Strasbourg, 11 December 2020 **CDL(2020)037**

Opinion No. 974/2019 Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

PRINCIPLES FOR A FUNDAMENTAL RIGHTS-COMPLIANT USE OF DIGITAL TECHNOLOGIES IN ELECTORAL PROCESSES

Approved by the Council of Democratic Elections at its 70th online meeting (10 December 2020) and adopted by the Venice Commission at its 125th online Plenary Session (11-12 December 2020)

on the basis of comments by

Mr Richard BARRETT (Member, Ireland)
Ms Herdís KJERULF THORGEIRSDOTTIR (Member, Iceland)
Mr Rafael RUBIO NUÑEZ (Member, Spain)
Mr José Luis VARGAS VALDEZ (Member, Mexico)

Table of Contents

I. INTRODUCTION

1. At its 119th plenary session (June 2019), the Venice Commission adopted the 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 the Use of digital technologies and elections (hereafter: the Joint report), previously adopted by the Council for Democratic Elections on 20 June 2019 (CDL-AD(2019)016), and decided to elaborate a Set of principles for a fundamental rights-compliant regulation of the use of digital technologies in electoral processes.

2. At the occasion of the adoption of the Joint report the Rapporteurs noted that "the internet and social media had opened new opportunities for political participation and had become essential in the electoral process". At the same time, "electronic challenges to democracy, including cybercrime, were nonetheless high and extremely complex, due in particular to the borderless nature of the internet and the private ownership of information. A legal response to these challenges was needed. Some form of regulation was called for, but it had to respect fundamental freedoms, in particular, freedom of expression, economic freedom, the right to privacy and social rights."[1]

3. The Rapporteurs of the Joint report were also appointed as Rapporteurs for the present Principles, namely Mr Barrett, Ms Kjerulf Thorgeirsdóttir, Mr Rubio Nuñez and Mr Vargas Valdez.

4. The present principles which were prepared on the basis of the comments submitted by the experts above, were approved by the Council for Democratic Elections at its 70th meeting (online, 10 December 2020) and adopted by the Venice Commission at its 125th plenary session (online, 11-12 December 2020).

II. BACKGROUND

A. Digital technologies and democracy

5. As stated in paragraph 143 of the Joint report, "[t]he relationship between democracy and digital technologies is quite complex. On the one hand, [digital tools] have become the dominant platform of political interaction in some democracies, [and they] 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 digital 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 strategically) feeding or hiding specific information to its users, thus fostering a partial understanding of reality and hampering freedom of expression."[2]

[1] See the Session report of 11 July 2019, CDL-PL-PV(2019)002rev, page 16.

[2] It should be noted that in addition to such dangers related to the deliberate manipulation and misuse of electoral tools and processes, technology also includes other risks that are not linked to any intentional harms or violations, for example: digital divide in the access to, or use of, digital technologies; the lack of knowledge of how the new online information spaces work (the role of media, the role of online platforms, the use of personal data to personalise communication with the voters, etc.), or the effects of the information overload, which can contribute to closing people off in their echo chambers. These topics are not analysed in detail in this document, but it is important to mention them for further studies, subprinciples or other documents that may be developed in the future, in terms of paragraph 21.

6. On the basis of this scenario, the debate between “apocalyptic and integrated” (Eco) has taken hold of the relationship between technology and democracy. “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 digital technologies foster some aspects of the democratic contest, they also hamper 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 supervise and regulate online social behaviour”.[3]

7. These dangers, directly linked to technology, affect the different phases of the electoral process, such as: the nomination of candidates, in which the collection of signatures for independent candidates or the realisation of primary elections can be done via applications that risk creating problems that affect the process; candidate and voter registration; voter information initiatives (voter education campaigns); the electoral campaign, impinging upon the free development of the voter’s will; political / campaign finance and its transparency; the voting process itself; vote counting and establishment of election results; the election dispute resolution process.

8. We are facing a number of threats that

a) are developed on various levels (national, local/sub-national and international);
b) utilise a new concept of time, in which informative immediacy affects decision-making and the fact that certain content can go viral very quickly may impact how remedies may be effectively applied;
c) involve a variety of different actors: parties, media, citizens and private businesses, which are outside regulatory models exclusively centred on the role of the media and of parties;
d) are carried out through actions that combine the advantages of the – rapidly evolving – new technological infrastructure and potential for manipulation.

9. As previously stated, such threats may not only lead to the alteration of final election results but may also harm fundamental democratic principles such as transparency or secrecy of the vote, among others. The ways by which they erode confidence in the democratic system and cast doubt upon the legitimacy of elected officials are almost as important. In any case, the aforementioned threats challenge both the “electoral democracy” – understood as the institutional activities and infrastructure that make elections possible, and commonly known in the internet context as “e-government” –, the “deliberative democracy” – understood as the participation by individuals in open debate in the belief that it will lead to better decisions on matters of common concern – and the “monitory democracy” – understood 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. Cyberthreats to elections thus take different forms depending on whether they concern electoral democracy (through attacks against the confidentiality, integrity and availability of election computers and data) or deliberative/monitory democracy (through information operations with violations of rules to ensure free, fair and clean elections).[4]

10. On the other hand, new technologies offer different solutions for the challenges that contemporary electoral processes are facing. There is a whole range of prospects that are becoming available to the democratic system, starting from logistical issues such as cost savings,

[3] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 47.
[4] See below under Principle 6.

the reduction of the impact on the environment as a result of reducing paper usage, and going up to issues that reinforce democratic legitimacy such as: citizen funding of campaigns; transparency of funding; electronic registration in the electoral roll (in countries where registration is necessary to vote); public declaration of electoral information that governments, political parties and candidates offer online - this public declaration is intended to guarantee the rights to use, share and comment on this information; quick sharing of electoral concerns to a global audience (e.g. the posting of a video of ballot box stuffing or videos of electoral violence), which can help document abuses that may otherwise have been hidden. Finally, the promotion of electoral participation by authorities should be considered, for example through advertising campaigns using social networks or through the use of technology to locate polling stations on a map.

11. Specifically, "[t]he 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[, while s]ocial media in particular constitute the predominant platform of political debate and, as such, they are sources of political information".[5] Moreover, internet helps to ensure that information reaches marginalised groups and diaspora and allow them to participate in electoral debates.

12. 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".[6]

13. From one point of view, the internet would be nothing more than a communication channel, more or less widespread among the population, and whose virtual character implies that is has only limited impact on decision-making. This vision ignores the impact that this "channel" has on the rest of the channels and, above all, the transformations it generates in the way society communicates and organises itself.

14. The internet clearly affects the ways people communicate, conduct their behaviour and form their opinions. The speed and scope of digital technology has not only transformed the way public opinion can be formed but also provided the means for distorting reality to an extent unknown before in the era of traditional journalism with the imparting of news, information and ideas. The misuse of digital technology to manipulate facts, to spread disinformation in a strategic, coordinated fashion, to conduct surveillance by collecting information from (and about) citizens, and engaging political stakeholder groups, has affected people's trust in democratic institutions and the rule of law. The impact of digital technology in empowering citizens and democratic representation is questioned in light of the above and the question arises whether or how this technology can be managed to prevent the factors distorting fundamental rights such as freedom of expression, opinion and information and the right to privacy with massive surveillance for political / financial purposes.

15. Those who argue that technology is transforming the very meaning of politics[7] maintain that the availability of a greater volume of information and greater transparency, directly related, is joined by participation, which has been called the recovery of power on the part of citizens. The growth in the information at citizens' disposal, in addition to the existing facility to relate to other

[5] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 35.

[6] Laidlaw 2015, p. 1.

[7] Kollock, P., Smith, M., *(*1995); Hagen, M. (1997); Castells, M. (1998); Bimber, B., (1998); Leadbetter, C., *(*1999); Hall, M., (1999); Clift, S., (1998); Badillo, Á. y Margenghi, P. (2001); Subirats, J. (2002); Rheingold, H., (2002); Savigny, H., (2002); Lim, M., (2002); Krueger, B. S., (2002); Tolbert, C. J., Mcneal, R. S., (2003); Bennett, W. L. (2003); Chadwick A. (2003, 2006); Rogers, R. (2004); Dahlgren, P. (2005); Simone, M (2006); Benkler, Y. (2006); Friedland, L., Hove, T. Y Rojas, H., (2006); Shirky, C., *(*2008); Drezner, D. y Farrel H., (2008); Dutton, W. H. (2010).

citizens, increases their capacity to receive information and process it, their ability to self-organise and their opportunities to make their proposals reach the institutions.[8] In short, this implies a major change in the way of doing politics, which has resulted in the emergence of new alternatives under informal or unusual political structures even in the electoral process. From voters, citizens who wish to do so are on their way to becoming part of political processes.

16. This change of protagonists means that politics, long reserved for politicians and the media, is giving more and more weight to citizens. Political communication, traditionally associated with information and propaganda, is becoming the construction of permanent political relations: an immense conversation of millions of people talking to millions of people (*one-to-one*), in their own words and over a long period of time; a conversation that when it finds a clear objective (be it an election or a decision by the authorities) becomes social mobilisation.

17. Elements are beginning to be questioned as a result of the impact of technology, such as the excess and speed of information that makes it difficult to distinguish facts from fiction and enables the drowning out of news of crucial public interest in the electoral process, which the public is entitled to receive, with strategic, misleading dis-information. The famous quote of James Madison in support of freedom of speech that "knowledge will forever govern ignorance; and a people who mean to be their own governors must arm themselves with the power which knowledge gives" is questioned in relation to digital technology and democracy. High expectations on the benefits of the use of technology to strengthen democracies are now countered by increasing concerns about the threats they pose: "Algocracy", "Dictadata", "Weapons of Math Destruction", are just some of the many terms used to describe this threat. Hence the important role of quality-, analysis-based journalism, which is also suffering from these developments but remains crucial to citizens' understanding of democratic electoral processes.

18. Although, as seen before, these dangers threaten the democratic process in general, they have to be analysed with caution when it comes to electoral campaigns. Innovation has always been central to campaigns. The one who knows, understands and can use new technologies has a competitive advantage, until everyone else adopts the same practices and they become normalised among all the candidates. Problems arise when technology stops being a competitive advantage and turns into a threat to the integrity of elections, restricting the right to free elections.

19. Now more than ever message transmission is leading a radical change in communication. We are witnessing the parallel proliferation of information and its pollution at a global scale. Political parties and candidates have been given new platforms where they can communicate directly with their electorate, and citizens themselves are given platforms that were previously the exclusive domain of political parties. Traditional advertisement has been replaced by new forms of communication that try to adapt messages to specific sections of the electorate as well as new communication channels. As a result, messages have become increasingly personalised. Those that design campaigns do no longer have to think about the masses, as most individuals are already either convinced or lost. Therefore, they must rather concentrate on the small group of swing voters, for which the campaign techniques gain a one-to-one or many-to-many focus. This change created by technology has direct consequences on various actors who are subject to the electoral legislation. They concern the specificity of data protection regulation; the use of censuses and databases; the purchase of online advertisement, especially on social media during election periods; the activity of individuals on social media the day before the election; or the publication of electoral polls on web pages that are not rooted in the national territory.

[8] On the other hand, it may be argued that this does not necessarily lead to greater user autonomy, because many users are poorly equipped to process information from various sources (they do not recognise the importance of their diversity), or do not wish to engage with any sources that may oppose their beliefs and opinions.

20. This 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. There are, roughly speaking, two different forms of problematic electoral campaigning which are facilitated in this context; firstly, manipulation by political parties, candidates and their campaigns and secondly, malicious activities such as concerted disinformation campaigns, problematic accounts (bots amplifying false messages, accounts impersonating legitimate actors, etc.) or cyber espionage, which involve potentially illegal activities. Moreover, the scattered and anonymous creation of content seriously hampers the identification and attribution of responsibilities for illegal online behaviours, where voters may be seriously affected in their decisions by misleading, manipulative and false information designed to influence their votes, undermining the exercise of the right to free elections and creates considerable risks to the functioning of a democratic system. Furthermore, the algorithms that govern search engines and social media may foster a partial and sometimes illusory understanding of politics and democracy.[9]

21. As it can be concluded from this section, digital technologies impact in different ways, both positive and negative, the different types of democracy (electoral, deliberative and monitory) and all the stages of electoral processes. Taking that into account, the following sections will mainly focus on the impact of Internet and social media on electoral campaigns. While the principles are applicable to the electoral cycle as a whole and highlight the importance of free communication during electoral periods, this approach opens the possibility for further development of other reports, principles or subprinciples that focus on technologies used in other stages of electoral processes, in future documents.

B. Involved actors

22. Traditionally, electoral campaigns have been understood as a series of actions carried out by the candidates, the political parties or their members to obtain citizen support, and this definition is what the legislation has primarily addressed. From this perspective, the campaign is foremost identified as the set of measures that have their origin in the political party (such as letters, posters, meetings, spots or public statements), while the state has a role in the organisation and oversight of the electoral process.

23. One of the most important features relevant to the impact of new technologies on electoral campaigns is the significant increase in the number of actors in the campaign, independent from the parties. Communication is no longer centralised, with just one individual source (be that a politician, party or media body) communicating with a large audience of individuals, but decentralised, with many individual sources communicating with the audience of individuals. Today anyone can show support for a particular candidate online, upload a video with critical content or send emails promoting a candidacy without any official relationship to the campaign. However, these activities may have a much greater impact on the final outcome of the campaign, causing a qualitative change, and can lead to controversies.

24. New actors, from civil society organisations or individuals, can play a key role in the campaign, not only spreading the candidate's messages online but also buying ads to reinforce or weaken the candidates' positions. These actors can act without a link with the official campaign and even work outside the national barriers. Against this background, the responsibility of social media platforms within the framework of current political / campaign finance regimes to ensure transparency and accountability of ad placement, expenditure and attribution in order to better inform citizens of the context in which electoral choices are being made, gains critical importance.

[9] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 37, which refers to Quintana 2016; Fidler 2017; Van Dijck 2013; McChesney 2013.

25. With these new actors, anonymous profiles have appeared which are allowed by social platforms. 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. By giving 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 behaviour, by which individuals neglect personal responsibility and submit themselves to the will of the collective.

26. The voter decision-making process is thwarted by the creation and mass dissemination of false information through fake profiles, many of which are automated. The above-mentioned anonymity even makes it possible for candidates and parties to develop unofficial campaigns, taking advantage of the freedom of being outside of electoral regulation – as they may appear as ordinary citizens or use false identities in order to achieve greater impact on the electoral campaign. These options have created new and grave challenges to existing political / campaign finance regimes.

27. New technologies provoke the passage of campaigns based on information or propaganda, clearly distinguishable depending on the originator, political party or media source, to a format in which conversation becomes a key element, increasingly gaining importance, and in which opinions, personal information, unofficial meetings and official or unofficial propaganda broadcastings merge. The combination of this aspect with the proliferation of actors in campaigns generates problems regarding the possible extension of the responsibility of politicians before citizens for the content of their communications.

28. Another group of actors to be considered are the mass media, a notion whose scope has been questioned due to the emergence of the internet: does it extend further to online versions of written or audio-visual media only, or also to individual bloggers who publish information or opinions using new technologies with their own webpages, which are their own property and responsibility?[10]

29. Hence, as the distinction between media and individuals on the internet becomes less relevant, the focus should be on the content rather than the subjects. For example, traditional means of soliciting votes the day before an election, such as through conversation, differ greatly from those proposed by new technologies, which allow the same person to send an anonymous chain of SMS, “bombardment” of emails and comments or even create paid advertising on a webpage or blog. Expansion of political campaigning undermines traditional filters based on journalism values of truth, fact-checking and separation of opinion from fact. This has weakened the effectiveness of the traditional rules governing false and misleading claims.

30. Finally, intermediaries such as search engines and, perhaps even more pronounced, social media platforms,[11] have gained powerful new gatekeeper positions that enable them to influence the outcome of electoral processes. Search engines, seen as trustworthy by a majority, have the

[10] See e.g. the Judgment of the Court of Justice of the European Union (Grand Chamber) of 16 December 2008 (case C 73/07), which states that the importance of freedom of expression requires broad interpretation of the notion of "journalism", precisely, to provide greater protection to the dissemination of content online; the data protection exemptions “apply not only to media undertakings but also to every person engaged in journalism” (paragraph 58); “the medium which is used to transmit the processed data, whether it be classic in nature, such as paper or radio waves, or electronic, such as the internet, is not determinative as to whether an activity is undertaken ‘solely for journalistic purposes’” (paragraph 60).

[11] So far, social media platforms have proved more problematic, possibly because they allow third parties to access their user databases, they enable extraction of an enormous amount of users’ personal data, and at the same time they are not limited to search results but can offer specific tailored messages in a personalised space.

potential to influence the electorate's attention and voting preferences. A biased search engine result ranking can shift undecided voters towards one candidate. This could lead to new forms of influence in the elections that are not captured by existing rules.

31. As outlined in the Joint report,[12] "the small number of very powerful private actors that literally own the information highways have 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. […] However, this is done on a voluntary and unregulated basis, without a recognised rule of law-based framework."[13]

C. New challenges in terms of time and space

32. Electoral campaigns confined to the territories where the elections were taking place, have been radically changed with the possibilities of the internet. As a result, we are confronted with the problem of transforming the digital world into the real one, in traditional terms. In this process, the legislator will have to look at elements such as the server in which the web page is hosted (something that does not affect its availability), IP address (place of the connection which facilitates the activity) or ownership of the site, and nationality of the owner.

33. However, these "physical" realities do not influence the impact that something published on the internet, in a given territory, can have. Today, the fact that mass media and individuals are located "virtually" beyond our borders is likely to lead to the prohibition of certain activities including the publication of online advertising the day before the election, or the publication of confidential information during Election Day such as the results of exit polls. These possibilities demonstrate that it is necessary to establish the criteria that would prevent even parties or candidates themselves from developing campaigns by providing information from outside the national territory, either by hosting the website or the place where people running the online campaign can connect.

34. It is also difficult to apply the criteria of proportionality and equality of informative space in the systems that demand it. While there is a requirement for internet spaces and social media (especially in the public media) to guarantee equity, it seems to be rather complicated to apply traditional criteria to an information space as open as the internet.

35. The internet offers parties and candidates the possibility to maintain "offices of permanent information", which provide citizens with the opportunity to access infinite amounts of information in a range of formats. This "timelessness", provided by new technologies, also influences election campaigns. Two essential elements of the internet are its instantaneity and its interactivity, which significantly affect the time frame established for the realisation of the electoral campaign. It would be interesting to reconsider the concept of soliciting votes, a process which is divided between periods of pre-campaign (or permanent campaign) and campaign. Similarly, the expediency of distinguishing between financing of campaigns and financing of political parties appears questionable.

---

[12] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 145.

[13] Moreover, the national regulatory frameworks vary widely and have had differing impact on both technology companies and their own impact on election processes.

36. It is also necessary to address the issue of the ban of political campaigns during the day before the election, whose nature clashes with that of the internet as an asynchronous medium, in which content is permanent and accessible to everyone at all times, without political parties needing to take any action whatsoever: political events, messages, videos, propaganda, etc. from the entire campaign are available to the citizen, including the day before the election. The problem is of a quantitative nature, as a similar problem can be noted with regards to electoral posters that fill the streets throughout the campaign and whose immediate withdrawal the day before the election is not only impossible but also has never been proposed as a guarantee for the electoral process. It also seems clear that the mass mailing of emails and SMS as part of the campaign or further electoral advertisement the day before the election would contradict the logic of the current legislation.

37. Finally, the timelessness and extraterritoriality of new technologies pose a challenge to the investigation, prosecution and sanction of illegal activities relating to electoral processes. This challenge has already been described in the Joint report and needs to be addressed.

D. International standards and rights in conflict

38. The aforementioned threats 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 (hereafter UDHR), the International Covenant on Civil and Political Rights (hereafter ICCPR), 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).

39. The Joint report includes an overview of relevant European and international standards and instruments, with a particular focus on the ECHR and other legal instruments developed by the Council of Europe. This overview is referred to in the present context.[14] Council of Europe standards and policies in the field are also presented in the Compendium "Elections, digital technologies, human rights".[15]

40. The Joint report concludes that "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."[16]

41. In this connection, the Joint report stresses that "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 work 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

[14] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraphs 48ff.
[15] See https://edoc.coe.int/fr/elections/8142-elections-digital-technologies-human-rights-compendium.html .
[16] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 142.

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."[17]

42. "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."[18]

43. There are several factors which make any regulation in this area particularly difficult: as mentioned previously, the borderless nature of the internet; the involvement of a variety of – in particular private – actors; the fact that some regulations – e.g. in the area of campaign funding – are either not applicable or inadequate in the online-context. In addition, there are several fundamental rights and freedoms at stake which may in certain situations conflict with each other, in particular freedom of expression, personal data protection and privacy, the right to free elections, equality, and freedom of commerce.

44. For example, as stressed in the Joint report,[19] according to the European Court of Human Rights (hereafter the ECtHR) the rights to freedom of expression (Article 10 of the ECHR) and to free elections (Article 3 of Protocol No. 1 to the ECHR) are on the one hand prerequisites of each other,[20] but on the other hand they 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".[21] At the same time, any restrictions on freedom of expression must be proportionate to the legitimate aim pursued and necessary in a democratic society.

III. SET OF PRINCIPLES

45. To face the challenges posed by the use of digital technologies to "electoral democracy", "deliberative democracy" and "monitory democracy", the Joint report included several recommendations to be taken from an interdependent and global perspective. It stressed in particular that "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

[17] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 150.
[18] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 151.
[19] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 151.
[20] Plaizier, 2018.
[21] ECtHR, *Bowman v. the United Kingdom,* 19 February 1998, no. 24839/94; ECtHR, *Orlovskaya Iskra v. Russia*, 21 February 2017, no. 42911/08.

indispensable to face these challenges and to ensure the right to free elections and the functioning of democracy in the future."[22]

46. With these considerations in mind, the Venice Commission has developed several principles which should be respected by law-makers, regulators and other actors[23] involved in the use of digital technologies in elections and which are set out below. They emphasise the need for a human rights-compliant approach; human rights and fundamental freedoms must be translated into the digital environment. In order to ensure a global and coherent response to the above-mentioned challenges, it may prove necessary to go a step further and develop new international legal instruments. In this perspective, the Venice Commission supports current work undertaken by relevant Council of Europe bodies including the Ad Hoc Committee on Artificial Intelligence (CAHAI), the European Committee on Democratic Governance (CDDG) and the Committee of Experts on Media Environment and Reform (MSI-REF).

Principle 1
The principles of freedom of expression implying a robust public debate must be translated into the digital environment, in particular during electoral periods.

47. The protection of freedom of expression, opinion and information is essential for the democratic political process. In the case-law of the ECtHR the concept of democratic society is particularly relevant regarding the political deliberations preceding elections. The political discourse enjoys the highest protection extending to all individuals the right to participate in the debate.[24] For this reason the information flow is protected from both sides, that of imparting and receiving and not only vertically but also horizontally, i.e. between the network-users themselves.

48. The ECtHR has held that principles from the Court's case law regarding freedom of expression must be translated into the digital environment: Article 10 does not only protect the content of information but also the means of its dissemination, since any restriction based on the latter necessarily interferes with the right to receive and impart information.[25] In the digital public square content policies must be in line with freedom of expression principles. Ensuring an open public debate is the key question in this respect: "The free exchange of opinions and ideas" emphasised by the ECtHR Grand Chamber[26] is crucial for the democratic environment.

49. Article 10 is the only provision in the ECHR which accompanies the rights therein with duties and responsibilities. In the ECtHR case-law, the press (printed press, broadcast media, online media etc.) is the public watchdog which plays a crucial role for democracy. It has the duty to impart to the public information and ideas of all kinds of public interest, and it is furthermore the corollary right of the public to receive information and ideas of all kinds – also those that shock, offend and disturb[27] and may therefore "rock the boat"; opinions expressed in strong, exaggerated language, satires exaggerating and distorting reality with the aim to provoke and agitate are protected under Article 10.[28] Not only is the press protected in its special role of acting as public watchdog – the role of other social watchdogs is furthermore recognised, including NGOs, political activists, political opposition, scientists, intellectuals, bloggers and all those

[22] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 153.
[23] In this connection, attention is also drawn to the Global Network Initiative and its "Principles on Freedom of Expression and Privacy" which are aimed at providing direction and guidance to the ICT industry and its stakeholders: https://globalnetworkinitiative.org/gni-principles/
[24] Herdís Thorgeirsdóttir, Journalism Worthy of the Name, Freedom within the Press and the Affirmative Side of Article 10 of the European Convention on Human Rights, Martinus Nijhoff Publishers, 2005.
[25] See ECtHR, *Autronic AG v. Switzerland*, 22 May 1990, no. 12726/87.
[26] ECtHR, *Gillberg v. Sweden*, 3 April 2012, no. 41723/06.
[27] ECtHR, *Handyside v. the United Kingdom*, 7 December 1976, no. 5493/72.
[28] ECtHR, *Eon v. France*, 14 March 2013, no. 26118/10; ECtHR, *Kuliś and Różycki v. Poland*, 6 October 2009, no. 27209/03; ECtHR, *Alves da Silva v. Portugal*, 20 October 2009, no. 41665/07.

wanting to contribute to a critical public discourse as well as to controversial information and ideas.[29]

50. The UN Human Rights Committee's General Comment No. 34 on Article 19 of the ICCPR states in this respect:

> *"43. Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information-dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information-dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."*[30]

51. The ECtHR has recognised that the internet has become one of the principal means of exercising the right to freedom of expression and information. Therefore, measures blocking access are only compatible with the ECHR if a strict legal framework is in place regulating the scope of the ban and affording the guarantee of judicial review to prevent possible abuses.[31] Furthermore, Recommendation CM/Rec(2016)5 on internet freedom provides that the internet is to be available, accessible and affordable to all groups of the population without any discrimination, and that all measures taken by State authorities or private-sector actors to block or otherwise restrict access to an entire internet platform (social media, social networks, blogs or any other website) or information and communication technologies (ICT) tools (instant messaging or other applications), or any request by State authorities to carry out such actions must comply with the conditions of Article 10 of the Convention regarding the legality, legitimacy and proportionality of restrictions.

52. The UN Human Rights Council on 1 July 2016 passed a non-binding resolution condemning countries that intentionally disrupt citizens' internet access. The resolution builds on the UN's previous statements on digital rights, reaffirming the organisation's stance that "the same rights people have offline must also be protected online", in particular the freedom of expression covered under Article 19 of the ICCPR and of the UDHR.[32]

53. There has been a growing tactic among many governments (even regimes associated with democracy rather than authoritarian rule) to shut down the internet to stifle dissent.[33] The justification authorities often use is that they are trying to stop the spread of hateful and dangerous misinformation, which can move faster on Facebook, WhatsApp and other services than their ability to control it. But as the internet becomes more integral to all aspects of life, the shutdowns affect far more people than only protesters or those involved in politics.[34]

54. The legality of internet shutdowns is not often tested in courts. The ECtHR in cases concerning the blocking of access to the internet held that there has been violation of Article 10

---

[29] See ECtHR, *Observer and Guardian v. the United Kingdom*, 26 November 1991, no. 13585/88; ECtHR, *Guerra and Others v. Italy*, 19 February 1998, no. 116/1996/735/932.
[30] Adopted by the United Nations Human Rights Committee at its 102nd session (11-29 July 2011).
[31] ECtHR, *Ahmet Yıldırım v. Turkey,* 18 December 2012, no. 3111/10.
[32] Resolution No. 32/13, see https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13 .
[33] See e.g. the Wall Street Journal, https://www.wsj.com/articles/internet-shutdowns-become-a-favorite-tool-of-governments-its-like-we-suddenly-went-blind-11582648765; Freedom House, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.
[34] Shutdowns can even be devastating to people just trying to make a living, see https://www.nytimes.com/2019/12/17/world/asia/india-internet-modi-protests.html.

of the ECHR when the measure in question produced arbitrary effects and the judicial review of the blocking of access had been insufficient to prevent abuses.[35]

Principle 2
During electoral campaigns, a competent impartial Electoral Management Body (EMB) or judicial body should be empowered to require private companies to remove clearly defined third-party content from the internet, based on electoral laws and in line with international standards.

55. The case-law of the ECtHR recognises the right of individuals to access the internet[36] and makes it clear that in the digital public square, content policies must be in line with freedom of expression principles deriving from Article 10 of the ECHR. Political speech in particular enjoys the highest protection.

56. However, this right is not unlimited. In particular, during electoral campaigns, State authorities must be in a position to request private companies to remove third-party content inserted in violation of electoral legislation, in conformity with the conditions for restriction to freedom of expression defined in human rights treaties.[37]

57. The body competent for making such a request should be either an impartial electoral management body[38] or a court and act speedily. The decision of the electoral management body should be submitted to judicial review; this review should also be exercised very speedily in order not to render the request inefficient in case it has suspensive effect or, on the contrary, to exclude in practice any remedy against a violation of freedom of expression if it does not have such effect.

58. The principle of freedom of expression should not be interpreted in the sense that private companies have no responsibility for divulging political information from third parties. As explained in the Joint Report, "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 "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." All these conducts could facilitate, conceal or even constitute offences against democracy that must be prosecuted and sanctioned.

Principle 3
During electoral periods, the open internet and net neutrality need to be protected.

59. As already stated in the Joint Report, the challenge of simultaneously protecting freedom of speech, commercial rights and electoral equality without affecting other human rights require the recognition of: (1) the transnational nature of the problem; (2) the essential role played by the gatekeepers of information highways; and (3) the need to strengthen the international legal framework "in order to establish more efficient mechanisms of transnational cooperation among

[35] ECtHR, *Ahmet Yıldırım v. Turkey*, 18 December 2012, no. 3111/10.
[36] ECtHR, *Ahmet Yıldırım v. Turkey,* 18 December 2012, no. 3111/10.
37 Recommendation CM/Rec(2016)5 on internet freedom (Guidelines 2.2.1 - 2.2.2); Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries (Guideline 1.3.1).
[38] In some countries it may not be only Electoral Management Bodies (EMBs), but also media regulators and/or Data Protection Authorities (DPAs) in charge of certain aspects of electoral campaigning activities. In such situations, States should enable continuous cooperation between the relevant bodies.

nations and private actors, and, if possible, to procure a greater uniformity among national legislations". Furthermore, States and private actors must work on regulatory models based on the co-responsibility of them both, and on the promotion of self-regulation[39] "like the mandatory adoption of ethics and corporate social responsibility codes, among internet service providers, and search-engine and social media companies." This is essential to ensure the rights to equality of opportunity and freedom of voters to form an opinion, the respect of which is essential to the holding of elections in conformity with international standards.[40]

60. The principle of net neutrality means that Internet service providers (ISPs) must treat all internet communications equally, i.e. they may not discriminate or give advantage to any particular content by imposing economic barriers (e.g. by charging money for specific content) or structural obstacles by blocking or slowing down. This means that a level playing field must be guaranteed for users and content providers and ISPs must be prevented from unilaterally deciding on the availability of online contents. This is the reason why net neutrality is essential for an open democratic dialogue,[41] in particular during the crucial period of elections. Some countries, though, have chosen to pursue the goals of free, open, universal internet access by other regulatory strategies.

61. Recommendation CM/Rec(2016)1 of the Committee of Ministers of the Council of Europe 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. Furthermore, Regulation (EU) 2015/2120 lays down measures concerning open internet access.[42]

62. However, the question of net neutrality is quite complex. It has been stated that "there is no single policy instrument that allows realisation of the range of valued political and economic objectives simultaneously. Contrary to some of the claims advanced in the current debate, safeguarding multiple goals requires a combination of instruments that will likely involve government and nongovernment measures. Furthermore, promoting goals such as the freedom of speech, political participation, investment, and innovation calls for complementary policies."[43]

63. A noteworthy initiative to address issues of political manipulation, misinformation, fake news, privacy violations and other malign forces on the internet is a Contract for the Web proposal by the World Wide Web Foundation.[44] Such an initiative, if broadly supported and implemented at global level, could have the particular advantage of avoiding situations where the owner of a social media platform can alone determine what constitutes permissible speech.

64. In any case, the Venice Commission reiterates the recommendations it has made previously[45] which are aimed at, during electoral periods, ensuring net neutrality, considering legally strengthening users' rights to an open internet, ensuring that any restrictions on access to

---

[39] Recently, the discourse regarding private actors' responsibilities in the electoral context has shifted towards co-regulatory models, where the State would either (i) impose some basic obligations (going further than ethics, such as specific obligations of transparency), but the implementation would be a matter of self-regulatory bodies, with the possibility of State oversight; or (ii) introduce only backstop legislation to provide oversight for self-regulatory measures.

[40] Venice Commission, CDL-AD(2002)023rev-cor, Code of Good Practice in Electoral Matters, I.2.4 and I.3.1.

[41] Cf. Paolo Damiani, *The Open Internet vs. Net Neutrality and the Free Internet*. Federalismi. 2019: Net neutrality protects freedom from discrimination among types or sources of internet traffic, without regard to any competing interests or countervailing considerations."

[42] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120.

[43] Johannes M. Bauer & Jonathan A. Obar (2014) *Reconciling Political and Economic Goals in the Net Neutrality Debate*, The Information Society, 30:1, 1-19, DOI; see 10.1080/01972243.2013.856362.

[44] This initiave has been launched by the inventor of the web, Sir Tim Berners-Lee. See https://webfoundation.org/2019/11/launching-the-contract-for-the-web/ .

[45] See 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 152.

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.

Principle 4
Personal data need to be effectively protected, particularly during the crucial period of elections.

65. Article 8 of the ECHR provides for the protection of the right to privacy. This right ensures 'the development and fulfilment of individuals' personality'.[46] On this basis, the ECtHR has developed extensive case law concerning personal data protection.[47] In addition, a series of legal standards have been developed by the Council of Europe for the protection of privacy and personal data, notably in the context of social media.[48] In particular, the Council of Europe Modernised Convention on the protection of individuals with regard to automatic processing of personal data (Convention 108+),[49] which is open to any country in the world and which sets international standards, should serve as the universal treaty for data protection.[50]

66. Citizens need to be protected in the processing of personal data particularly during the election period when large amounts of personal data are processed, including those available in the electoral registers. As regards the registers data privacy has to be balanced against the transparency required for electoral integrity. New technologies pose new threats to the privacy of the voters, which currently includes the right to keep their vote confidential but should be extended to include the right to gather information before making a decision, and the right to private online browsing and free communication throughout the internet. The individual's online behaviour cannot be monitored without the free, specific, informed and unambiguous consent of the data subject or other legitimate basis laid down by law according to Article 5(2) of Convention 108+. Furthermore, when the processing concerns sensitive categories of data such as information revealing political opinions, an explicit consent may also be required as complementary protection (Article 6 of Convention 108+).

67. The data processing in both electoral and political advertising (in particular microtargeting advertising) context shall comply with data protection principles under Article 5 of Convention 108+. These personal data must be processed in compliance with purpose limitation and data minimisation principles. In particular, according to Recommendation CM/Rec(2012)4 of the Committee of Ministers on the protection of human rights with regard to social networking services, social networks should secure the informed consent of their users before their personal data is shared with other categories of people or companies or used in ways other than those necessary for the specified purposes for which they were originally collected. In order to ensure users' valid consent, they should be able to "opt in" to a wider access to their personal data by third parties (e.g. when third party applications are operated on the social network). Equally, users should also be able to withdraw their consent.

68. Considering that personal data for the information they reveal relating to political opinions falls within the scope of special categories of data under Art. 6 of the Convention 108+, this type

---

[46] ECtHR (Chamber), *A.-M.V. v. Finland,* 23 March 2017, no. 53251/13, paragraph 76, available at https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-172134%22]}

[47] 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.

[48] See 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraphs 76ff.

[49] Convention for the protection of individuals with regard to the processing of personal data as modernised by the Amending Protocol CETS 223, available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[50] The Preamble of this Convention explicitly refers to 'the right to the personal autonomy and the right to control one's personal data', underscoring the significance of the freedom of making choices.

of processing is subject to stricter regime. Data controller in both electoral and political advertising context shall process this type of personal data in compliance with the additional appropriate safeguards enshrined in law.

69. According to Article 9(1)(a) of Convention 108+, every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration. Profiling implemented by solely automated decision making can be considered as 'significantly affecting individuals if it involves the risk of manipulation.[51] Profiling for microtargeting in certain cases can be subject to this restriction. Data controllers shall take this right into account while using this type of advertising.

70. These factors kept in mind, a radical change worldwide would be required. Firstly, it would be necessary for all existing political entities to develop privacy policies. The regulators would need to establish the criteria for the permitted use of personal information on electoral processes. Any change in the data protection policy should be communicated to the electoral authorities responsible for the process, and failure to comply with these rules would lead to sanctions. Moreover, all those included in the database should be kept informed and removal from the database should be possible at any time.

71. In any case, in line with the Venice Commission's previous recommendations, it is necessary to affirm and protect the right to anonymity on the internet, regulate and strictly limit the creation and use of profiles and to consider developing a specific (international/Council of Europe) legal instrument to address the risks that the use of digital technologies in elections represents to personal data protection.[52] It is also essential to ensure easy access by users to their personal data in hands of the ISPs, including personal data for the information they reveal relating to political opinions in particular.

Principle 5
Electoral integrity must be preserved through periodically reviewed rules and regulations on political advertising and on the responsibility of internet intermediaries.

72. As has been described in the Joint report, there is a range of international and Council of Europe standards which are aimed at protecting the integrity of elections, ensuring they are free and fair, and not captured by a narrow range of interests. However, the legislative steps taken in the past focused on the offline context and their applicability and efficacy turned out to be severely limited in the information age – when democracy too has to adapt to the electronic environment ("e-democracy"). Inter alia, spending limits imposed on broadcasting have become less meaningful in times of digital advertising while transparency regulations ensuring that citizens are aware of campaign finance and spending are difficult, if not impossible to implement across borders in the digital environment. Problems in this area include, among others, outdated regulation of electoral campaigning from the perspective of media coverage, as well as the wider perspective of electoral communication; the enhanced role of internet intermediaries without enhanced responsibilities; lack of transparency of digital spending; difficulties in tracking the sources of campaign financing; political redlining – only engaging with voters considered worthy of campaigning (swing, undecided voters); decline of the journalism ethics filter; and privacy concerns.

[51] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal data. Profiling and Convention 108+: Suggestions for an update. Strasbourg: November 7, 2019.
[52] See 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 152.

73. Therefore, the Venice Commission has issued two recommendations[53] which remain highly relevant and need to be implemented:

- Revising 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);
- Ensuring accountability of internet intermediaries,[54] 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.

74. In the same vein, the Parliamentary Assembly of the Council of Europe[55] has recently called on member states to strengthen "transparency in political online advertising, information distribution and algorithms and business models of platform operators", in particular by "guaranteeing, where political parties and candidates have the right to purchase advertising space for election purposes, equal treatment in terms of conditions and rates charged" and by "developing specific regulatory frameworks for internet content at election times and including provisions on transparency in relation to sponsored content on social media, so that the public is aware of the source that funds electoral advertising or any other information or opinion […]."[56]

75. Measures to address the above-mentioned problems should strive to increase transparency of electoral communication in order to counter manipulative practices, foster transparency of electoral spending, ensure transparency and control of algorithms for the sake of diversity exposure, guarantee the protection of privacy in order to counter microtargeting of voters and ensure accurate and reliable information in order to empower voters in their choices and provide oversight over the electoral processes.

76. Different measures have been taken by the EU, EU member states, the US, Canada and tech companies themselves to increase transparency and limit undue influence of malevolent actors. Such attempts to regulate online political advertising include disclosure provisions requiring to reveal who is behind the advertising, who created it and the amount of money spent; prohibition of campaign spending by foreigners; and voluntary transparency measures by social networks and other internet platforms.

77. That said, it seems questionable whether transparency of paid political advertising is enough or if more is needed to roll back the situation where financial power can manipulate the electoral process to the extent that democracy is severely threatened. Paid political advertisements do not only provide advertisers an unfair advantage in proliferating highly targeted and often misleading messages but enable them to seriously endanger what should be "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" as provided for in Article 3 of Protocol No. 1 to the

[53] See 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 152.
[54] See also the requirements of transparency and accountability set by Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries (Guideline 2.2).
[55] See Resolution 2326 (2020) "Democracy hacked? How to respond?", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=28598&lang=EN&search=Kjog.
[56] In line with Resolution 2254 (2019) "Media freedom as a condition for democratic elections", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=25409&lang=en.

ECHR. Banning paid political advertising on social media may therefore be considered an option in order to ensure a fair electoral process.

78. It is also being debated how to address the current situation where a few private companies "have global control over the flow of information and are thus in a position to shape the political discourse and opinion formation" and who as owners of the information superhighways "are powerful and deregulated enough to dictate conditions on social, individual and political freedoms".[57] The Parliamentary Assembly of the Council of Europe[58] has recently called on member states "to break up the monopoly of tech companies controlling, to a great extent, citizen's access to information and data" in order to ensure an "open and free internet" which "serves the purpose of the voters to become more informed and engaged." The Venice Commission supports this appeal. Principle 8 regarding the adoption of self-regulatory mechanisms expands on this matter.

Principle 6
Electoral integrity should be guaranteed by adapting the specific international regulations to the new technological context and by developing institutional capacities to fight cyberthreats.

79. The Council of Europe has identified two types of cyberthreats to elections.[59] First, threats to electoral democracy, namely "attacks against the confidentiality, integrity and availability of election computers and data", compromising voter databases or registration systems; tampering with voting machines to manipulate results; interference with the function of systems on election day; and illegal access to computers to steal, modify, disseminate sensitive data. Second, threats to deliberative democracy, i.e. "information operations with violations of rules to ensure free, fair and clean elections" related to data protection, political finances, media coverage of electoral campaigns and broadcasting and political advertising. Such threats are addressed by the Council of Europe Convention on Cybercrime ETS 185 of 2001 ("Budapest Convention").[60]

80. 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. Effective international cooperation and cooperation with service providers is required. While the Budapest Convention in its current form includes detailed provisions on international cooperation combining expedited provisional measures to secure data with provisions on mutual legal assistance, they 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. 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.[61]

81. In order to guarantee the right to free elections "under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature" as provided for in Article 3

[57] See 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 13.
[58] See Resolution 2326 (2020) "Democracy hacked? How to respond?", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=28598&lang=EN&search=Kjoq.
[59] See the document concerning "*Cybercrime in the election process: the role of the Budapest Convention*", 15th European Conference of Electoral Management Bodies "Security in Elections", Oslo, Norway, 19-20 April 2018: https://rm.coe.int/coe-cyber-vc-oslo-april-2018-v1/16807bc437.
[60] See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[61] See https://www.coe.int/en/web/cybercrime/t-cy-drafting-group .

of Protocol No. 1 to the ECHR, the Venice Commission has issued three recommendations concerning cyberthreats[62] which remain relevant and need to be implemented:

- Criminalising cyber-attacks against the confidentiality, integrity and availability of election computers and data in pursuance of the Budapest Convention on Cybercrime;
- Providing 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;
- Preparing national Electoral Management Bodies (EMBs) for emergency situations and having in place crisis management organisation; EMBs should be provided with adequate resources and training to adopt digital technologies and address the related cybersecurity risks.

82. In this area which is subject to extremely rapid technical developments and to newly emerging threats to the right to free and fair elections, a constant review and update of laws and available tools for their effective implementation is necessary. At the same time, it is crucial that legal solutions balance between the right to free elections and other fundamental rights such as freedom of expression and data protection as highlighted above under the previous principles.

83. In addition, conflict resolution mechanisms (CRM) in this area need to be defined. The transnational and extraterritorial nature of digital technologies poses several challenges: the definition or creation of adequate competent authorities, different national regulations, extraterritoriality issues, etc. Furthermore, the private and commercial nature of internet companies require CRM more suitable to the logic of market (i.e. alternative dispute resolution mechanisms such as arbitration) – without ruling out jurisdictional procedures before international courts.

84. There is no internationally established criterion on how to solve jurisdictional issues to prosecute cybercrimes and online illicit behaviours. A comparative analysis[63] shows that some countries solve territoriality claims based on the following categories: location of acts; location of persons; location of effect; nationality of the perpetrator; or nationality of the victim.

85. Another challenge is the design of multiple regulatory and conflict-resolution approaches which would encompass both alternative and jurisdictional models. Moreover, the transnational nature of online behaviours requires an international authority (e.g. an international court) competent to solve conflicts beyond national and regional borders.

86. Finally, institutional capacities need to be strengthened to prevent cyber threats to democracy and electoral processes. Elections should be declared as a critical infrastructure, and the technological capacities and legal attributions of electoral authorities to control, investigate and prosecute illegal online behaviours should be strengthened.

Principle 7
The international cooperation framework and public-private cooperation should be strengthened.

87. Given the transnational nature of the problem and the essential role played by private actors, in particular by the internet intermediaries (i.e. mainly search-engine and social media

[62] See 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 149.
[63] Brenner, Susan & Koops, Bert-Jaap. (2005). *Approaches to Cybercrime Jurisdiction*. Journal of High Technology Law. 4.

companies, and also internet service providers), the Venice Commission has recommended[64] to strengthen the international framework (1) to establish more efficient mechanisms of transnational cooperation among national authorities and private actors, and, if possible, (2) to procure a greater uniformity among national legislations. Similar objectives have been set by the UN Global Programme on Cybercrime.[65]

88. Concerning international cooperation, as already stressed under the preceding principle it is necessary to create mechanisms to make the exchange of information and the investigation, prosecution and sanction of illegal conducts related to the subject of democracy and new technologies more efficient. This also implies determining in which areas it is a priority to promote legislative homologation in several countries. The efficiency in prosecuting offenses against democracy is particularly relevant during an electoral process, because such irregularities may have a direct impact on the validity of the election.

89. Suggestions for an efficient transnational collaboration have been made, e.g. with respect to standardised application formats; legal clarity of procedural rules; identity authentication of applicant and receiver; establishment of transparency standards in reports; determining under what standards decision making should be guided; a transnational appeal system; and establishment of official and efficient channels of dialogue between stakeholders.[66]

90. The transnational nature of cyber threats to democracy requires the active collaboration of governments, companies and individuals. Public-private cooperation is an important aspect of the use of new technologies in elections.[67] Operators and platforms should cooperate with electoral authorities, both in order to detect threats and to spread official information. Also, research and cooperation between electoral authorities, academics and practitioners should be encouraged in order to assess the real impact of digital technologies on electoral processes and the efficiency of the measures adopted. One important aspect is clarification of the respective responsibilities.

91. Another idea of cooperation could be the creation of a "Digital Corporate Responsibility Certificate" to be awarded to internet intermediaries by an international organisation in which experts from governments, companies and civil society, from as many countries as possible, participate. Such an initiative could follow the example of certifications issued by ISO (International Organisation for Standardisation) whose experts develop relevant international standards for the market that foster innovation and provide solutions to global challenges. ISO 26000 defines "social responsibility" as "the responsibility of an organisation with respect to the impacts of its decisions and activities on society and the environment" and includes the following principles: accountability; transparency; ethical behaviour; respect of the interests of involved parties; respect of the principle of legality; respect of international behaviour regulations; and respect of human rights.[68]

---

[64] See 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 149.

[65] United Nations. *Global Programme on Cybercrime*, see https://bit.ly/358EsaD.

[66] De la Chapelle, Bertrand & Fehlinger, Paul. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*. Centre for International Governance Innovation and Chatham House. 2016. Available at: https://www.cigionline.org/sites/default/files/gcig_no28_web.pdf.

[67] See e.g. the EU Code of Practice on Disinformation. Some other examples of such cooperation are referred to in the 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraphs 105f., including the Advisory Council for Internet and Elections of Brazil, cooperation of operators and platforms with electoral authorities in Mexico and Panama, as well as various fact-checking initiatives. Note also that in September 2019, Facebook, Twitter and Microsoft met with US government representatives to discuss possible collaboration strategies for the US federal elections of 2020, primarily to avoid foreign interference; see Isaac, Mike. *Big Tech Companies Meeting with U.S. Officials on 2020 Election Security*. New York Times. 2019. Available at: https://nyti.ms/33IIwhm.

[68] See ISO 26000, available at: https://www.iso.org/iso-26000-social-responsibility.html

92. The Venice Commission has also recommended[69]

- to foster education to strengthen legal and democratic culture among citizens, based on the co-responsibility of private and public actors; and
- to empower voters towards a critical evaluation of electoral communication targeted action for preventing exposure to false, misleading and harmful information through education and advocacy.

93. Education should allow citizens to confront the new digital reality, not just in terms of the functions of technology, but also in terms of its effects, teaching them to distinguish between the important and the irrelevant, between truth and lies. Beyond the educational strategies of the state, companies and civil society organisations could make alliances both to educate internet users and to evaluate the effectiveness of the controls implemented by companies.[70]

94. Finally, in a mature and full democracy the media must guarantee freedom of expression and be transparent to the public that listens to it, sees it, or reads it. Therefore, the Venice Commission has recommended[71] to promote greater quality in journalism, by 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.

95. In this connection, it must be noted that the characteristics of the digital environment pose serious challenges both for the design and implementation of codes of journalistic ethics[72] and for the verification of the veracity of the information, since digital channels favour immediacy and anonymity over veracity, accuracy and responsibility. Online-specific issues and considerations should be appropriately embedded in the existing ethical codes, or digital journalistic ethics codes should be adopted. States, EMBs, media and platforms should also be encouraged to collaborate on verification projects.

Principle 8
The adoption of self-regulatory mechanisms should be promoted.

96. There are valid concerns about the proliferation of illegal or abusive content online such as spread of disinformation campaigns; about (domestic or foreign) governments or powerful corporations sponsoring groups to influence elections; powerful corporations or actors sponsoring attacks on opponents in elections; or non-state actors exploiting the political discourse. The internet is, like the global market, much more difficult to handle, oversee, control than any domestic entity. On the one hand, unaccountable content regulation and overbroad censorship by tech companies – which would turn them into semi-tribunals (leaving network users without any judicial oversight or right to appeal) – must be avoided. On the other hand, social media companies and ISPs do have human rights responsibilities towards their users.

---

[69] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraphs 149 and 152.
[70] The shared responsibility of the state and the private sector is also stressed, for example, in the *Online Harms White Paper* (2019) presented by the Executive Branch to the UK Parliament: United Kingdom Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department. *Online Harms White Paper*. 2019. Available at: https://bit.ly/32L4ajH.
[71] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 152.
[72] While media content and commitment to the principles of professional journalistic ethics do not differ much depending on the medium used, in the digital environment there are several additional ethical considerations, such as how to engage with user-generated content, how to ensure a right to reply, etc.

97. Consequently, the Venice Commission has previously recommended to promote *inter alia* self-regulation, like the mandatory adoption of ethics and corporate social responsibility codes, among internet service providers, and search-engine and social media companies.[73] Similarly, the Parliamentary Assembly of the Council of Europe has called on professionals and organisations in the media sector to develop self-regulation frameworks that contain professional and ethical standards relating to their coverage of election campaigns, including respect for human dignity and the principle of non-discrimination.[74] Measures such as the adoption of corporate digital ethics codes and of self-regulatory mechanisms to solve conflicts between companies and users would also allow greater regulatory flexibility for the benefit of the interests of users and companies, while depressurising the relationship with the government and promoting co-responsibility of online behaviours.

98. According to the OSCE Online Media Self-Regulation Guidebook[75] "the basic rule that needs to be respected is that the more internal the self-regulatory process is, the more effective, the more proportionate and the more respectful of fundamental rights it will be." At the same time, the Guidebook also warns of several risks, namely with respect to effectiveness (ultimately, companies cannot force anyone to comply with their codes), priorities (internet intermediaries are private companies whose priority is to make profits and stay in business, not to protect freedom of expression) and undesirable incentives (resource-limited law enforcement authorities will de-prioritise particular online offences if they believe that they can rely on internet intermediaries).

99. In a mature and full democracy, a content platform or a social network must, as far as possible, guarantee the veracity of published content, or at least warn of the potential risks implied by certain publications or sources. Platforms have already adopted a set of measures such as requiring that political and issue ads be clearly labelled and restricting them to authorised users; deletion of fake accounts; approval of particular content and sources; increasing transparency in the process of buying political ads (buyers, amount, content, etc.). While such initiatives – which have been adopted either voluntarily or to comply with the law – are generally to be welcomed, they also run the risk of placing the responsibility of guaranteeing fundamental rights in private hands.[76]

100. In any case, it is crucial that the response to the challenges posed by digital technologies on democracy and human rights is not left to self-regulatory mechanisms alone. As has recently been stated by the Parliamentary Assembly of the Council of Europe,[77] "despite this contribution by the private sector, many regulatory problems remain unresolved and can only be tackled through international conventions as well as legislation at national and international level. Best practices and a better security agency co-operation should become normative in the defence of democratic elections." Furthermore, "researchers and journalists must have better access to data on fake accounts and disinformation without social media companies strictly controlling them. Policy makers cannot regulate what they don't understand, nor can they implement them and sanction non-compliance without independent checks and controls." This should also apply to independent election observers (national but also international), while ensuring the protection of freedom of speech and the privacy of users. In addition, transparency and accessibility of private company regulations (e.g. electoral content policies), including appeals mechanisms, and transparency on the data that they remove/allow, need to be ensured.

---

[73] 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 the Use of digital technologies and elections, CDL-AD(2019)016, paragraph 149.

[74] In line with Resolution 2254 (2019) "Media freedom as a condition for democratic elections", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=25409&lang=en .

[75] Organisation for Security and Co-operation in Europe (OSCE). *The Online Media Self-Regulation Guidebook*. 2013. Link: https://www.osce.org/fom/99560.

[76] It should be noted, however, that very similar practices can already be found in the field of intellectual property law.

[77] See the Explanatory memorandum of Resolution 2326 (2020) "Democracy hacked? How to respond?", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=28598&lang=EN&search=Kjoq.

101. In this connection, it has also been rightfully stated[78] that any solutions by tech companies should be "cautious, adaptable, and innovative, while fully complying with international freedom of expression standards". Examples for such solutions are specific codes of conduct adopted jointly by companies and public institutions, e.g. the EU Code of Practice on Disinformation and the Code of Conduct on Countering Illegal Hate Speech Online which has been developed by the European Commission in collaboration with several major digital technology companies (Facebook, Microsoft, Twitter and YouTube). The most ambitious task in this area would be the creation of an independent self-regulatory body for social media at international level.[79]

102. Furthermore, social media companies, search engines, content aggregators and other relevant internet intermediaries need to e.g. state in their agreements the rules that users must abide by, the terms of service governing the use of the social media platforms and what kind of content the company will prohibit (provided that such a prohibition is general and not prohibiting otherwise legal speech), and offering a quick and reliable appeals process for users who believe their content was illegally or improperly blocked or removed. As already mentioned, social media sites have already implemented content-moderation policies under which they remove certain content.[80] Direct incitement to violence or illegal activity is not protected speech, and it can and should be barred from social media platforms and the internet.[81]

[78] Article 19. *Self-regulation and "hate speech" on social media platforms*. 2018. London. Available at: https://bit.ly/2Wx4y3X.
[79] Ibid.
[80] Cf. the Report "Free Speech and the Regulation of Social Media Content" by the US Congressional Research Service, of 27 March 2019. Available at: https://fas.org/sgp/crs/misc/R45650.pdf.
[81] See the reasoning of the ECtHR in the case of *Delfi AS v. Estonia* (Application no. 64569/09, ECtHR, 16 June 2015).