Strasbourg, 10 December 2024 **CDL-AD(2024)044**

Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

INTERPRETATIVE DECLARATION

OF THE CODE OF GOOD PRACTICE IN ELECTORAL MATTERS AS CONCERNS DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE

Approved by the Council for Democratic Elections at its 81st meeting (Venice, 5 December 2024) and adopted by the Venice Commission at its 141st Plenary Session (Venice, 6-7 December 2024)

on the basis of comments by

Mr Oliver KASK (Substitute member, Estonia)
Ms Herdís KJERULF THORGEIRSDÓTTIR (Member, Iceland)
Mr Martin KUIJER (Member, The Netherlands)
Mr Cesare PINELLI (Substitute member, Italy)
Mr Rafael RUBIO NUÑEZ (Expert, Former member, Spain)
Mr José Luis VARGAS VALDEZ (Expert, Former member, Mexico)

Table of Contents

Introduction

1. The 2002 Code of good practice in electoral matters ("the Code") is the reference document of the Council of Europe in the field of elections, reflecting European electoral heritage. It enshrines five key principles of democratic elections: universal, equal, free, secret and direct suffrage and identifies conditions for implementing these principles: respect for fundamental rights, regulatory levels and stability of electoral law, and procedural guarantees.[1] The latter include the organisation of elections by an impartial body, the observation of elections, and an effective system of appeal.

2. Technological developments have created new opportunities and challenges for democracies that could have hardly been foreseen at the time of the adoption of the Code. In view of these developments and recent instruments adopted by the Venice Commission and the Council of Europe,[2] the Council for Democratic Elections proposed at its 79th meeting to prepare an interpretative declaration to the Code concerning the use of digital technologies and artificial intelligence during electoral processes (Venice, 14 December 2023). At its 137th plenary session the Venice Commission was informed of this proposal (Venice, 15-16 December 2023).

3. Mr Oliver Kask, Ms Herdis Kjerulf Thorgeirsdottir, Mr Martin Kuijer, Mr Cesare Pinelli, Mr Rafael Rubio Núñez, and Mr José Luis Vargas Valdez acted as rapporteurs for this interpretative declaration.

4. The interpretative declaration was drafted on the basis of comments by the rapporteurs. Together with its explanatory report, it was approved by the Council for Democratic Elections at its 81st meeting (Venice, 5 December 2024) and adopted by the Venice Commission at its 141st Plenary Session (Venice, 6-7 December 2024).

Interpretative declaration on digital technologies and artificial intelligence

1. Free suffrage: the freedom of voters to form an opinion (see the Code, guideline I.3.1)

5. The freedom of voters to form an opinion includes the right to have access to all kinds of information enabling them to be correctly informed before making a decision, the right to private online browsing, and the right to make confidential communications on the internet.

6. It is necessary to ensure that obligations on personal data protection are observed, in line with international standards. In particular, individuals should not be subject to a decision based solely on automated processing of data which significantly affects them or which entails whichever restriction of lawful content.

7. To protect the freedom of voters to form an opinion, the free exchange of opinions and ideas online and open public debate should be facilitated. This requires internet access and the effective right to seek, receive, and share information of all kinds. The principle of non-discriminatory treatment of internet traffic and the users' right to receive and impart information and to use services of their choice should be upheld.

---

[1] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters.

[2] See, in particular, Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections and Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes. See also the Council of Europe CM/Inf(2018)15, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data as amended by the Protocol CETS No 223 as well as the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS 225).

8. Whenever artificial intelligence systems are being used in elections, voters should be informed that they are interacting with such systems rather than with a human. Political “deep fakes”, namely the distribution of deceptive artificial intelligence-generated content to influence an election or to infringe voters’ freedom to make informed decisions, should be prohibited and sanctioned.

2. Equal suffrage: equality of opportunity (see the Code, guideline I.2.3)

9. Equality of opportunity also applies to the use of digital technologies and artificial intelligence in the electoral campaign, including the functions and services of internet intermediaries.

10. Candidates and/or parties must be granted fair and equitable access to public media, ensuring representation without discrimination. Legal provisions should also be adopted to ensure that there is a minimum access to privately owned online media and to the functions and services provided by internet intermediaries. In the digital realm, equality of opportunity also encompasses the principle of fairness in content dissemination and access.

11. Online electoral advertising must always be identified as such and must be transparent regarding the identity of its sponsor and the dissemination technique being used. Funding of online activities must be transparent, with potential limits on political parties’ spending on digital advertising. Social media platforms should be required to consistently disclose data on political advertising and their sponsors. Banning certain forms of paid political advertising on social media during electoral periods may be an option, particularly when automated mass dissemination or micro-targeting techniques based on artificial intelligence are being employed. The option to prohibit political parties and candidates from campaigning anonymously could also be justified.

3. The positive obligations of public authorities and the co-responsibility of private actors (see the Code, guidelines I.2.3.a and I.3.1.c)

12. The State has an obligation to take effective steps to ensure a supportive environment for robust public debate, preventing and punishing infringements of the voters’ freedom to form an opinion, including by private actors, as well as to prevent inequality in media coverage during elections.

13. An independent body should be mandated to enforce these regulations.

14. State authorities should address the challenge posed by organised information disorder campaigns, which have the potential to undermine the integrity of electoral processes.

15. Electoral integrity on the internet should be guaranteed on the basis of law, *inter alia* with specific rules against cyberthreats. Providing for criminal sanctions may be justified to deal with the most serious cases.

16. Specific rules should make it clear who is accountable for decisions made by artificial intelligence systems.

17. The State’s duty of neutrality also includes an obligation to build resilience among voters and to raise public awareness about the use of digital technologies in elections, including through the provision of appropriate information and support.

18. Cooperation between different public authorities, including across borders, ought to be strengthened.

19. Provisions should be established to ensure the cooperation of internet intermediaries and other private actors with governments, among themselves, and with academia and civil society.

4. Respect for fundamental rights (see the Code, guideline II.1)

20. The positive responsibility of the State to prevent undue interference with the principles of the European electoral heritage must not lead to undue state intervention.

21. Democratic elections are not possible without respect for *inter alia* freedom of expression, including media freedom. Any restrictions to these rights must have a basis in law, be necessary and in the public interest, and comply with the principle of proportionality (see the Code, guideline II.1.b).

22. Sanctions should be imposed by an independent and impartial body and subject to an effective system of appeal.

5. Specific provisions on the use of digital technologies by Election Management Bodies

23. Nothing in the Code nor in this interpretative declaration prevents the introduction of digital technologies in elections, provided that their use complies with respect for human rights, democracy, and the rule of law. The adoption of any technology should be done transparently, by broad consensus after extensive public consultations with all relevant stakeholders, and with the political commitment to fully implement it in good faith, with adequate procedural and judicial safeguards and means by which to evaluate in a timely manner any alleged failure to do so.

24. Digital technologies and artificial intelligence should only be used when appropriate safeguards are in place, particularly to ensure secure, reliable and transparent use. Use of digital technologies and artificial intelligence should be made in full respect of the principles of individual autonomy, privacy, equality and non-discrimination.

25. Universal suffrage also requires that the use of digital technologies is sufficiently easy to access and user-friendly to enable members of all groups, including persons with disabilities and older persons, to vote independently.

26. Removal from the electoral register shall not be subject to a decision based solely on automated processing of personal data, unless explicit consent is provided by the individual concerned, or when it is based on law with suitable safeguards that ensure the respect for the rights and freedoms of the individuals concerned.

27. When digital technologies are used in elections, specific provisions should additionally be foreseen to sustain the procedural guarantees in the Code:

a. The impartiality, independence and professionalism of election management bodies should be reinforced.

b. The use of digital technologies and artificial intelligence should be transparent to ensure electoral integrity and impartiality, especially in the processing of votes. Opportunities for election observers to monitor the use of digital technologies and artificial intelligence may need to be balanced against cybersecurity considerations and/or protection of sensitive personal data.

c. Digital technologies should be independently audited, and the findings of the auditing body should be public.

d. There should be a possibility to challenge before an independent body both the process of adoption of the tool by the electoral management body and the concrete decisions taken by or on the basis of a recommendation of an artificial intelligence system.

Explanatory report

I. General Remarks

28. Advancements in digital technologies and artificial intelligence[1] have introduced new opportunities and challenges for democracies that were scarcely imaginable when the 2002 Code of Good Practice in Electoral Matters was adopted.

29. According to the 2019 Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections, "[d]igital (or "new") technologies and social media […] have revolutionised the way people interact and exercise their freedom of expression and information, as well as other related - and sometimes conflicting - fundamental rights. People who engage in social media may use the internet to organise and demand better services, more transparency and meaningful participation in the political arena. Individuals all over the globe are now able to shape global perceptions, position topics in their national agendas and foster political activism. This digital transformation is recasting the relation between states and citizens."[2]

30. As noted later in the 2020 Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, a debate has emerged regarding the relationship of technology to democracy between "apocalyptic and integrated" views.[3] On the one 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."[4]

31. On the other hand, digital tools and technologies provide a range of opportunities and can improve efficiency and effectiveness in numerous fields, including electoral processes. As noted in the recently adopted Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS 225), "developments in science and technology and the profound changes brought about through activities within the lifecycle of artificial intelligence systems, […] have the potential to promote human prosperity as well as individual and societal well-being, sustainable development, gender equality and the empowerment of all women and girls, as well as other important goals and interests, by enhancing progress and innovation."[5]

32. The principles enshrined in the Code take on a special meaning in a digital environment in so far as the use of digital technologies may offer unprecedented opportunities to achieve their full realisation. At the same time, however, digital technologies also have the potential to pose

---

[1] All references to artificial intelligence in this interpretative declaration are based on the definition of "artificial intelligence systems" in the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS 225). These are understood as a "machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments", art. 2. See also the Explanatory Report, paras 23-25.

[2] Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 4.

[3] Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, paras 5-6. The terms between inverted commas have been used by Umberto Eco.

[4] Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 143.

[5] See the preamble of the Council of Europe's Framework Convention on Artificial Intelligence (CETS 225).

aggravated risks to these very same principles and to the conditions for their implementation, including the procedural guarantees.

33. In general, States are required to adopt and maintain measures that seek to ensure that digital technologies (including artificial intelligence) are not used to undermine the integrity, independence and effectiveness of democratic institutions and electoral processes. One modality is to entrust an electoral management body with the task of ensuring the integrity of the electoral system and thereby ensuring the reliability of the electoral processes and its outcomes.

34. Unlike previous exercises, this interpretative declaration is not restricted to a specific provision of the Code. Instead, it seeks to provide an updated framework for the guidelines throughout the entire Code. The declaration begins with guideline I.3.2 on the freedom of voters to form an opinion, as this issue is particularly affected by the use of digital technologies and artificial intelligence in electoral processes. Due to the prevalence of digitally-driven information disorders and plethora of information available online, voters are not only hindered in their ability to form opinions about candidates and electoral alternatives, but they are sometimes also misled about registration, voting procedures, or even the integrity of election results.[6] For this reason, this guideline becomes central to this declaration. The declaration further proposes expanding the scope of guideline I.2.3 on equality of opportunity, since this guideline partly overlaps with the freedom of voters to form an opinion.[7] Moreover, it provides a comprehensive interpretation of the positive obligations of public authorities in relation to both guidelines and emphasises the importance of respecting fundamental rights as a prerequisite for the effective implementation of the Code's principles. Lastly, it elaborates on the provisions governing the use of digital technologies by electoral management bodies.

II. Comments to the interpretative declaration on digital technologies and artificial intelligence

1. Free suffrage: the freedom of voters to form an opinion (see the Code, guideline I.3.1)

35. One aspect of free suffrage is the free formation of the elector's opinion.[8] The freedom of voters to form an opinion includes the right to be correctly informed before making a decision, the right to private online browsing, and the right to make confidential communications on the internet.[9] More specifically, the freedom of voters to form an opinion entails the right to have access to all kinds of information from online sources, the right to private browsing and to confidential communications on the internet, as well as the protection from undue influence on voting behaviour.

36. The voter's freedom to form an educated opinion may be affected by online information disorders, including the distribution of false information about election campaigns of political opponents. These phenomena have worsened as a result of the use of digital technologies (sometimes with the use of deep fake audio, photos, and videos, automated generated 'comments' under posts to manipulate public opinion, etc.). This freedom may be also infringed by the monitoring of people's online activity without their consent and for the purpose of

[6] Through the interpretative declaration and the explanatory report, "information disorders" should be understood broadly at the challenges related to mis-, dis- and malinformation. See Wardle, Claire and Derakhshan, Hossein, Council of Europe report DGI(2017)09, Information Disorder: Toward an interdisciplinary framework for research and policy making.
[7] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, para. 27.
[8] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, guideline I.3.1 and para. 26. Similarly, the Explanatory Report to the Council of Europe's Framework Convention on Artificial Intelligence stresses that the integrity of democracy and its processes is based on the assumptions that "individuals have agency (*capacity to form an opinion* and act on it)", para. 47 [emphasis added]. See also footnote 34 below.
[9] Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 122.

understanding and exploiting their behavioural paths, by the misuse of personal data facilitating micro-targeting as well as targeted messages which allow political candidates and parties to make different promises to different people, or by the use of ranking mechanisms in search engines.[10] Information disorders have also been a leverage to discredit the objectivity and reliability of news coverage, usually through automated means such as bots. The use of paid influencers' accounts by government actors and political parties to spread their views or campaign for them is yet another concerning practice. Political advertising can thus "be a vector of disinformation, in particular where the advertising does not disclose its political nature, comes from [foreign] sponsors […] or is subject to targeting techniques or ad-delivery techniques."[11]

37. Most breaches of the freedom of voters to form an opinion are the result of misuses of personal data. For this reason, it is necessary to ensure that obligations on personal data protection are observed, in line with international standards.[12] Likewise, individuals should not be subject to a decision based solely on automated processing of data which significantly affects them without having their views taken into consideration.[13] This provision therefore applies, but is not limited, to both automated procedures for micro-targeting by internet intermediaries, as well as to their content moderation methods. Individuals also have the rights to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to them; as well as to object at any time, on grounds relating to their situation, to the processing of personal data concerning them, unless the controller demonstrates legitimate grounds for the processing which override their interests or rights and fundamental freedoms.[14]

38. Individuals should neither be subject to a decision that entails whichever restriction of lawful content. While artificial intelligence can help moderate harmful content on digital platforms, there is also a risk that automated monitoring will result in whichever restriction of lawful content.[15]

39. To protect the freedom of voters to form an opinion, the free exchange of opinion and ideas online and open public debate should be facilitated. Even if these are not unique to electoral periods, this freedom also entails a right to access to the internet. This right has been recognised in the case-law of the European Court of Human Rights,[16] while the Venice Commission has previously acknowledged that the internet has become one of the principle means of exercising the right to receive information and ideas "regardless of frontiers."[17] Open access to the internet

[10] See, for example, Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, paras 43, 122, and 127. On micro-targeting, see the Judgment of the Court of Justice of the EU (CJEU) in the case of Maximilian Schrems v. Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, 4.10.2024, Case C-446/21.

[11] See also the Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, para 4.

[12] These include, but are not limited to, the Council of Europe CM/Inf(2018)15, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data as amended by the Protocol CETS No 223. For more specific guidance, see also the Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, adopted by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, paras 65-71.

[13] Art. 9(1)(a) of the modernised Convention 108.

[14] Arts. 9(1)(c) and (d) of the modernised Convention 108.

[15] Council of Europe's Ad hoc Committee on Artificial Intelligence, Feasibility study on a legal framework on AI design, development and application based on Council of Europe's standards adopted by the CAHAI, para. 27.

[16] See Ahmet Yıldırım v. Turkey, Application no. 3111/10 (ECtHR, 18 December 2012), para. 53, and Cengiz and Others v. Turkey, Application nos. 48226/10 and 14027/11 (ECtHR, 1 December 2015).

[17] See, for example, Venice Commission, CDL-AD(2013)024 Opinion on the Legislation pertaining to the Protection against Defamation of the Republic of Azerbaijan; Venice Commission, CDL-AD(2015)015 Opinion on Media Legislation (ACT CLXXXV on Media Services and on the Mass Media, Act CIV on the Freedom of the Press, and the Legislation on Taxation of Advertisement Revenues of Mass Media) of Hungary; and Venice Commission, CDL-AD(2016)011 on Turkey - Opinion on Law No. 5651 on regulation of publications on the Internet and combating crimes committed by means of such publication ("the Internet Law"), para. 98. See also, Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule

has the potential of informing voters about electoral issues who would otherwise not likely be informed about such matters.

40. In the case of measures addressing the online information disorders, net neutrality should be upheld. The principle of network neutrality underpins *non-discriminatory treatment of internet traffic* and the users' right to receive and impart information and to use services of their choice.[18] However, net neutrality is not absolute, nor should it be used as a liability shield to exempt internet intermediaries from accountability for user-generated content on their platforms (e.g., those protections typically under Section 230 of the United States' Communications Decency Act of 1996).[19]

2. Equal suffrage: equality of opportunity (see the Code, guideline I.2.3)

41. The Explanatory Report to the Code states that "[f]reedom of voters to form an opinion partly overlaps with equality of opportunity.[20]

42. Media failure to provide impartial information about the election campaign and candidates is one of the most frequent shortcomings arising during elections.[21] This issue has become even more salient in the online media, where professional journalists no longer act as information gatekeepers and new actors do not necessarily ensure adherence to the statutory requirements.[22] In turn, the distinction between political communication, political advertising and the individual expression of opinions becomes blurred.[23]

43. Equality of opportunity also applies to digital technologies and artificial intelligence, including the functions and services of internet intermediaries.[24] References to "radio and television air-time" in guideline I.2.3.b of the Code should therefore not be interpreted as restricted to these

---

of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 54, and Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, principle 3 (paras 59-64).

[18] Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, para. 4. See also Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 139 and CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, principle 3 (paras 59-64).

[19] For example, Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality already notes that equal treatment of Internet traffic "does not preclude Internet traffic management measures which are necessary and proportionate to [*inter alia*]: give effect to a court order or an order of a regulatory authority", para. 2.2.

[20] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, para. 27.

[21] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, para. 19.

[22] See Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, paras 12 and 15.

[23] See Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 64.

[24] According to Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, internet intermediaries are "[a] wide, diverse and rapidly evolving range of players [that] facilitate interactions on the internet between natural and legal persons by offering and performing a variety of functions and services. Some connect users to the internet, enable the processing of information and data, or host web-based services, including for user-generated content. Others aggregate information and enable searches; they give access to, host and index content and services designed and/or operated. Some facilitate the sale of goods and services, including audio-visual services, and enable other commercial transactions, including payments" (para. 4). Internet intermediaries may include, but are not limited to, social media platforms, search engines, as well as chatbots and other forms of generative artificial intelligence. See also Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 12.

media outlets.[25] References to "audiovisual media" in guideline I.2.3.c should also be understood as applying to online and digital media.[26] When ensuring equality of opportunity online, however, due account should be taken of the significant differences as regards the influence between traditional (broadcast) media and new (online) media.[27]

44. Candidates and/or parties must be granted fair and equitable access to online media, ensuring representation without discrimination.[28] Legal provisions should also be adopted to ensure that there is a minimum access to privately owned online media and to the functions and services provided by internet intermediaries, as well as to digital tools and artificial intelligence technologies to manage their campaigns.[29]

45. Additionally, fairness in content dissemination and access should be observed. Namely, regulations should be implemented to ensure that artificial intelligence algorithms by internet intermediaries do not favour certain parties or candidates over others, maintaining a balance in the visibility of electoral content. To this end, independent and ongoing audits of the artificial intelligence algorithms used in electoral campaigns should be enforced.

46. Regulating the funding of political parties and electoral campaigns remains an important factor in the regularity of the electoral process.[30] Funding of online activities must also be transparent.[31] Online electoral advertising must always be identified as such and must be transparent regarding the identity of its sponsor and the dissemination technique being used. Social media platforms should be required to consistently disclose data on political advertising and their sponsors.

47. Notwithstanding the foregoing, existing regulations on electoral campaigns in times of digital political advertising have turned out to be severely limited.[32] Spending by political parties on digital advertising may therefore be limited.[33] Banning certain forms of paid political advertising on social media during electoral periods may be an option, particularly when automated mass dissemination or micro-targeting techniques based on artificial intelligence are being employed.[34] The option to prohibit political parties and candidates from campaigning anonymously could also be justified.

---

[25] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, guideline I.2.3.b. The same applies to the "public facilities for electioneering purposes" mentioned in paras 18 and 19 of the Explanatory Report.
[26] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, guideline I.2.3.c.
[27] In the case Animal Defenders Intl v. UK, Application no. 48876/08 (ECtHR, 22 April 2013), para. 119, the European Court of Human Rights considered coherent a distinction based on the particular influence of the broadcast media vis-à-vis newer media such as the Internet. In particular, the Court noted that the information emerging from the internet and social media did not have the same synchronicity or impact as broadcasted information, given the continuing function of radio and television as familiar sources of entertainment in the intimacy of the home and because of the choices inherent in the use of the internet and social media. See also Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, para. 65.
[28] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, paras 18 and 19.
[29] The Explanatory report to the Code states that "[i]n conformity with freedom of expression, legal provision should be made to *ensure that there is a minimum access to privately owned audiovisual media*, with regard to the election campaign and to advertising, for all participants in elections" [emphasis added]. See Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, para. 20.
[30] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, para. 107.
[31] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, para. 108.
[32] See Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, para. 72.
[33] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, guideline I.2.3.e) and para. 21.
[34] See Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, para. 68.

3. The positive obligations of public authorities and the co-responsibility of private actors (see the Code, guidelines I.2.3.a and I.3.1.c)

48. The State has an obligation to take effective steps to ensure a supportive environment for robust public debate, preventing and punishing infringements of the voters' freedom to form an opinion as well as for preventing inequality in media coverage during elections.[35] The fight against information disorders, including disinformation explicitly aimed at questioning or misleading about the basic aspects of electoral procedures, calls for regulation by the state and an independent body with adequate resources and powers to enforce such regulation.

49. Electoral integrity on the internet should be guaranteed on the basis of law, *inter alia* with specific rules against cyberthreats.[36] Electoral integrity can be defined as the set of norms, principles and values inherent to democratic elections and which apply to the entire electoral process. It is, in particular, the ethical behaviour of all electoral actors as well as the respect of the principles of equity, transparency and accountability during the entire electoral process.

50. A regulation aimed at removing content that could be considered distortions of freedom of speech, such as false information and hate speech, would in principle appear justified. However, collaboration with internet intermediaries and monitoring of dissemination techniques may be appropriate measures, avoiding content regulation that may endanger freedom of expression. Providing for criminal sanctions may be justified to deal with the most serious cases.

51. New means to deal with these challenges may need to be employed as well, such as fact-checking, media literacy programmes, or investments in quality journalism.[37] Voter education programmes are also one of the main programmes to be put in place.[38]

52. An independent body should be mandated with the enforcement of these regulations and the implementations of these programmes. This body should have adequate resources and powers to implement their mandate and act speedily.[39]

---

[35] See, respectively, Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, paras 26 and 19 to 21. Similarly, art. 5.2 of the Council of Europe's Framework Convention on Artificial Intelligencestates that "[e]ach Party shall adopt or maintain measures that seek to protect its democratic processes in the context of activities within the lifecycle of artificial intelligence systems, including individuals' fair access to and participation in public debate, as well as *their ability to freely form opinions*" [emphasis added]. The Explanatory Report identifies examples of risks posed by artificial intelligence to democratic institutions and process, including to "political pluralism […] and fair access to and participation in public debate" as well as to "participation in democratic processes through free and fair elections, and a plurality of forms of meaningful civil and political participation", paras 46.d) and e), respectively. Based on these risks, examples of such obligations are suggested, such as "general cybersecurity measures against malicious foreign interference in the electoral process or measures to address the spreading of misinformation and disinformation", para. 47.

[36] On international cybersecurity standards, see the Council of Europe's Convention on Cybercrime (ETS No. 185) and particularly the T-CY Guidance Note #9 on aspects of election interference by means of computer systems covered by the Budapest Convention, adopted by the Cybercrime Convention Committee (T-CY). See also Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, principle 5.

[37] See Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 138.

[38] See, for example, Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, paras 92 and 93. See also the Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, para. 4.

[39] Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, principle 2 (paras 55-58).

53. Despite the above, enforcement of national regulations may be hampered by the universality of the Internet, understood as its capacity to affect wherever people are located.[40] Therefore, cooperation between different public authorities, including across borders, ought to be strengthened.[41] Particular attention should be paid to cooperation between national authorities and international organisations, as well as with International Election Observation Missions.

54. State authorities will also need the cooperation of both citizenry and internet corporations.[42] Provisions should be established to ensure the cooperation of internet intermediaries with governments in implementing these rules and programmes. For example, a competent impartial electoral management body or other impartial authority should be empowered to require private companies to remove clearly defined content from the internet, based on electoral laws and in line with international standards.[43] Cooperation should also be ensured among internet intermediaries, as well as with academia and civil society.

55. Distinguishing the responsibilities of platforms according to their dimension, increasing their responsibilities to the extent that their dimension is bigger, may appear necessary even if we refer to electoral matters.

56. Since digital technologies and artificial intelligence carry risks throughout the entire electoral process, and may even erode public trust, these positive obligations should not be constrained to the campaign period so as to safeguard the integrity of the election as a whole.

4. Respect for fundamental rights (see the Code, guideline II.1)

57. The positive responsibility of the State to prevent undue interference with the principles of the European electoral heritage must not lead to undue state intervention.[44]

58. Democratic elections are not possible without respect for *inter alia* freedom of expression, including media freedom.[45]

59. Any restrictions on the operation of internet intermediaries are only permissible to the extent that they have a basis in law, are necessary, in the public interest, and comply with the principle of proportionality.[46] Any such 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 guideline II.1.b.[47]

---

[40] The universality of the Internet has also been referred to as the transnational, extraterritorial, and timeless nature of digital technologies. See Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, paras 32-37 and 83.
[41] See, for example, Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, paras 87 and 88.
[42] See Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 138.
[43] See Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, principle 2 (paras 55-58).
[44] See Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 136.
[45] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, guideline II.1.a, which refers to freedom of expression and of the press.
[46] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, guideline II.1.b. In the case of data protection regulations, for example, article 11 of the modernised Convention 108 also stresses that lawful restrictions must respect the essence of fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society.
[47] Namely, that “Restrictions of these freedoms [namely, freedom of expression and of the press, freedom of circulation inside the country, freedom of assembly and freedom of association for political purposes, including the

60. Permissible restrictions generally should be content-specific. Generic bans on the operation of certain sites and systems are not compatible with the provisions of the European electoral heritage.[48] It is also inconsistent with these provisions 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. However, in case the webpage or system is managed by a foreign entity and has on many occasions disseminated false information aimed at influencing the election results, a general ban could be acceptable.

61. Sanctions should be imposed by an impartial body and subject to an effective system of appeal.[49]

5. Specific provisions on the use of digital technologies by Election Management Bodies

62. Nothing in the Code nor in this interpretative declaration prevents the introduction of digital technologies in elections, including artificial intelligence. Digital technologies may actually be used to ensure the respect for the freedom of voters to form an opinion and the principle of equality of opportunity by the media and by internet intermediaries. The following possibilities are just a few examples: the use of artificial intelligence could be considered to tackle the dissemination of false information in political campaigns through the possibility of performing real-time information reviews in an accessible manner; to answer citizens' questions about the electoral process, the electoral rules, on ways to exercise the right to vote, etc; and support election administrations in ancillary processes, such as voter registration.

63. In this context, a distinction should be made between rules addressed to designers and providers of digital technologies in elections, including artificial intelligence, and those addressed to electoral management bodies using these technologies. The latter are subject to much stricter standards, including all those applicable under the rule of law. Election management bodies should therefore adhere to the previous provisions in the interpretative declaration and, additionally, to those detailed in this section.

64. Election management bodies should comply with additional standards and requirements as new insights emerge about the impact of digital technologies and artificial intelligence in electoral processes.[50] The adoption of digital technologies and artificial intelligence tools by electoral management bodies should respect the rule of law principles related to, *inter alia*, transparency, accountability, and responsibility in the decision-making process regarding the purchase, implementation, monitoring, and use of digital technologies and artificial intelligence.

65. The Venice Commission has consistently expressed the view that any successful changes to electoral legislation and practice should be built on at least the following three essential elements: 1) a clear and comprehensive legislation that meets international obligations and standards and addresses prior recommendations; 2) the adoption and enforcement of legislation, including on digital technologies and artificial intelligence, by broad consensus after extensive public consultations with all relevant stakeholders; and 3) the political commitment to fully

---

creation of political parties] must have a basis in law, be in the public interest and comply with the principle of proportionality."

[48] See Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 137.

[49] Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, guidelines II.3.1 and II.3.3 as well as para. 19. See also Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), CDL-AD(2019)016, Joint Report on Digital Technologies and Elections, para. 137, and Venice Commission, CDL-AD(2020)037, Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, principle 2 (paras 55-58).

[50] *Inter alia*, and without prejudging on-going work on its update, those standards and requirements stemming from the Rule of Law Checklist. See Venice Commission, CDL-AD(2016)007, Rule of Law Checklist.

implement such legislation in good faith when using digital technologies and artificial intelligence, with adequate procedural and judicial safeguards and means by which to timely evaluate any alleged failure to do so.

66. The Code already states that electronic voting methods should only be used when they are secure, reliable, and transparent.[51] Additionally, the use of digital technologies and artificial intelligence should be made in full respect of the principles of individual autonomy,[52] privacy,[53] equality, and non-discrimination.[54] These requirements should apply to any technology used by the election authorities throughout the electoral cycle, including digital electoral registers.[55] Additional requirements may apply to different technologies.[56]

67. A problem observed in the development of artificial intelligence involves the fact that this technology has shown biases related to ethnicity, nationality, sexual orientation, and gender identity, to name just a few examples. The development of artificial intelligence should therefore be done in a way that discrimination is avoided, especially if these are based on political affiliation, as they would jeopardise the principles of impartiality and neutrality in the administration of the electoral process.

68. In order to comply with the principle of universal suffrage, the user interface of digital systems shall be easy to understand and use by all voters and the systems shall be designed, as far as is practicable, to enable persons with disabilities and special needs to use them independently.[57]

---

[49] The Code states that systems are secure if they can withstand deliberate attacks and that they are reliable if they can function on their own, irrespective of any shortcomings in the hardware of software (Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, para. 43). According to the Code, it should also be possible to check that the system is functioning properly (Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, para. 44).

[52] Individual autonomy is enshrined in art. 7 of the Council of Europe's Framework Convention on Artificial Intelligence (CETS 225). According to the Explanatory Report to the Council of Europe's Framework Convention on Artificial Intelligence, "[i]ndividual autonomy is one important aspect of human dignity and refers to the capacity of individuals for self-determination; that is, their ability to make choices and decisions, including without coercion, and live their lives freely. In the context of artificial intelligence, individual autonomy requires that individuals have control over the use and impact of artificial intelligence technologies in their lives, and that their agency and autonomy are not thereby diminished.", para. 55).

[53] The right to privacy is enshrined in art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005), most known as the European Convention on Human Rights (ECHR). In the electoral context, it is closely connected the principle of secret suffrage (see Venice Commission, CDL-AD(2002)023rev2-cor, Code of Good Practice in Electoral Matters, guidelines I.4). International obligations on data protection are also related to the right to privacy (see paras 37-38 above).

[54] The prohibition of discrimination is enshrined in art. 14 of the ECHR.

[55] Other Council of Europe's standards on the use of digital technologies in electoral processes have also similarly broadened their material scope. For example, the scope of the Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting was broadened in the updated Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting from "an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote" to "the use of electronic means to cast and/or count the vote". In turn, the recently adopted Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States "cover the use of ICT solutions by, or on behalf of, the relevant electoral authorities, in all the stages of the electoral process except e-voting and e-counting".

[56] See the above-mentioned recommendations and guidelines. See also the Guidelines on the protection of individuals with regard to the processing of personal data for the purpose of voter registration and authentication as well as the paper on Sensitive Personal Data, Biometrics, and the Registration and Authentication of Voters: The Application of Council of Europe Convention 108, which have been adopted by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In the case of artificial intelligence, due account should be taken of transparency-related aspects, such as explainability and interpretability (Explanatory Report to the Council of Europe's Framework Convention on Artificial Intelligence, paras 60-61).

[57] Standards 1 and 2 of the CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, and guideline 2 of the Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States.

Unless digital channels are universally accessible, they shall be only an additional and optional means.[58]

69. Due to the rapid evolution of technical solutions, especially artificial intelligence, the integrity and security of election technologies should be addressed with special care. As risks change rapidly, special procedures for risk assessment and risk management should be set-up and updated regularly.

70. There is also a threat that digital technologies and artificial intelligence may be used in a biased way to control the actions of opposition parties and leave the government parties' actions out of the scope of similar controls.

71. The procedural guarantees in the Code should therefore especially be observed when election technologies are used. Specific new provisions may need to be foreseen in the regulatory framework to mitigate any potential threats.

a. The impartiality, independence and professionalism of election management bodies are essential when digital technologies imply more tasks and their centralisation in these bodies, who should be accountable for how they are used.[59] In turn, election authorities will also need the cooperation of cybersecurity, data protection, and law-enforcement agencies, as well as citizen organisations and corporations.

b. Election management bodies should disclose the use of digital technologies, including algorithms and artificial intelligence systems. Legislation should contain clear rules on how far observers have access to digital systems or algorithms. Even though digital technologies and artificial intelligence systems are continuously developing and so are continuously changing the security mechanisms and needs, electoral legislation should provide, in a manner as detailed as possible, which data is publicly accessible. Observation missions, in turn, should consider incorporating specialists and resources dedicated to addressing these specific issues within their teams.

[58] Standard 3 of the CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, and guideline 3 of the Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States.

[59] The principle of accountability is not originally stated in the Code but is common in international standards on digital technologies. For example, under the modernised Convention 108, accountability is understood as the responsibility for and ability to demonstrate compliance with legal provisions (art. 10(1)). The Explanatory Report to the Council of Europe's Framework Convention on Artificial Intelligence refers to this principle as the "need to provide mechanisms in order for individuals, organisations, or entities responsible for the activities within the lifecycle of artificial intelligence systems to be answerable for the adverse impacts on human rights, democracy or the rule of law resulting from the activities within the lifecycle of those systems" (para. 66). Overall, it is understood that "[t]his principle emphasises the need for clear lines of responsibility and the ability to trace actions and decisions back to specific individuals or entities in a way that recognises the diversity of the relevant actors and their roles and responsibilities" (Explanatory Report to the Council of Europe's Framework Convention on Artificial Intelligence, para. 68). In the specific case of digital election technologies, no specific definition of accountability is yet provided. However, under Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting accountability requirements for Member States are outlined, including: developing and updating technical, evaluation, and certification standards to reflect legal and democratic principles; ensuring independent evaluations of e-voting systems before introduction and after significant changes; issuing clear certificates that identify evaluation subjects and include safeguards against modifications; and maintaining an open, comprehensive audit system for e-voting to actively report potential issues (paras 36-39). In turn, the Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States states that "it should be possible to make someone accountable if unauthorised changes or errors occur. It is essential to provide for an accountable and transparent procedure concerning how to interact with a running system, correct any data, or change or replace a malfunctioning system. Interacting with a running system for such purposes should be addressed in the risk analyses" (guideline 4).

c. If public access to some of the processes or content of digital systems is limited due to security reasons, independent auditing should be foreseen. The conclusions of such audits should be public.