Strasbourg, 4 June 2020 **CDL-EL(2020)002***

Opinion No. 974/2019 Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

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

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 (Substitute Member, Mexico)

**This document has been classified restricted on the date of issue. Unless the Venice Commission decides otherwise, it will be declassified a year after its issue according to the rules set up in Resolution CM/Res(2001)6 on access to Council of Europe documents.*

This document will not be distributed at the meeting. Please bring this copy.

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 adopted by the Council for Democratic Elections at its … meeting (Venice, …) and by the Venice Commission at its … plenary session (Venice, …).*

II. BACKGROUND

A. Digital technologies and democracy – benefits and risks

5. The debate between "apocalyptic and integrated" (Eco) has taken hold of the relationship between technology and democracy. 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 ways society communicates and organises itself.

6. 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 if or how this technology can be regulated 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.

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

7. Those who argue that technology is going to transform the very meaning of politics[2] believe that the availability of a greater volume of information and greater transparency, directly related, would be 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 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. 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 today.

8. 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.

9. 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 fictions 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.

10. Although these dangers threaten the democratic process in general, they are analysed with caution when it comes to elections. Technology is radically changing the way campaigns are carried out. Innovation has always been central to electoral 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, inhibiting the right to free choice or altering the results from the ballot boxes.

11. This danger is directly linked to technology and affects the different phases of the electoral process: 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; the electoral campaign, impinging upon the free development of the voter's will; the voting process itself; vote counting and establishment of election results.

12. We are facing a number of threats that

a) are developed on various national and international levels;
b) utilise a new concept of time, in which informative immediacy affects decision-making;
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;

[2] 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).

d) are carried out through actions that combine technological infrastructure and misinformation.

13. Such threats may not only lead to the alteration of final election results. The ways by which they erode confidence in the democratic system (for example by delaying recounts) and cast doubt upon the legitimacy of elected officials are almost as important. Those attacks could provoke reactions that would create greater limitation on the use of information, legitimising illiberal models of democracy. 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.

14. Now more than ever message transmission is leading a radical change in communication, as citizens themselves are given platforms that were previously the exclusive domain of political parties. Traditional publicity 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 publicity, 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.

15. New technologies also allow for the consideration of other elements that have yet to be investigated properly in terms of the voting processes. From logistical issues such as cost savings, the reduction of the impact on the environment as a result of reducing paper usage, 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, to guarantee the rights to use, share and comment on their information, the promotion of electoral participation by authorities, whether that would be through advertising campaigns using social networks or through the use of technology to locate polling stations on a map – there is a whole range of prospects that are becoming available to the democratic system.

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

information to its users, thus fostering a partial understanding of reality and hampering freedom of expression."[3]

B. Involved actors

17. Traditionally, electoral campaigns have been understood as a series of actions carried out by the candidate, the political party or its 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.

18. 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.

19. New actors, from civil society organisations or individuals, can play a key role in the campaign, not only spreading the candidate messages in the internet 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.

20. 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 off the impression that they have widespread support, these features create a bandwagon effect, and others accept the ideas shared by this apparent majority. This generates herd behaviour, by which individuals neglect personal responsibility and submit themselves to the will of the collective; they imitate one another and deny discrepancy.

21. The voter decision-making process is complicated 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.

22. New technologies provoke the passage of campaigns based on information or propaganda, clearly distinguishable depending on the issuer, 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 will generate problems regarding the possible extension of the responsibility of politicians before citizens for the content of their communications.

[3] Ibid, paragraph 143.

23. Another group of actors to be taken into account are the mass media, a notion whose scope has been questioned due to the emergence of the internet: whether it has to be extended only to online versions of written or audio-visual media, or also to any citizens who publish information or opinions using new technologies such as blogs or webpages, which are their own property and responsibility.[4]

24. 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.

25. Finally, intermediaries such as search engines 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 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.

26. As outlined in the Joint report, "the small number of very powerful private actors that literally own the information highways have own commercial interests and rights that tend to collide with both civil and political rights and electoral principles. These internet providers have taken up the gatekeeping role which originally belonged to the traditional media, without however having adopted the ethical obligations of the media. Private technology companies are thus censoring content which they consider 'harmful', without them being accountable and their measures being transparent. It is true that social platforms have recently adopted a series of measures for preventing false news and limiting their spread particularly during electoral periods. […] However, this is done on a voluntary and unregulated basis, without a recognised rule of law based framework."[5]

C. New challenges in terms of time and space

27. If until now electoral campaigns were held exclusively in the territories where they were going to take place, this tendency has radically changed, enhanced by 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.

28. 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

[4] 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).

[5] CDL-AD(2019)016, paragraph 145.

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.

29. 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.

30. 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 still making a difference between financing of campaigns and financing of political parties appears questionable.

31. 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 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 publicity the day before the election would contradict the logic of the current legislation.

32. 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

33. 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).

34. The Joint report includes an overview of relevant European and international standards and instruments, with a particular focus on the European Convention on Human Rights (hereafter ECHR) and other legal instruments developed by the Council of Europe. This overview is referred to in the present context.[6] Council of Europe standards and policies in the field are also presented in the Compendium "Elections, digital technologies, human rights".[7]

[6] CDL-AD(2019)016, paragraphs 48ff.
[7] See https://edoc.coe.int/fr/elections/8142-elections-digital-technologies-human-rights-compendium.html .

35. 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."[8]

36. 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 works on a 2nd Additional Protocol to the Convention should permit added options for enhanced international cooperation and access to data in the cloud. Furthermore, a series of legal standards are in place for the protection of privacy and personal data in the context of social media. In particular, the Modernised Convention on the protection of individuals with regard to automatic processing of personal data, which is open to any country in the world and which sets international standards, should serve as the universal treaty for data protection. Finally, a number of legal instruments have been developed to ensure free elections, in particular through electoral campaign funding regulations and measures to prevent inequality in media coverage during elections both online and offline."[9]

37. "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."[10]

38. 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, freedom of commerce.

39. For example, as stressed in the Joint report,[11] 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,[12] 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".[13] At the same time, any restrictions on freedom of

[8] CDL-AD(2019)016, paragraph 142.
[9] CDL-AD(2019)016, paragraph 150.
[10] CDL-AD(2019)016, paragraph 151.
[11] CDL-AD(2019)016, paragraph 151.
[12] Plaizier, 2018.
[13] *Bowman v. the United Kingdom,* Application no. 24839/94 (ECtHR, 19 February 1998); *Orlovskaya Iskra v. Russia*, Application no. 42911/08 (ECtHR, 21 February 2017).

expression must be proportionate to the legitimate aim pursued and necessary in a democratic society.

III. SET OF PRINCIPLES

40. 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 indispensable to face these challenges and to ensure the right to free elections and the functioning of democracy in the future."[14]

41. With these considerations in mind, the Venice Commission has developed several principles which should be respected by law-makers, regulators and other actors 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 works 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.

42. 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.[15] 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.

43. 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.[16] 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[17] is crucial for the democratic environment.

44. Article 10 is the only provision in the ECHR which accompanies the rights therein with duties and responsibilities. In ECtHR jurisprudence 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

[14] CDL-AD(2019)016, paragraph 153.
[15] 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.
[16] See *Autronic AG v. Switzerland*, Application no. 12726/87 (ECtHR, 22 May 1990).
[17] *Gillberg v. Sweden*, Application no. 41723/06 (ECtHR, 3 April 2012).

shock, offend and disturb[18] 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.[19] 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 wanting to contribute to the public discourse critical as well as controversial information and ideas.[20]

45. 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."*[21]

Principle 2
Government shutdowns of the internet should be prevented.

46. 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.[22]

47. 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.[23]

48. 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.[24] 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.[25]

49. 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

[18] *Handyside v. the United Kingdom*, Application no. 5493/72 (ECtHR, 7 December 1976).
[19] E*on v. France*, Application no. 26118/10 (ECtHR, 14 March 2013); *Kuliś and Różycki v. Poland*, Application no. 27209/03 (ECtHR, 6 October 2009); *Alves da Silva v. Portugal*, Application no. 41665/07 (ECtHR, 20 October 2009).
[20] See *Observer and Guardian v. the United Kingdom*, Application no. 13585/88 (ECtHR, 26 November 1991); *Guerra and Others v. Italy*, No. 116/1996/735/932 (ECtHR, 19 February 1998).
[21] Adopted by the United Nations Human Rights Committee at its 102nd session (11-29 July 2011).
[22] *Ahmet Yıldırım v. Turkey,* Application no. 3111/10 (ECtHR, 18 December 2012).
[23] Resolution No. 32/13, see https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13 .
[24] 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.
[25] 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.[26]

Principle 3
Private companies should not be made liable to remove third party content from the internet absent a judicial oversight (except for cases of imminent danger).

50. The UN Special Rapporteur on freedom of opinion and expression noted in 2018 that one of the greatest threats to online free speech was "the murkiness of the rules" and that states circumvented human rights obligations by going directly to the companies, "asking them to take down content or accounts without going through legal process."[27]

51. As the Special Rapporteur had already stated in 2017, "the liability placed upon private companies to remove third party content absent a judicial oversight is not compatible with international human rights law."[28] Such liability needs to be avoided, except for cases of imminent danger. Private companies may not be given the power to regulate the exercise of freedom of expression. Turning private companies into semi-tribunals leaves network users without any judicial oversight or right to appeal. Any legislation restricting the right to freedom of expression and the right to privacy must be applied by a body which is independent of any political, commercial or unwarranted influences in a manner that is neither arbitrary nor discriminatory.[29] Similar safeguards are called for in the Council of Europe Recommendation CM/Rec(2018)2.[30]

52. In this connection, attention is again drawn to the ECtHR jurisprudence which recognises the right of individuals to access the internet[31] and which 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.

Principle 4
The open internet and net neutrality need to be protected.

53. According to the principle of net neutrality, Internet service providers (ISPs) grant access to any content without giving advantage to any particular content by imposing structural or economical barriers. I.e. it is required to guarantee an even floor for users and content providers and to prevent ISPs from unilaterally deciding the availability of online contents. This is the reason why net neutrality is essential for an open democratic dialogue,[32] in particular during the crucial period of elections.

54. 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

[26] *Ahmet Yıldırım v. Turkey*, Application no. 3111/10 (ECtHR, 18 December 2012).
[27] See https://www.ohchr.org/EN/NewsEvents/Pages/FreedomExpressionReport.aspx.
[28] https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf. As for the case of *Delfi AS v. Estonia*, (Application no. 64569/09, ECtHR, 16 June 2015) where the ECtHR confirmed the liability of an online news portal for offensive comments posted by its readers, it must be noted that according to the Court, in this case the impugned comments obviously constituted hate speech that directly advocated acts of violence and therefore the assessment of their unlawful nature did not require any linguistic or legal analysis by Delfi since the remarks were on the face manifestly unlawful. Therefore, it has been observed that this judgment was not to be interpreted as imposing a form of "private censorship", cf. https://strasbourgobservers.com/2015/06/18/delfi-as-v-estonia-grand-chamber-confirms-liability-of-online-news-portal-for-offensive-comments-posted-by-its-readers/.
[29] See the report of the UN Special Rapporteur on freedom of opinion and expression of 16 May 2011, https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[30] Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries (Guideline 1.3).
[31] *Ahmet Yıldırım v. Turkey, Application no. 3111/10 (ECtHR, 18 December 2012)*.
[32] Cf. Paolo Damiani, *The Open Internet vs. Net Neutrality and the Free Internet*. Federalisimi. 2019: Net neutrality protects freedom from discrimination among types or sources of internet traffic, without regard to any competing interests or countervailing considerations."

and to access to information, and the right to privacy. Furthermore, Regulation (EU) 2015/2120 lays down measures concerning open internet access.[33]

55. 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."[34]

56. In any case, in line with the Venice Commission's previous recommendations, it is necessary to ensure net neutrality, to consider legally strengthening users' rights to an open internet, to ensure that any restrictions on access to internet content are based on a strict and predictable legal framework regulating the scope of any such restrictions, and to ensure that judicial oversight to prevent possible abuses is guaranteed.[35]

Principle 5
Personal data needs to be effectively protected.

57. Article 8 of the ECHR provides for the protection of the right to privacy. On this basis, the ECtHR has developed extensive case law concerning personal data protection.[36] In addition, a series of legal standards have been developed by the Council of Europe for the protection of privacy and personal data in the context of social media.[37] In particular, the Council of Europe 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.

58. 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 disseminated or 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' 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.

59. Internet users need to be protected against the collection and processing of personal data, particularly during the crucial period of elections. 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 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 consent as it contradicts the very principle of free and fair elections.

60. This factor 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 campaigns. Any

[33] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120.
[34] 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.
[35] See CDL-AD(2019)016, paragraph 152.
[36] 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.
[37] See CDL-AD(2019)016, paragraphs 76ff.

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.

61. 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 high risk that the use of digital technologies in political campaigns and advertising represents to personal data protection.[38] It is also essential to ensure easy access by users to their personal data in hands of the ISPs, including political data in particular.

Principle 6
Rules and regulations on political advertising and on the responsibility of internet intermediaries need to be kept under review.

62. As has been described in the Joint report,[39] there is a range of international and Council of Europe standards on election campaigns and especially campaign financing which are aimed at protecting the integrity of elections, ensuring they are free and fair, and not captured by a narrow range of interests.[40] However, the legislative steps taken in the past focused on the offline context and their applicability and efficacy in times of digital political advertising turned out to be severely limited. 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.

63. Therefore, the Venice Commission has issued two recommendations[41] 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,[42] 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.

64. In the same vein, the Parliamentary Assembly of the Council of Europe[43] 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

[38] See CDL-AD(2019)016, paragraph 152.
[39] See CDL-AD(2019)016, paragraphs 59ff.
[40] See the Council of Europe "Study on the use of internet in electoral campaigns" of 2017, DGI(2017)11.
[41] See CDL-AD(2019)016, paragraph 152.
[42] 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).
[43] 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.

"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 […]."[44]

65. Regarding the above-mentioned problems relating to the ban of political campaigns during the day before the election – whose nature clashes with that of the internet an asynchronous medium –, they might be resolved by prohibiting the addition of new materials including the employment of online print campaigns, as well as mass mailing of emails and SMS as part of the campaign or further electoral publicity, on that day.

66. 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; voluntary transparency measures by social networks and other internet platforms.

67. Recent discussion has focused on paid political advertisements on social media, many containing blatant lies. Twitter decided to ban these ads in October 2019 in order to stop the spread of misinformation and Google has imposed strict limits on ad targeting; Facebook announced that artificial intelligence technology would come up with algorithms allowing the flagging of harmful speech.

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

69. 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".[45] The Parliamentary Assembly of the Council of Europe[46] 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.

[44] 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.
[45] See CDL-AD(2019)016, paragraph 13.
[46] 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.

Principle 7
Regulations on the prevention and criminalisation of cyber threats to elections and on procedural tools for their implementation need to be constantly reviewed and updated and backed up by adequate institutional capacities of relevant authorities including the electoral supervisory mechanisms.

70. The Council of Europe has identified two types of cyber threats to elections.[47] 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").[48]

71. 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 warranted. 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.[49]

72. 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 of Protocol No. 1 to the ECHR, the Venice Commission has issued three recommendations concerning cyberthreats[50] 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.

73. 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, as highlighted above under the previous principles.

[47] 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.
[48] See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[49] See https://www.coe.int/en/web/cybercrime/t-cy-drafting-group .
[50] See CDL-AD(2019)016, paragraph 149.

74. 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.

75. There is no internationally established criterion on how to solve jurisdictional issues to prosecute cybercrimes and online illicit behaviours. A comparative analysis[51] shows that some countries solve territoriality claims based on the following categories: location of acts; location of computers; location of persons; location of effect; location of computers; nationality of the perpetrator; nationality of the victim.

76. 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.

77. 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 8
The international cooperation framework and public-private cooperation should be strengthened.

78. Given the transnational nature of the problem and the essential role played by private actors, in particular by the internet intermediaries (i.e. internet service providers, and search-engine and social media companies), the Venice Commission has recommended[52] to strengthen the international framework (1) to establish more efficient mechanisms of transnational cooperation among nations and private actors, and, if possible, (2) to procure a greater uniformity among national legislations. Similar objectives have been set by the UN Global Programme on Cybercrime.[53]

79. 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.

80. 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.[54]

[51] Brenner, Susan & Koops, Bert-Jaap. (2005). *Approaches to Cybercrime Jurisdiction*. Journal of High Technology Law. 4.
[52] See CDL-AD(2019)016, paragraph 149.
[53] United Nations. *Global Programme on Cybercrime*, see https://bit.ly/358EsaD.
[54] 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.

81. The transnational nature of cyber threats to democracy also requires the active collaboration of governments, companies and individuals. Public-private cooperation is an important aspect of the use of new technologies in elections.[55] 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 respective responsibilities.

82. 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.[56]

83. The Venice Commission has also recommended[57]

- 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.

84. 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.[58]

85. 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[59] 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.

[55] Some examples of such cooperation are referred to in the Joint report (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/33lIwhm.

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

[57] CDL-AD(2019)016, paragraphs 149 and 152.

[58] 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.

[59] CDL-AD(2019)016, paragraph 152.

86. 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 and for the verification of the veracity of the information, since digital channels favour immediacy and anonymity over veracity, accuracy and responsibility. The creation and adoption of digital journalistic ethics codes should therefore be promoted. States, EMBs, media and platforms should also be encouraged to collaborate on verification projects.

Principle 9
The adoption of self-regulatory mechanisms should be promoted.

87. There are valid concerns about the proliferation of illegal or abusive content online such as hate speech and 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.

88. Consequently, the Venice Commission has previously recommended to promote self-regulation, like the mandatory adoption of ethics and corporate social responsibility codes, among internet service providers, and search-engine and social media companies.[60] 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.[61] 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.

89. According to the OSCE Online Media Self-Regulation Guidebook[62] "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).

90. 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,

[60] CDL-AD(2019)016, paragraph 149.
[61] 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 .
[62] Organisation for Security and Co-operation in Europe (OSCE). *The Online Media Self-Regulation Guidebook*. 2013. Link: https://www.osce.org/fom/99560.

they may also run the risk of placing the responsibility of guaranteeing fundamental rights in private hands.[63]

91. It is therefore 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,[64] "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."

92. In this connection, it has also been rightfully stated[65] 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 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.[66]

93. Furthermore, social media companies and ISPs could 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.[67] 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.[68]

94. Finally, 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.[69] 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.

[63] It should be noted, however, that very similar practices can already be found in the field of intellectual property law.
[64] 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.
[65] Article 19. *Self-regulation and "hate speech" on social media platforms*. 2018. London. Available at: https://bit.ly/2Wx4y3X.
[66] Ibid.
[67] 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.
[68] See the reasoning of the ECtHR in the case of *Delfi AS v. Estonia* (Application no. 64569/09, ECtHR, 16 June 2015).
[69] 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/ .