* 2014.

election itself but rather at undermining public trust in the process and public trust in the political system. The openness of a liberal democracy is a strength but also a vulnerability. Digital technologies should not be allowed to sap the confidence of the public in the electoral process, hence the necessity of reassuring the public about the security of such technologies. To this end, digital technologies should be introduced gradually and may be combined with traditional methods. Innovation cannot come at the cost of legal requirements, including security.

121. These challenges need to be addressed from an interdependent stance, which means to that (1) the transnational nature of the problem and (2) the essential role played by the gatekeepers of information highways (i.e. internet service providers) to investigate and prosecute cybercrimes must be recognized. The international framework needs to be strengthened in order to establish more efficient mechanisms of transnational cooperation among nations and private actors, and, if possible, to procure a greater uniformity among national legislations. In the end, the solution seems to be "to adapt the constitutional framework of modern democracies" to the new electronic environment in which cybercrime thrives and in which governments, corporations and citizens interact and make democracies possible.[124]

B. Challenges to deliberative democracy

122. The principle of free suffrage is grounded on the freedom of voters to form an opinion. This freedom, which partly overlaps with equality of electoral opportunity, requires the state, and public authorities generally, to honour their duty of even-handedness, particularly where the use of the mass media, billposting, the right to demonstrate on public thoroughfares and the funding of parties and candidates are concerned.[125] The freedom to form an opinion includes the right to be correctly informed before making a decision, the right to private online browsing and the right to make confidential communications on the internet. The monitoring of people's online activity without their consent and for the purpose of understanding and exploiting their behavioral paths undermines these rights.

123. Technology is changing the way electoral campaigns are managed. The internet is a powerful platform for political parties to present their agenda to the electorate and to mobilise a larger support base for their causes. The cost of communicating with voters can be substantially lower via this medium than via broadcast media, given the availability of free blog and video sharing platforms and social media. Small political parties with limited resources and independent candidates in particular can benefit from this type of communication.

124. However, the changes in the production and consumption of election-related content pose challenges for established institutions and principles of regulation of election communications such as freedom of association, spending limits and regulation of political advertising. They undermine the ability of existing regulation to maintain the level playing field in electoral communication between new and established, rich and poor, corporate and civil society campaigns. New intermediaries and platforms now occupy the important gatekeeper positions once occupied by journalists, but have not yet adopted the ethical obligations of the media. This presents a threat to elections and potential for corrupt practices to emerge. The CoE Election Study 2017 identifies a number of concerns for the fairness and legitimacy of electoral processes, such as the lack of transparency of campaigning, spending, messages and algorithms used in digital advertising, large-scale invasions of privacy, lack of journalism filter to fact-check political messages, the increased amount of disinformation, and lacunas in electoral campaigning regulation (e.g. impossibility to enforce silence periods), and which concludes that

[124] Mecinas Montiel 2016, p. 427.
[125] Venice Commission, Code of good practice in electoral matters, explanatory report, Free suffrage.

"the current regulatory framework no longer suffices for maintaining a level playing field for political contest and for limiting the role of money in elections."[126]

125. Traditional electoral campaigning is being challenged by new forms of communication channels which are not only a help in spreading a message at a low cost but also make use of specific marketing techniques that best adapt to specific sections of the electorate. Mechanisms such as the use of personalized ads and messages, which are applicable to any field of digital marketing, have been recently used in the electoral arena providing some actors who have access to these mechanisms with a non-transparent advantage. Electoral messages have thus become increasingly personalized. Those who design campaigns do not have to think about the majority of the electorate who have already their mind set on how to cast their vote. As such, they can concentrate on small groups of swing voters. The new campaign techniques provide with the possibility of tailored electoral messages somewhat disguised as general, politically neutral messages. Exercising such hidden influence is facilitated by the use of social platforms, not only because of their data processing algorithms but mainly because they provide with the possibility of directly targeting specific groups of profiles with personalized ads and messages, while the targeted users do not detect the personalisation. With the aid of technology, campaigning techniques have shifted to an evolutionary concept of the one to one or the many to many approach: this is what Joseph Pine calls "mass customization".[127] Unlike the traditional mass media, which in principle have a declared political colour which is known to the reader, internet providers do not have a declared political line, so that in the absence of a clear indication that the information provided by them is in fact a partisan political ad, the users may be under the impression that such information is politically neutral.

126. The manipulation of electoral preferences has been examined by Rob Epstein, and more particularly the influence of search engines rankings (especially Google for its predominance) on voting preferences (referred to as Search Engine Manipulation Effect, SEME).[128] According to a 2015 study, higher-ranked items connected with web pages that favor one candidate, have an impact on the opinions of undecided voters.[129] Evidence from five experiments in two countries suggests that "(i) biased search rankings can shift the voting preferences of undecided voters by 20% or more, (ii) the shift can be much higher in some demographic groups, and (iii) such rankings can be masked so that people show no awareness of the manipulation." The authors of the study conclude that "if Google favours one candidate in an election, its impact on undecided voters could easily decide the election's outcome." While the results of this study may need to be corroborated by further research, one might concur with the authors' conclusion that it is "even more disturbing" that "the search-ranking business is entirely unregulated".

127. In this context, it should be borne in mind that search engine rankings are a product of complex algorithms and are not necessarily manipulative in design, but are in fact aiming to provide the most topical, relevant and new results; however, the algorithms can be manipulated by different websites trying to acquire better rankings. In reality, we see that happening, and Google is constantly improving the search algorithm to prevent such intrusions. In any case, whether manipulation is intentional or not, the SEME entails two important consequences for

[126] CoE 2017 Election Study; See also the 2018 report on "Disinformation and electoral campaigns" (Doublet, 2018, CDDG(2018)11), which suggests the preparation by the Council of Europe of a broad Programme of Action in this area. It recommended, for example, defining the length of electoral campaigns to avoid the risk of significant digital campaigns before the electoral campaign period; requiring imprints of digital material to know who is behind online platforms; obtaining disclosure of spending made on digital electoral campaign activity by online platforms; banning funding of digital electoral expenditure by a foreign physical or legal person.
[127] PINE, B.J., II. (1993). Mass Customization: The New Frontier in Business Competition. Harvard Business School Press, Boston.
[128] Epstein 2016.
[129] Epstein and Robertson 2015.

democracy: the power to manipulate preferences could be used by private or public actors to affect electoral equity; and the fact that search-engine users are unaware of the criteria (coding) of the ranking mechanisms hinders their capacity to make fully informed decisions, and therefore to exert their freedom of expression.

128. The SEME is not exclusive of online search engines. Social media platforms are also governed by an underlying coding architecture that is not unbiased. Companies like Facebook, Twitter or Instagram, unlike the traditional media, are not politically oriented; they are primarily motivated by commercial interests and design their coding structure according to those interests. In this sense, the algorithms that govern social media foster a partial and sometimes illusory comprehension of politics and democracy, because they provide biased information that reflect the partial interests and behaviour of their users.[130]

129. Indeed, social media and search-engine companies can shape online social interactions not only because they have the power of coding the environments of such interactions, but also because of their capacity to profile ("profiling") and predict their user's attributes and behaviours. These companies can easily access "digital records of behaviour, such as Facebook Likes, browsing histories, search queries, or purchase histories can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender".[131] Furthermore, these architects can process such information to create highly accurate profiles of their users, predict their preferences, and even target them with individualised data and advertising in order to promote or discourage specific behaviours.[132]

130. On one side, companies like Facebook or Google commoditise their users' information and sell them in the market. Buyers, on the other side, use such information with little or no accountability to influence consumers and sometimes voters, through "tailored ads based on personal data".[133] That was exactly the case of Cambridge Analytica. The current business model for many websites offers content in exchange for personal data. The fact that people give away their personal information in exchange for free services enables widespread data collection by the websites which may lead to their use and misuse by various actors.

131. Even if it is true that social media users must explicitly accept the general privacy conditions imposed by the social media companies, they have little or no control on who is authorised to "buy" their personal information, or to what uses it should be put. This situation undermines the fundamental right to privacy and personal data protection, because it curbs the user's capacity to impose limits on the use of his/her personal information.[134] In the ruling 292/2000, the Constitutional Tribunal of Spain established that "the fundamental right to the protection of personal data… grants the incumbent with a set of powers to impose on third parties the duty to perform or refrain from performing specific behaviours, which grants the individuals with the power to decide over their data… [a useless power] if the incumbent has no

---

[130] Van Dijck 2013; McChesney 2013.
[131] Graepel *et al*. 2013.
[132] For instance, according to an account by Robert Epstein (2016):
"… a study by Robert M Bond, now a political science professor at Ohio State University and others, published in Nature in 2012, described an ethically questionable experiment in which, on election day in 2010, Facebook sent 'go out and vote' reminders to more than 60 million of its users. The reminders caused about 340,000 people to vote who otherwise would not have. Writing in the New Republic in 2014, Jonathan Zittrain, professor of international law at Harvard University, pointed out that, given the massive amount of information it has collected about its users, Facebook could easily send such messages only to people who support one particular party or candidate, and that doing so could easily flip a close election – with no one knowing that this has occurred. And because advertisements, like search rankings, are ephemeral, manipulating an election in this way would leave no paper trail."
[133] Christopher Wylie, as quoted by Guimón 2018.
[134] Davara 2003, p. 43-44.

knowledge of what information is in the hands of third parties, who are those parties, and to which use will the information be put."[135]

132. The use and abuse of personal data for electoral purposes, cloaked as freedom of commerce, might pose a serious threat to free elections and electoral equity at least in three aspects: first, because private actors might use such information to directly exert undue influence on the electoral competition; second, because internet and social media companies, arguing freedom of commerce, might restrict the access to such information according to their political preferences, hence granting an opaque advantage to some parties or candidates over others; and third, because the commoditisation of personal data represents a challenge to the surveillance of money in political campaigns.

133. The risk to undermine the rights to privacy, free elections/electoral equity and freedom of expression and opinion – and, as some experts argue, even freedom of thought – suggests a need to regulate the commercial rights of internet and social media companies. That said, to completely forbid the "commoditisation of information" would also hinder the development of the internet and, consequently, the access to an apparently limitless source of political information and democratic action. As long as societies do not find new forms to finance the internet, to impose excessive limits on the commoditisation of personal information could curtail fundamental political rights such as freedom of expression and freedom to organise political action. The paradox is that the same technologies that have enhanced the possibilities of expression, are the ones that curtail such possibilities.[136]

134. On the one hand, the right to access the internet is a necessary condition for the full exercise of freedom of expression, which is a necessary condition for the existence of a democratic society.[137] On the other hand, the internet itself poses different sets of threats to democracy. As social media and the internet are not (and should not be) a space located outside legal parameters,[138] there is an urgent need to find solutions to these conflicts of rights that allow for a reasonable protection of privacy, political and commercial rights.

---

[135] As referred by Davara 2003. Own translation.

[136] In the words of Laidlaw (2015, p. xi-xii):*"[T]he communication technologies that enable or disable participation in discourse online are privately owned…Thus, we inevitably rely on these companies to exercise the right to freedom of expression online, and they thereby become gatekeepers to our online experience…*
Our reliance on these gatekeepers to exercise the right to free speech has had two effects. First, such gatekeepers have increasingly been the target of legal measures designed to capitalise on their capacity to regulate third-party conduct… Second, …speech regulation in cyberspace has largely been left to self-regulation, in much the same way that regulation of the internet in general has been light-touch…. The result is a system of private governance running alongside the law, without any of the human rights safeguards one normally expects of state-run systems, such as principles of accountability, predictability, accessibility, transparency and proportionality".

[137] *Lingens v. Austria*, Application no. 9815/82 (ECtHR, 8 July 1986): "freedom of expression, as secured in paragraph 1 of Article 10 (art. 10-1), constitutes one of the essential foundations of a democratic society". Furthermore, in the case of *Ahmet Yıldırım v. Turkey* (Application no. 3111/10, 18 December 2012), the ECtHR has ruled that internet blocking may be "in direct conflict with the actual wording of paragraph 1 of Article 10 of the Convention, according to which the rights set forth in that Article are secured 'regardless of frontiers'".
See also Laidlaw (2015, p. 19-21):
"Democracy has always been embodied in the practices of communication, and freedom of expression has consistently been identified by the courts as central to democracy. In Lingens v. Austria, the European Court of Human Rights (ECtHR) famously commented that freedom of expression 'is one of the essential foundations of a democratic society'…
Many states, such as Estonia, Finland, France, Greece and Spain, have legislatively recognised internet access as a fundamental right. In 2003, the Committee of Ministers of the Council of Europe adopted a Declaration affirming the importance of freedom of expression on the internet. Since 2010, we have seen a paradigm shift at an international level in the recognition of human rights in the cyberspace. Access to the internet as a fundamental right received the United Nations (UN) stamp of approval in a report by Frank La Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression… This was followed up in 2012 by the UN Human Rights Council passing a resolution affirming internet freedom as a basic human right, in particular the right to freedom of expression".

[138] Electoral Tribunal of Mexico, g.

135. The lack of or insufficient regulation of the Internet and social media has left users with no legal recourse to protect their data and, most of all, their freedom of expression and democratic rights. On the one hand it is problematic when private technology companies are censoring content which they consider "harmful", without them being accountable and their measures being transparent.

136. On the other hand, the positive responsibility of the state to prevent undue interference by third parties must not lead to undue state intervention, through excessive or undue regulation which can result in undermining the very rights that it is meant to protect. Unjustified state surveillance of private communications and the different ways in which online platforms may be used so as to – intentionally or accidentally – affect the flow of information, directly curb the freedom of expression, hinder democratic dialogue, and infringe the principles of institutional neutrality and electoral equity. While it is understandable, in the context described above, that currently many states have on their agenda to tackle the issue of "fake news" with legislation, this may pose a threat to the fundamental right of freedom of expression and information – bearing in mind that exaggerated speech enjoys protection under international human rights standards such as Article 10 ECHR. Enabling the authorities to interfere with the public discourse may be abused to silence dissidents and prevent discussion which challenges mainstream thought and restricting criticism of societal attitudes. As the Venice Commission emphasised, "the mass media are not the only category that should be entitled to a high level of freedom of expression. Thus, persons who impart information and ideas on matters of public interest and contribute to the public debate on such matters, including members of campaign groups and elected representatives, should be allowed a high level of freedom of expression, including a certain degree of exaggeration and even provocation as long as they act in good faith and exercise due diligence in order to provide accurate and reliable information".[139]

137. The filtering, blocking and take-down of illegal content on the internet in order to combat notably hate crimes and national security, as well as to protect intellectual property and privacy or defamation rights are a necessary but delicate exercise which however may be abused and result in censorship and in illegitimate silencing of political opponents. Any such measures must be in accordance with the law, which includes a precise and narrow definition of the offences in cause,[140] and it must pursue one of the legitimate aims listed in Article 10 ECHR. The criteria of necessity in a democratic society and proportionality must always be respected.[141] Effective judicial review by independent and impartial courts must be guaranteed.

138. As regards "fake news", most of which do not fall under any of the categories that would allow prosecution, alternative means need to be employed, such as fact-checking (which, while not a panacea, is becoming more advanced and effective), media literacy programmes aimed at sensitisation about the problem and recognition of false content, and investments in quality journalism.[142] In this endeavour, state authorities will need the cooperation of both citizenry and internet corporations.

139. At the same time, it must be stressed that any measures to address the information disorder must be designed with great care, so as not to undermine the "net neutrality". This is the founding principle of the internet, whereby ISPs are to treat all online data equally and provide the conditions for unfettered user access, without discrimination based on content or

[139] CDL-AD(2013)024, Opinion on the legislation pertaining to the protection against defamation of the Republic of Azerbaijan, para. 37.
[140] See for example Venice Commission, Opinion the Federal law on combating extremist activity of the Russian Federation, CDL-AD(2012)016.
[141] See for example Venice Commission, Opinion on law no. 5651 on regulation of publications on the internet and combating crimes committed by means of such publication ("the internet law") of Turkey, CDL-AD-2016)011.
[142] Cf. the CoE Information Disorder Report 2017 which offers more than 30 recommendations for different stakeholders.

source. Protecting the democratic function of the internet from being monopolised by private corporate power calls for the equal treatment of all data sent and received without differential charges and service quality.[143] Abolishing the policy of "net neutrality", as the United States Federal Communication Commission agreed to do in December 2017,[144] allows ISPs to block or throttle (slow down) websites and charge for faster download and upload speeds. In such circumstances, online services, applications, and websites can be granted preferential treatment for any number of reasons, be they commercial or ideological – including in less democratic countries where ISPs are state-owned and censored, and where authorities may be tempted to give faster lanes of access to pro-government outlets.

140. To conclude, while excessive or inadequate regulation of the internet might be counterproductive and hinder the accessibility and development of the internet and, consequently, the freedom of expression and the democratic dialogue itself, the problem of disinformation disorder cannot be left unattended. The risk to undermine the rights to privacy by the misuse of personal information, and the damages to freedom of expression and electoral equity produced by the architecture of the internet (i.e. SEME, epistemic bubbles, echo chambers and fake news), along with the lack of regulation which has left citizens with no efficient legal recourse to protect their personal and political rights, are situations that call for urgent action.

141. Such action must include the powerful private actors who, while motivated by primarily commercial interests, have the power to hamper human rights, while maintaining an essential platform for democracy, and must recognise such responsibility.

VIII. Conclusions

142. The holding of democratic elections, hence the very existence of democracy, is impossible without respect for human rights, particularly the freedom of expression and of the press and the freedom of assembly and association for political purposes, including the creation of political parties. Respect of these freedoms is vital particularly during election campaigns. Restrictions on these fundamental rights must comply with the European Convention on Human Rights and, more generally, with the requirement that they have a basis in law, are in the general interest and respect the principle of proportionality. Clear criteria for balancing the competing rights should be set out in the legislation and effectively implemented through electoral and ordinary justice mechanisms.

143. The relationship between democracy and digital technologies is quite complex. On the one hand, the internet and social media have become the dominant platform of political interaction in some democracies, the use of those tools have strengthened the critical attitudes of citizens towards their governments and their widespread use facilitates the organisation of large-scale social movements and a closer interaction between citizens and political parties. On the other hand, the new virtual tools may be used, and sometimes are indeed used against elections to suppress voter turnout, tamper with election results, and steal voter information; against political parties and politicians to conduct cyber espionage for the purposes of coercion and manipulation, and to publicly discredit individuals; and against both traditional and social media to spread disinformation and propaganda, and to shape the opinions of voters. The new digital realm allows for new forms of criminality and data commercialisation that seriously threaten privacy rights, and modulates social interactions by selectively (and sometimes

[143] From the perspective of both constitutional law and international human rights law it is crucial to take into account the reality of the influential actors outside the elected authorities preventing the realisation of fundamental rights. See Thorgeirsdóttir, Herdis (2005), *Journalism Worthy of the Name: the Affirmative Side of Article 10 of the ECHR*, Kluwer Law International.

[144] The net neutrality regulations enacted in 2015, which sought to stop the ISPs giving preferential treatment to sites and services that paid them to accelerate their data, officially expired in June 2018.

strategically) feeding or hiding specific information to its users, thus fostering a partial understanding of reality and hampering freedom of expression.

144. The internet-based services have enriched and diversified news sources, facilitating individuals' access to information and their decisions on the most crucial matters in democracy, notably on the choice of their legislature. However, at the same time, information disorder – misinformation, disinformation and malinformation – may distort the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their votes. This environment potentially undermines the exercise of the right to free elections and creates considerable risks to the functioning of a democratic system.

145. The small number of very powerful private actors that literally own the information highways have own commercial interests and rights that tend to collide with both civil and political rights and electoral principles. These internet providers have taken up the gatekeeping role which originally belonged to the traditional media, without however having adopted the ethical obligations of the media. Private technology companies are thus censoring content which they consider "harmful", without them being accountable and their measures being transparent. It is true that social platforms have recently adopted a series of measures for preventing false news and limiting their spread particularly during electoral periods. There is a concept of corporate social responsibility, some sort of self-regulation for businesses with the primary goal of "doing no harm" and abiding by the rule of law and human rights principles, including the right to a remedy for their users, and being liable for their products (under commercial law, competition law, environmental law, etc.).[145] However, this is done on a voluntary and unregulated basis, without a recognised rule of law based framework .

146. While states have a positive responsibility to prevent undue interference with civil and political rights by third parties, undue state intervention through excessive or undue regulation can result in undermining the very rights that it is meant to protect. Unjustified state surveillance of private communications and the different ways in which online platforms may be used so as to – intentionally or accidentally – affect the flow of information, directly curb the freedom of expression, hinder democratic dialogue, and infringe the principles of institutional neutrality and electoral equity. Enabling the authorities to interfere with the public discourse may be abused to silence dissidents and prevent discussion which challenges mainstream thought and restricts criticism of societal attitudes. In particular, the filtering, blocking and take-down of illegal content on the internet in order to combat notably hate crimes and to protect national security, as well as intellectual property and privacy or defamation rights must be in accordance with the law, which includes a precise and narrow definition of the offences in cause, and it must pursue one of the legitimate aims listed in Article 10 ECHR. The criteria of necessity in a democratic society and proportionality must always be respected. Effective judicial review by independent and impartial courts must be guaranteed.

147. As regards "fake news", alternative means need to be employed, such as fact-checking, media literacy programmes aimed at sensitisation about the problem and recognition of false content, and investments in quality journalism.

148. At the same time, it must be stressed that any measures to address the information disorder must be designed with great care, so as not to undermine the principle of "net neutrality". The internet should remain an open platform.

---

[145] Facebook, Google and Twitter are signatories to the Code of Practice against disinformation and have committed to report monthly on measures taken ahead of the European Parliament elections in May 2019: see the April reports on the implementation of the Code of Practice, https://ec.europa.eu/digital-single-market/news-redirect/651264.

149. To face these challenges, several measures need to be ensured from an interdependent and global perspective, notably:

As regards electoral democracy:

A. Criminalise cyber-attacks against the confidentiality, integrity and availability of election computers and data in pursuance of the Budapest Convention on Cybercrime:
B. Provide the criminal justice authorities with the necessary powers to secure electronic evidence of violations of rules on protection of personal data, on political finances, on media coverage or on the broadcasting of election;
C. Prepare national Electoral Management Bodies (EMBs) for emergency situations and have in place crisis management organization; EMBs should be provided with adequate resources and training to adopt digital technologies and address the related cybersecurity risks;

As regards deliberative democracy:

D. Recognise (1) the transnational nature of the problem and (2) the essential role played by the internet intermediaries (i.e. internet service providers, and search-engine and social media companies);
E. Strengthen the international framework (1) to establish more efficient mechanisms of transnational cooperation among nations and private actors, and, if possible, (2) to procure a greater uniformity among national legislations;
F. Work on a regulatory and adjudicatory model based on the co-responsibility of private and public actors, and on multiple regulatory and conflict-resolution approaches. Such model might include at least four strategies, all of them able to constantly adapt to the ever-changing environment of the internet and communication technologies:

- Promote further research and cooperation among electoral authorities, academics and practitioners in order to assess the real impact of digital technologies on electoral processes and the efficiency of the adopted measures;
- Foster education to strengthen legal and democratic culture among citizens;
- Promote self-regulation, like the mandatory adoption of ethics and corporate social responsibility codes, among internet service providers, and search-engine and social media companies; and
- provide remedial mechanisms in laws, policies and alternate conflict resolution mechanisms.

150. At the level of the Council of Europe, much has already been done to meet the above-mentioned challenges. Inter alia, the Budapest Convention provides for a range of tools for the prevention of cybercrime – including during the electoral process – and for international cooperation aimed at securing electronic evidence; importantly, current works on a 2nd Additional Protocol to the Convention should permit added options for enhanced international cooperation and access to data in the cloud. Furthermore, a series of legal standards are in place for the protection of privacy and personal data in the context of social media. In particular, the Modernised Convention on the protection of individuals with regard to automatic processing of personal data, which is open to any country in the world and which sets international standards, should serve as the universal treaty for data protection. Finally, a number of legal instruments have been developed to ensure free elections, in particular through electoral campaign funding regulations and measures to prevent inequality in media coverage during elections both online and offline.

151. At the same time, several Council of Europe documents suggest that there is room for further improvement. In particular, the CoE Information Disorder Report 2017 made a number of recommendations directed at governments, education ministries, media organisations, technology companies and civil society to address the challenges posed by the increasing mis-, dis- and mal-information and their impact on democratic processes; and the CoE Election

Study 2017 concluded that the current regulatory framework no longer suffices for maintaining a level playing field for political contest and for limiting the role of money in elections, and it suggested a number of measures to remedy this situation.

152. Taking the main results of these documents and of the present study into account, the recent shift in the influence of internet-based channels of electoral communication calls for action in the following areas:

A. Revision of rules and regulations on political advertising: in terms of access to the media (updating broadcasting quotas, limits and reporting categories, introducing new measures covering internet-based media, platforms and other services, addressing the implications of micro targeting) and in terms of spending (broadening of scope of communication channels covered by the relevant legislation, addressing the monitoring capacities of national authorities);

B. Accountability of internet intermediaries in terms of transparency and access to data enhancing transparency of spending, specifically for political advertising. In particular, internet intermediaries should provide access to data on paid political advertising, so as to avoid facilitating illegal (foreign) involvement in elections, and to identify the categories of target audiences.

C. Quality journalism: strengthening of news accuracy and reliability, enhanced engagement with the audience, strengthening of public service media and local media, and empowering self-regulation with an added focus on transparency of online news and their circulation;

D. Empowerment of voters towards a critical evaluation of electoral communication targeted action for preventing exposure to false, misleading and harmful information (with due reflection on the limits of fact-checking initiatives; efforts on media literacy (including social media literacy) through education and advocacy;

E. Open internet: ensuring net neutrality, considering legally strengthening users' rights to an open internet, and ensuring that any restrictions on access to internet content are based on a strict and predictable legal framework regulating the scope of any such restrictions, and ensuring that judicial oversight to prevent possible abuses is guaranteed;

F. Data protection: affirming and protecting the right to anonymity on the internet, regulating and strictly limiting the creation and use of profiles, in all kinds of different contexts. In addition, the Council of Europe might consider adopting guidelines on the restrictions to be imposed on surveillance technologies, including the international trade in such technologies; promoting Convention 108 as the "gold global standard"; and possibly developing a specific legal instrument to address the high risk that the use of digital technologies in political campaigns and advertising represents to personal data protection.

153. As stressed earlier, the borderless nature of the internet and the private ownership of the information highways render the current challenges to democracy and electoral processes particularly complex. International cooperation and involvement of the relevant private actors are therefore indispensable to face these challenges and to ensure the right to free elections and the functioning of democracy in the future.