The Venice Commission's Digital Doctrine: Harmonising Law, Technology, and Democracy*

Rafael Rubio Núñez

Table of Contents

1. Introduction. – 2. Technology and Democracy: Not Just Elections. – 3. A Systematic Approach to the Use of Technology in Elections. – 4. Doctrine in Action: Cancellation of Election Results. – 5. Conclusion.

1. Introduction

In 1974, when the World Wide Web was merely conceptual, Ted Nelson said: «If you are interested in democracy and its future, you better understand computers» (Nelson & Brand, 1974). In the current era, it is impossible to discuss democracy without considering technological developments. Yet given the Commission's age and distinguished membership, one might assume it is not a particularly technological institution. The assertion is demonstrably false. Since its inception, the Venice Commission (VC) – an organization that prioritizes democracy and the rule of law – has consistently engaged with technological issues such as data protection, the impact of technology on freedom of expression and information pluralism, and certain technological aspects of the right of association. In addition to those early efforts, the Commission in recent years has devoted increasing attention to the impact of digital technologies on electoral processes: protecting freedom of expression online, guaranteeing equality of opportunity for competitors in the digital campaign environment, safeguarding personal data and voter privacy, and ensuring transparency in digital campaign financing. The Commission also stresses the accountabil-

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Disclaimer: The author has participated in some of the opinions analyzed.

This contribution has been made within the Complutense research group on technology and democracy and has the support of the Research Project "Institutional and regulatory guarantees. Electoral and digital oversight authorities in the face of interference, hostile narratives, targeted advertising, and polarization" (PID2022-137245OB-I00) and as a staff member of the Jean Monnet Chair Decoding-i-Disorders (European Information Law Responses (press, audiovisual, and social media) at the Complutense University of Madrid.

ity of internet intermediaries (such as social media and search platforms) for their pivotal role in shaping political discourse and underscores the need for robust guarantees in electoral administration when new technologies are introduced – from impartial oversight and auditing of e-voting systems to strong cybersecurity measures treating elections as critical infrastructure.

In the VC's doctrine on technology and democracy, two distinct stages can be discerned. In the first stage, up until 2019, the Commission addressed these issues either indirectly (when dealing with topics like freedom of expression or freedom of association) or directly (when examining specific technological questions such as data protection or electronic voting). In the second stage, starting in 2019, the Commission began to confront the relationship between technology and elections in a more systematic and comprehensive way.

2. Technology and Democracy: Not Just Elections

2.1. Data Protection and Digital Development

One technology-related topic on which the VC systematically issued opinions and reports during this period is data protection and digital development. In 2007, the VC adopted the "Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights". It noted that since video surveillance entails the collection of personal data, its use engages the right to privacy; accordingly, such surveillance must be regulated in a manner that respects private life and other fundamental freedoms[1]. It identified important relevant provisions on personal data protection stemming from Article 8 of the European Convention on Human Rights (ECHR), the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, now the modernized Convention 108+), and EU Directive 95/46/EC (now the General Data Protection Regulation, GDPR).

Also in 2007, the VC adopted the "Report on the Democratic Oversight of the Security Services"[2]. It noted that technological advances in data collection, processing and analysis – and in surveillance – had «dramatically increased the capacity» of security agencies to interfere with human rights, and that powerful surveillance tools had become readily available even to private organizations.[3]

Later, in 2014, the Commission adopted the "Report on the Democrat-

[1] Venice Commission, *Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights,* CDL-AD(2007)014, 2007, 39-40.

[2] Venice Commission, *Report on the Democratic Oversight of the Security Services*, CDL-AD(2007)016, 2007.

[3] *Ibid.,* 58-59.

ic Oversight of Signals Intelligence Agencies". The VC concluded that signals intelligence has a large potential for infringing the right to private life and other human rights: it can be regulated in a lax fashion – meaning that large numbers of people may be swept up and intelligence on them retained – or it can be regulated more tightly, minimizing actual infringements[4].

More recently, the VC has adopted the "Report on a Rule of Law and Human Rights Compliant Regulation of Spyware"[5].

In addition, it issued at least two country-specific opinions related to data protection legislation. In 2002, the Commission had already raised questions about whether and how Article 8 of the ECHR might provide a general right to personal data protection[6] regarding an opinion of a draft law from Luxembourg. In 2023, the VC adopted an "Opinion on the Law on the Special Investigation Service and on provisions of the Law on Personal Data Protection" concerning the Personal Data Protection Service in Georgia[7]. That Opinion stressed the need for an independent data protection authority and the importance of respecting the mandate of its office holders[8].

Finally, the collection of data and surveillance are flagged as challenges to the rule of law in the "Rule of Law Checklist". The 2016 checklist likewise highlighted data protection and surveillance, posing questions to ensure that personal data collection and processing – whether by state or private actors – have adequate safeguards, and asking what guarantees exist against abuse in targeted, strategic, or video surveillance[9].

2.2. Electoral Processes and Electronic Vote

One of the VC's main areas of activity is the electoral field. Since 2002, its "Code of Good Practice in Electoral Matters" has become a benchmark. In this area, the Commission gradually refined its doctrine on the use of technology in electoral processes, as set out in a 2018 compilation covering digital technologies from voter registration through results transmission[10]. The Commission's role in this topic has also been reviewed from

[4] Venice Commission, *Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)011, 2015, 27.

[5] Venice Commission, *Report on a Rule of Law and Human Rights Compliant Regulation of Spyware*, CDL-AD(2024)043, 2024.

[6] Venice Commission, *Opinion on the Draft Law of Luxembourg on the Protection of Persons in Respect of the Processing of Personal Data,* CDL-AD(2002)019, 2002, 13.

[7] Venice Commission, *Georgia — Opinion on the Law on the Special Investigation Service and on the Provisions of the Law on Personal Data Protection concerning the Personal Data Protection Service*, CDL-AD(2023)044, 2023.

[8] *Ibid.,* 44.

[9] Venice Commission, *Rule of Law Checklist*, CDL-AD(2016)007, 2016.

[10] Venice Commission (compilation), *Compilation of Venice Commission Opinions and Reports concerning Digital Technologies in the Electoral Process*, CDL-PI(2018)011, 2018.

academic perspectives[11].

The Commission has reiterated a basic principle for introducing such technology in elections: before any new technologies are adopted, a number of issues should be thoroughly considered. These include a risk assessment of the costs, benefits and challenges; harmonization of new provisions with existing data protection laws and standards; ensuring trust in the process; necessary pilot projects and check-ups; proper procurement procedures; public testing and certification of equipment; contingency plans for technology failure; sufficient training for electoral staff; and effective voter and party awareness-raising. A gradual approach – piloting over several elections, starting with local elections – is recommended to build confidence in the system and to resolve technical issues for effective implementation, as it was mentioned in the Joint Opinion on the draft electoral code of Armenia[12].

2.2.1. Electoral Process

The VC also appointed relevant guidelines regarding voter registration[13]: «Effective measures in favour of voters abroad imply making their registration and the exercise of their right to vote as easy as possible, if necessary by multiplying the number of polling stations and voting methods (including postal, internet and proxy voting). If no precautions are taken, there is however a risk of electoral fraud»[14]. The Commission further stated: «A centralized register could also facilitate the collection and publication of data on the number and type of changes made to voter lists, which has been previously recommended by ODIHR as a means to enhance transparency»[15].

At the same time, the VC is aware of the need to use such a register – which includes «the voter's name, address, date and place of birth and place and conditions of voting to enhancing 'public control' over the Register» – strictly for its intended purpose. It notes that «political parties tend to act for political motives and may seek to use the Register for partisan purposes, perhaps as a tool for campaigning. The implementation of this provision will need to be monitored with careful scrutiny»[16].

---

[11] C. Fasone – G. Piccirilli, *Towards a* Ius Commune *on Elections in Europe? The Role of the Code of Good Practice in Electoral Matters in 'Harmonizing' Electoral Rights*, in *Election Law Journal: Rules, Politics, and Policy,* 16, 2017.

[12] Venice Commission, *Armenia — Joint Opinion on the Draft Electoral Code*, CDL-AD(2016)019, 2016, 66.

[13] For example, the *Summary report on voters residing de facto abroad* and the *Uzbekistan - Joint opinion on the draft election code*; both of them adopted by the Council for Democratic Elections.

[14] Venice Commission, *Summary Report on Voters Residing de facto Abroad*, CDL-AD(2015)040, 2015, 36.

[15] Venice Commission, *Uzbekistan — Joint Opinion on the Draft Election Code*, CDL-AD(2018)027, 2018, 45.

[16] Venice Commission, *Joint Opinion on the Draft Law on State Register of Voters of Ukraine*, CDL-AD(2007)026, 2007, 40.

This concern about the privacy impact of voter registration is also evident regarding voter identification. As one opinion observed, «the system will have to process and store personal data, which invokes the application of numerous standards for the processing of personal data through electronic means (…)»[17].

It was noted that identity controls at the polling station can be made more efficient through measures like issuing specific voter ID documents, using biometric measures to detect duplicate registrations, adopting anti-counterfeiting features on IDs, online verification of voters' identities, and controlled destruction of unclaimed ID documents. As appointed by the VC in the "Summary report on voters residing de facto abroad": «Fraud is made more difficult if supplementary measures are taken against the falsification of identity documents – for example by the use of biometric data […]. When a centralised electoral register is available (and reliable), an online verification of the identity of voters in this register also prevents double voting»[18].

The Commission's doctrine also references vote counting and results transmission. It cautions that while technology can improve the efficiency of tabulation, any legal provisions for its use must be accompanied by detailed regulations on technical solutions and procedures. These should cover procurement, testing, auditing, and public access to the technologies used. ODIHR and the VC therefore recommend that election codes include detailed provisions on the voting, counting and tabulation technologies and procedures, just as it was analysed in the joint opinion on the drat election code of Uzbekistan[19].

2.2.2. Electronic Vote

References to electronic voting are even more numerous and have also been explored from academic perspectives[20]. The VC noted in the Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report, that although «the advantage of these methods becomes apparent when a number of elections are taking place at the same time»[21]. Also, «electronic voting is neither generally permitted by human rights nor ruled out a priori. Instead, its acceptability depends on the legal, operational and technical standards implemented in the procedure»[22]. In other words, compatibility with democratic principles depends on adequate provisions

[17] Venice Commission, *Joint Opinion on the Draft Election Code of Bulgaria*, CDL-AD(2014)001, 2014, 66.

[18] Venice Commission, *Summary Report on Voters Residing de facto Abroad*, CDL-AD(2015)040, 2015, 39.

[19] Venice Commission, *Uzbekistan — Joint Opinion on the Draft Election Code*, cit., 102.

[20] R.M. Alvarez - I. Levin – J. Pomares – M. Leiras, *Voting Made Safe and Easy: The Impact of e-Voting on Citizen Perceptions*, in *Political Science Research and Methods*, 1(1), 2013, 117 ff.

[21] Venice Commission, *Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report*, CDL-AD(2002)023rev2-cor, 2002, 32.

[22] Venice Commission, *Report on the Compatibility of Remote Voting and Electronic Voting with the Standards of the Council of Europe*, CDL-AD(2004)012, 2004, 66.

in national law and practice, considering technical and social conditions. By request of Bulgaria for a joint opinion on its draft electoral code, the Committee of Ministers of the Council of Europe has underlined in its Recommendation (2004)11 that «e-voting shall be as reliable and secure as democratic elections and referenda which do not involve the use of electronic means»[23].

To strengthen guarantees, «the introduction of electronic voting – especially when conducted in an uncontrolled environment […] – should only be an alternative means to voting in a controlled environment. Remote electronic voting is particularly controversial because it cannot guarantee secrecy and it cannot be observed through the methods commonly applied to observation of voting in the controlled environment of a polling station. The adequacy of electronic voting in situations where confidence in the impartiality of the election administration is limited should be carefully evaluated. Should there be a decision to implement electronic voting, its legal basis should be drafted in an equally detailed and accountable manner as for traditional voting in a controlled environment»[24].

Similarly, the VC appointed some issues trough different joint opinions requested also by Bulgaria and Georgia in this topic. «While remote voting via the Internet and other forms of electronic voting are generally considered compatible with the standards of the Council of Europe, this compatibility largely depends on whether adequate technical security has been provided and social conditions in the country have been considered. As electronic voting via the Internet is an alternative voting channel to paper-based voting, its legal basis has to be drafted in an equally detailed and accountable manner»[25]. The VC adds that «the introduction of electronic voting should be done gradually (…) with contingency plans for backup voting arrangements should the electronic voting system fail»[26]. It considered it appropriate that «the idea to undertake experimental remote voting is in line with OSCE/ODIHR recommendations to have pilots before deciding on the increased and binding usage of new voting technologies»[27].

The *Code of Good Practice in Electoral Matters* states that «electronic voting should be used only if it is safe and reliable; in particular, voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage; the system must be transparent»[28]. It further explains that «electronic voting methods […] are secure if the system can withstand deliberate attack; they are reliable if they can function on their own, irrespective of any shortcomings in the hardware or

[23] Venice Commission, *Joint Opinion on the Draft Election Code of Bulgaria*, cit., 65.

[24] Venice Commission, *Joint Final Opinion on the Electoral Code of Armenia*, CDL-AD(2011)032, 2011, 62.

[25] Venice Commission, *Joint Opinion on the Election Code of Bulgaria*, CDL-AD(2011)013, 2011, 49.

[26] Venice Commission, *Joint Opinion on the Draft Election Code of Bulgaria*, cit., 66.

[27] Venice Commission, *Bulgaria — Joint Opinion on Amendments to the Electoral Code*, CDL-AD(2017)016, 2017, 77.

[28] Venice Commission, *Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report*, cit.

software. Furthermore, the elector must be able to obtain confirmation of his or her vote and, if necessary, correct it without the secrecy of the ballot being in any way violated. […] The system's transparency must be guaranteed in the sense that it must be possible to check that it is functioning properly»[29]. Likewise, the *Revised Code of Good Practice on Referendums*[30] stipulates that «electronic voting should be in conformity with the *Recommendation of the Committee of Ministers to member States on standards for e-voting*. In particular, it should be used only if it is secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters; the system must be transparent; unless channels of remote electronic voting are universally accessible, they shall be only an additional and optional means of voting»[31].

The VC has stressed that certain precautions are needed to minimize the risk of fraud in e-voting – for example, enabling the voter to immediately verify their vote after casting it. It noted that with such voting, ballot papers must be designed to avoid confusion. To facilitate verification and recounts, it may be provided that a machine could print votes onto paper ballots, placed in a sealed container. Whatever method is used must ensure vote confidentiality. «There should also be some kind of device for mixing the ballot papers so that if it proves necessary to open the container for checking, papers cannot be linked to particular voters – for example, those turning out early or late in the day», as it was mentioned in the *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe*[32]. Moreover, «to establish specific standards, it will be necessary to compare the precautionary measures for e-enabled voting with those for postal voting. In this context, it is necessary to ensure that the confidentiality of electronic voting is guaranteed by measures comparable with those applicable to postal voting – especially by preventing data manipulation, protecting anonymity to prevent possible disclosure of voters' choices, and by maintaining the authenticity and integrity of the votes cast»[33]

Also, a 2018 *Report on the Identification of Electoral Irregularities by Statistical Methods* warned that «the use of electronic election technologies might enable a single actor (including a foreign power) to completely control election results, absent a durable, tamper-evident, voter-verified paper trail that is used to check the electronic results by a rigorous audit»[34].

[29] *Ibid.,* 43-44.

[30] Venice Commission, *Revised Code of Good Practice on Referendums*, CDL-AD(2022)015, 2022.

[31] *Ibid.*

[32] Venice Commission, *Report on the Compatibility of Remote Voting and Electronic Voting with the Standards of the Council of Europe*, cit., 66.

[33] *Ibid.*

[34] Venice Commission, *Report on the Identification of Electoral Irregularities by Statistical Methods*, CDL-AD(2018)009, 2018, 31.

2.3. Freedom of Expression and Media Pluralism in the Digital Sphere

During this first stage, the VC also issued a series of opinions in response to country-specific requests on basic democratic issues like freedom of expression and freedom of association, which often had digital aspects.

To start, the VC found that an overly broad definition of "electronic publications" in a national law was problematic: it was «nebulously and broadly defined, therefore jeopardising clarity and foreseeability of the law's scope», which was mentioned in the opinion requested by Albania, regarding some amendments to its Audio-visual Media Service Law[35]. Furthermore, as journalism moves from print to Internet, «it is increasingly important that equivalent defences are provided in defamation laws to those who act, respectively, as mere conduits for information on the Internet or who host websites. It is also important that hosts are required to set up an effective (self-policing) notice and takedown procedure. In the *Opinion on the Legislation pertaining to the Protection against Defamation of the Republic of Azerbaijan*, requiring a complainant to go to court to get an order for takedown does not sufficiently protect the person defamed. In addition, this discourages Internet service providers from taking responsibility, once on notice, for the websites they host»[36].

On the ability to limit freedom of expression online, the VC opined in the case of Turkey, regarding the regulation of publications on the Internet and combating crimes committed by means of such publication ("the Internet Law"), that «the power of the Presidency [in this context, an administrative authority] to give ex officio blocking orders without prior judicial review should be removed and […] the duty to carry out the balancing between the right to privacy and the freedom of expression should, in the case of a decision with such serious consequences, be incumbent primarily on a judge and not on an administrative body»[37].

More recently, the VC ruled on an urgent request from Turkey, through a joint opinion with the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe, regarding the draft amendments to the Penal Code and the provision on "false or misleading information". It considered that while «information disorder (misinformation, disinformation and malinformation) is one of the important issues of these days and globally there is a need to tackle the serious problems of disinformation campaigns»[38], (in the case at hand «there was no pressing social need to introduce the criminal provisions, which would open the door to possible

[35] Venice Commission, *Albania — Opinion on Draft Amendments to Law No. 97/2013 on the Audiovisual Media Service*, CDL-AD(2020)013, 2020, 27.

[36] Venice Commission, *Opinion on the Legislation pertaining to the Protection against Defamation of the Republic of Azerbaijan*, CDL-AD(2013)024, 2013, 92.

[37] Venice Commission, *Opinion on Law No. 5651 (Regulation of Publications on the Internet — "the Internet Law"),* CDL-AD(2016)011, 2016, 72.

[38] Venice Commission, *Turkey — Urgent Joint Opinion on Draft Amendments to the Penal Code regarding "False or Misleading Information"*, CDL-AD(2022)034, 2022, 88.

threats and arbitrary restrictions of freedom of expression»[39]. The opinion also recalled the need to affirm and protect the right to anonymity on the Internet, to regulate and strictly limit the creation and use of profiles, and to ensure that users have easy access to their personal data held by ISPs[40].

2.4. Technological Aspects of the Exercise of Freedom of Association and Political Participation

In this overview of technology-related issues addressed by the VC, we also find those concerning certain technological aspects of the exercise of freedom of association and political participation.
On one hand, the advantages of using digital tools to facilitate participation are highlighted. By request of Uzbekistan, in the joint opinion of the VC and OSCE/ODIHR on the draft Law "On freedom of conscience and religious organisations", it was noted that «the submission of required documentation electronically may help facilitate registration, [but] when putting in place such mechanisms, it is essential to ensure that the registration procedure remains accessible to all, inclusive and non-discriminatory»[41]. Along the same lines, in the joint opinion regarding the draft law on the legislative initiative of the citizens from Albania, the Commission issued an opinion on the use of technology in the collection of signatures for citizens' initiatives, recommending clarification of the exact requirements for digital signatures to ensure equal treatment between the collection of traditional and digital signatures, and easy access to the process in both cases[42].
However, the availability of such information online may threaten privacy, leading the VC to clarify, in the joint opinion on draft laws on transparency in the funding of public associations in Ukraine, that «public disclosure – on the Internet – of personal and financial information on public associations' employees, donors and beneficiaries could not be justified»[43].

3. A Systematic Approach to the Use of Technology in Elections

In recent years, the VC has confronted the complex interplay between digital technologies and electoral processes in a more systematic way. As

[39] *Ibid.,* 89.

[40] *Ibid.,* 90.

[41] Venice Commission, *Uzbekistan — Joint Opinion on the Draft Law "On Freedom of Conscience and Religious Organisations"*, CDL-AD(2020)002, 2020, 80.

[42] Venice Commission, *Albania — Joint Opinion on the Draft on the Legislative Initiative of the Citizens (with OSCE/ODIHR)*, CDL-AD(2018)026, 2018, 33.

[43] Venice Commission, *Joint Opinion on Draft Laws No. 6674 and 6675 on Transparency in the Funding of Public Associations (Ukraine)*, CDL-AD(2018)006, 2018, 72.

elections increasingly involve online communication – from social media campaigning to artificial intelligence – traditional democratic safeguards face new challenges. The Commission's doctrine on this subject has been developed in a trilogy of key documents: a 2019 Joint Report on Digital Technologies and Elections (a study prepared with the Council of Europe's Information Society department)[44], the 2020 *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes*[45], and the 2024 *Interpretative Declaration of the Code of Good Practice in Electoral Matters as concerns Digital Technologies and Artificial Intelligence*[46]. Each document built upon the previous one, reflecting the rapid evolution of digital threats and the need to update electoral standards.

The Joint Report (2019) provided an exhaustive analysis of how social media, big data and other digital tools were affecting democracy, identifying risks ranging from online disinformation campaigns to the misuse of personal data and cyber-attacks on election infrastructure. Its conclusions offered detailed recommendations for states and international bodies to adapt legal frameworks and practices. The sobering assessment was that the Internet and social media, while empowering new forms of political participation, had also become avenues for manipulating voters and undermining fair elections on an unprecedented scale. It stressed that existing regulations were often inadequate in this "information age" and that urgent action was needed to protect electoral democracy. This has also been found as a concern in several studies and academic research[47].

In response to those findings, the VC in 2020 adopted a concise set of *Principles* aimed at guiding member states in regulating digital technologies during elections in line with European fundamental rights standards. These eight principles encapsulate the balance that must be struck between innovative electoral practices and the core values of democratic elections. The Commission noted that any legal response must respect freedoms – in particular freedom of expression, privacy and data protection, and electoral equality – even as it addresses the novel threats posed by borderless online political activity. The 2020 Principles highlighted issues such as ensuring a robust digital public debate, defining the power and duties of authorities to act against unlawful online content during campaigns, protecting an open Internet (net neutrality), providing effective safeguards for personal data, achieving transparency in online political advertising, and preventing cyber-threats to elections.

Finally, in 2024, the VC integrated these insights into its authoritative *Code of Good Practice in Electoral Matters*. The Interpretative Declaration on Dig-

---

[44] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections*, CDL-AD(2019)016, 2019.

[45] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* CDL-AD(2020)037, 2020.

[46] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, CDL-AD(2024)044, 2024.

[47] J.A. Tucker – A. Guess – P. Barberá – C. Vaccari – A. Siegel – S. Sanovich – D. Stukal – B. Nyhan, *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, in *ssrn.com*, 2018.

ital Technologies and AI updated the Code's application, making explicit how each fundamental principle of democratic elections – free suffrage, equal suffrage, secret suffrage, etc. – should be guaranteed in the context of digital innovation. This declaration, accompanied by an explanatory report, is now a reference point for election observation and reform, detailing concrete safeguards. It confirms, for example, that voters' freedom to form an opinion includes rights such as unimpeded access to diverse online information and private Internet communications, and it sets conditions on the use of artificial intelligence in campaigning. It also reinforces states' positive obligations to address phenomena like organized disinformation, while cautioning against undue state interference with political speech.

Across these documents, the VC's doctrine can be synthesized into major thematic areas: freedom of expression, equality of opportunity, protection of personal data, transparency in campaign financing, responsibilities of Internet intermediaries, guarantees in electoral administration, and others. Throughout, the language and approach reflect the style of the VC and the European Court of Human Rights – formal, precise and rooted in fundamental rights law as applied to new technological realities.

3.1. Freedom of Expression in the Digital Election Context

Freedom of expression – especially freedom of political debate – lies at the heart of any democratic election. The VC repeatedly affirms that the rights to free elections and to free expression are interdependent and mutually reinforcing[48]. In the digital age, this principle means that the vibrant exchange of ideas online must be protected during election periods just as it is offline. In the Principles for a fundamental rights-compliant use of technologies in electoral processes, the Commission stresses that political discourse enjoys the highest level of protection under Article 10 ECHR, and this extends fully to digital communications[49]. Voters and candidates alike have the right to use the Internet to impart and receive information, to engage in debate, and even to express controversial or critical opinions, without unreasonable hindrance[50]. The «free exchange of opinions and ideas» in the digital public sphere «is crucial for the democratic environment»[51]. Therefore, any regulation of online content around elections must be approached with great caution so as not to chill lawful political speech or skew the level playing field of debate.

[48] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections*, cit., 50.

[49] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 37.

[50] *Ibid.,* 47.

[51] *Ibid.,* 48.

3.1.1. Protecting Open Debate Online

A central tenet of the Commission's doctrine, drawing on the European Court of Human Rights (ECtHR), is that «principles from the Court's case law regarding freedom of expression must be translated into the digital environment»[52]. This implies, first, that the means of communication are protected alongside the content: restrictions targeting online platforms or social networks can interfere with Article 10 just as much as direct censorship of speech. For example, along these principles, it can be found that blocking access to websites or throttling Internet traffic during elections would generally violate the freedom to seek and impart information. The Commission explicitly supports the principle of **net** neutrality – the idea that Internet service providers should treat all data equally without discrimination – as essential to an open democratic debate[53]. Net neutrality guarantees a level playing field in the digital arena by preventing powerful gatekeepers from privileging or suppressing particular content or services for economic or political reasons. In the Commission's view, maintaining an "open Internet" is vital, especially during the crucial period of elections when voters must be exposed to diverse sources of information[54]. Member states are encouraged to legally safeguard network neutrality and users' equal access to online information as part of protecting freedom of expression[55].

At the same time, the VC acknowledges that some limited restrictions on expression are permissible to secure free and fair elections, provided they meet strict conditions. Drawing on ECtHR case law, in the joint report on Digital Technologies and Elections, appointed by the Commission and the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), it was noted that in the context of elections, states may impose certain narrow limits – for instance, campaign silence periods or rules against inflammatory speech – but only if they are clearly prescribed by law, pursue a legitimate aim (such as preventing violence or protecting voters from coercion), and are necessary and proportionate in a democratic society[56]. Any such measure must not become a tool for censorship or partisan advantage. The Commission reiterates that broad or arbitrary restrictions on online speech are unacceptable. For example, the blanket blocking of an entire online platform (as occurred in one case in Turkey[57]) was an overbroad measure violating Article 10[58]. The Commission thus urges governments to craft any content-based interventions with precision and to ensure ef-

[52] *Ibid.*

[53] *Ibid.,* 59.

[54] *Ibid.,* 64.

[55] *Ibid.,* 61.

[56] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 64.

[57] Freedom House, *Freedom on the Net 2014: Turkey,* Washington, D.C., 2014.

[58] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 54.

fective judicial oversight to guard against abuse[59].
The positive dimension of freedom of expression is also emphasised. In the 2019 joint report on digital technologies and elections, it was mentioned that the state must not merely refrain from interference, but has an obligation to «create a favourable environment for participation in public debate»[60].This positive duty entails actively preventing and sanctioning third-party interference with open debate, including interference by private actors[61]. For instance, if malicious groups engage in systematic online harassment of journalists or political candidates during the campaign, the authorities should be empowered to respond. The 2024 Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence makes this clear: «The State has an obligation to take effective steps to ensure a supportive environment for robust public debate, preventing and punishing infringements of voters' freedom to form an opinion, including by private actors»[62]. Here, the VC aligns with the principle that democratic governments must defend the integrity of the discussion space, which is an essential precondition for genuine elections. This may require updating electoral offenses to cover digital forms of intimidation or disruption. An independent body – such as an electoral commission or media regulator – should be mandated to enforce such rules impartially[63].

3.1.2. Countering Disinformation While Respecting Rights

One of the gravest concerns identified is the proliferation of online disinformation and propaganda campaigns aimed at misleading voters. The VC describes this "information disorder" – encompassing misinformation, disinformation, and malinformation – as a direct threat to voters' ability to form free and informed opinions[64].In the digital ecosystem, false or manipulative content can spread rapidly and widely, potentially encumbering voters' decision-making by drowning them in misleading narratives. Organized disinformation, sometimes amplified by automated bots or fake social media accounts, can distort public discourse and even suppress voter turnout or trust in the electoral process. The Commission warns that this polluted information environment «may distort the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to

[59] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 137.

[60] *Ibid.,* 51.

[61] *Ibid.,* 115-121.

[62] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 12.

[63] *Ibid.,* 54.

[64] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 39.

influence their votes»[65]. In other words, large-scale online falsehoods undermine the very *free suffrage* that genuine elections require.

Crucially, however, the VC advocates responses to disinformation that do not themselves undermine freedom of expression. The joint report on digital technologies and elections cautions that any measures to combat "fake news" must be designed with great care so as not to become a pretext for censorship[66]. The Commission invokes the principle of net neutrality here: heavy-handed filtering or blocking of content could violate the openness of the Internet and quash legitimate speech along with false content[67]. Therefore, rather than expansive state content bans, the Commission favours a combination of alternative strategies to counter false information:

- Independent fact-checking and rapid response initiatives to debunk viral falsehoods.[68]
- Media and digital literacy programmes to educate the public on how to identify and resist disinformation – including incorporating social media literacy into school curricula and running public awareness campaigns about the perils of online propaganda.
- Support for quality journalism and diverse news sources (including strong public service media and local news outlets) to ensure voters have access to accurate information[69].
- Codes of conduct or self-regulation for online platforms to prompt them to voluntarily police clearly harmful false content.

By strengthening the "accuracy and reliability" of news and empowering voters to critically evaluate what they see online, these measures seek to inoculate democracy against disinformation without resorting to speech bans. The Commission also notes the importance of transparency from platforms: for example, labelling state-sponsored media or providing context for contested information can help users gauge the truthfulness of content[70].

As indicated in the "Principles for a fundamental rights-compliant use of digital technologies in electoral processes", where content restrictions are unavoidable – for instance, to remove illegal content like incitement to violence or voter intimidation – the Commission insists on clear legal frameworks and due process. Under Principle 2 of the 2020 guidelines, during electoral campaigns a competent independent authority (an electoral commission or a court) should have power to order the prompt removal of unlawful third-party content online (e.g. egregious defamatory material or illegal propaganda), but only if defined by law and in line with international freedom of expression standards[71]. Any such take-down decisions

[65] *Ibid.,* 144.

[66] *Ibid.,* 137.

[67] *Ibid.,* 139.

[68] *Ibid.,* 38.

[69] *Ibid.,* 152.

[70] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 75.

[71] *Ibid.,* 55.

must be subject to speedy judicial review to prevent abuse or error[72]. The Commission stresses that private companies (social media firms, etc.) have responsibilities in this regard, but their content moderation should not occur in a legal void: there must be oversight to ensure they do not become unaccountable arbiters of truth[73].

The 2024 "Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence" reinforces this delicate balance. It states that «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»[74]. Thus, while authorities are expected to act against malign interference (e.g. foreign disinformation campaigns or cyber-propaganda), they must refrain from overbroad measures that would infringe fundamental freedoms or tilt the electoral playing field. The declaration specifically addresses "political deepfakes" – AI-generated fake videos or audio that deceptively impersonate candidates or spread false statements. The Commission's stance is unequivocal: such intentionally deceptive use of artificial intelligence to mislead voters or undermine their free formation of opinion «should be prohibited and sanctioned» by law[75]. Voters have a right to know when they are interacting with an AI-driven account or content rather than a real person, and the use of deepfake technology to falsify political content is seen as an unacceptable fraud on the electorate. Banning deepfakes in campaigns, under tailored legislation, is thus one of the few categorical content restrictions the Commission endorses – precisely because deepfakes by their nature subvert truthful debate and informed voting.

In summary, the VC advocates a holistic approach to safeguarding freedom of expression in elections: protect the digital public square as a space of open debate; empower citizens and media to counter falsehoods with truth; and narrowly target the most harmful forms of disinformation (like deepfakes or illegal content) through transparent legal processes. All such efforts should reinforce the electorate's ability to hear all sides and make political choices free of coercion or deception. The overarching message is that free expression is "the lifeblood of democracy" – even more so online – and must be preserved, while intelligently mitigating the new risks that the Internet poses to democratic discourse, which was also mentioned in the 2019 joint report on digital technologies and elections.

3.2. Equality of Opportunity and Fairness in Online Campaigning

Equal suffrage, in its qualitative sense, means that all candidates and parties should enjoy a fair and level playing field during an election. The VC's *Code of Good Practice* defines "equality of opportunity" as a core principle,

[72] *Ibid.,* 57.

[73] *Ibid.,* 15.

[74] *Ibid.,* 20.

[75] *Ibid.,* 8.

requiring that incumbents and challengers, large parties and small parties, are treated without discrimination by the law and authorities[76]. In the digital context, this principle faces novel tests. Online campaigning is not constrained by the traditional equal-access rules (like equal broadcast time on public TV) that many countries use to ensure fairness. Powerful actors can spend lavishly on social media ads, micro-target only certain voter segments, or leverage platform algorithms to amplify their messages disproportionately. Meanwhile, smaller or resource-poor actors might struggle for visibility amid the online cacophony. The VC has grappled with how to extend equality of opportunity into this new terrain so that electoral competition remains fair and genuinely competitive.

The 2024 Interpretative Declaration explicitly asserts that «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»[77]. In other words, the principle is technology-neutral: just because campaigning has moved online does not mean the requirement of equal conditions fades away. The declaration outlines several aspects of what fairness in online campaigning entails:

- Fair access to media and platforms: Candidates and parties must have reasonable access not only to public-service media, but also – to some degree – to privately owned online media and platforms. Traditionally, many democracies ensured equal opportunity by giving all candidates some airtime on state broadcasters. The Commission suggests that analogous thinking should apply to dominant social networks or video-sharing services if they are crucial channels for political communication. Legal provisions might guarantee a minimum access for all contestants to such privately run platforms, preventing these companies from arbitrarily denying service or favouring one political actor over another[78]. This does not mean private companies lose the right to moderate content, but there should be no discrimination on political grounds.
- Non-discriminatory content dissemination: Beyond access, equality of opportunity in the digital realm «encompasses the principle of fairness in content dissemination and access»[79]. This points to the role of algorithms and recommendation systems. If, for example, a platform's algorithmic news feed tends to create echo chambers or systematically promotes content from major parties while marginalising others, it could undermine equal exposure. The Commission implies that transparency or oversight of such algorithmic processes may be necessary to ensure smaller or newer political voices are not algorithmically silenced. States might encourage or require platforms to provide options for users to encounter a diversity of political content, or to avoid

[76] Venice Commission, *Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report*, cit., 27.

[77] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 9.

[78] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 4.

[79] *Ibid.,* 10.

practices that amount to partisan bias in distribution. The principle of net neutrality reinforces this, demanding that ISPs and platforms do not unfairly throttle or boost particular political content[80].

Another critical component of equal opportunity is financial fairness. If one party can vastly outspend others online – especially through unregulated channels – the playing field tilts. The VC observes in the "Principles for a fundamental rights-compliant use of digital technologies in electoral processes", that many existing campaign finance limits (for example, caps on TV advertising purchases or overall spending limits) have become «less meaningful in times of digital advertising»[81]. A relatively small budget can buy enormous reach on social media through micro-targeted ads, often evading traditional disclosure rules. Moreover, foreign or illicit funding can be channelled into online campaigns with less chance of detection.

To address this, the 2019 Joint Report urged that states:

- Update spending limits and reporting requirements to include expenditures on Internet-based platforms, online influencers, data analytics services, etc., not just traditional media.
- Introduce new measures covering micro-targeting – for instance, requiring that when campaigns use targeted online adverts, they report the categories of audiences targeted and the funds spent on each, to allow oversight of whether certain voter groups are being inundated or ignored.
- Enhance monitoring capacity of national authorities so they can effectively track digital campaign expenditures, possibly by investing in new tools or training to audit online ad libraries and trace funding flows[82].

The Commission also flags the problem of "political redlining" – the practice of only engaging with voters deemed electorally valuable (swing voters) and ignoring "safe" districts or opposition strongholds. Micro-targeting exacerbates this by enabling extreme selectivity. While such strategies are not outright illegal, they raise concerns for the ideal of broad-based campaigning and equal voter influence. If whole segments of the electorate receive no information because they are algorithmically written off, the spirit of equal suffrage suffers. The Commission's solution, mentioned in the principles, is largely to shine light on these tactics: transparency in online campaigning can discourage extreme segmentation and ensure voters are aware when they are being targeted or omitted[83].

To concretely bolster equality, the Commission and other Council of Europe bodies have suggested specific regulatory frameworks for online election content. The VC echoes the Parliamentary Assembly in saying that «where political parties and candidates have the right to purchase advertising space for election purposes, [they should have] equal treatment

[80] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes, CDL-AD(2020)037*, cit., 60.

[81] *Ibid.,* 72.

[82] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 152.

[83] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 72.

in terms of conditions and rates charged»[84]. Additionally, any sponsored political content on social media should be clearly labelled and traceable to its source, so that the public knows who is behind it[85].

The 2019 Joint Report also notes the decline of the "journalistic ethics filter" in online politics[86]. In the past, professional journalists and editors acted as intermediaries, applying standards of balance and verification that indirectly enforced fairness (e.g. giving a right of reply, or covering all major parties). Now, campaigns can communicate unmediated via Facebook or YouTube, bypassing those norms. To compensate, the Commission advocates encouraging self-regulation among online political advertisers and platforms – for instance, adopting voluntary codes that commit to fairness and truthfulness in political ads[87]. Furthermore, supporting independent fact-checkers and watchdog NGOs can help maintain an equitable information environment by calling out unfair smear campaigns or disproportionate coverage[88].

In summary, equality of opportunity in digital campaigning demands updating and expanding legal safeguards so that no candidate enjoys an undue advantage online. Through the Interpretative declaration of the Code of good practice in electoral matters and also the joint report on digital technologies and elections, the VC's doctrine calls for: guaranteeing minimum access for all competitors to key communication channels, including private online platforms[89]; insisting on non-discriminatory treatment by Internet intermediaries in content curation and dissemination; transparency and limits in online political advertising to prevent money or data-driven tactics from giving one side an unfair edge[90]. This includes disclosing sponsors and spending, and possibly banning certain micro-targeted ads during the sensitive pre-election period[91]. It also means ensuring that if any actor uses the online sphere for campaigning, others are not de facto prevented from doing likewise under equivalent terms and costs[92].

Ultimately, equal suffrage in the digital age means every voter's voice has equal weight and every candidate has a fair chance to reach voters, regardless of the new technologies deployed. The VC's recommendations strive to preserve that ideal against the distortions that unregulated digital cam-

---

84 *Ibid.,* 74.

85 *Ibid.,* 99.

86 *Ibid.,* 124.

87 *Ibid.,* 97.

88 C. López-Marcos - P. Vicente-Fernández, *Fact Checkers Facing Fake News and Disinformation in the Digital Age: A Comparative Analysis between Spain and United Kingdom*, in *Publications,* 9(3), 2021, 36.

89 Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 10.

90 Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 152.

91 Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 11.

92 Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 168.

paigning might introduce.

3.3. Protection of Personal Data and Voter Privacy

The right to privacy and the protection of personal data have emerged as central concerns in digital-era elections. Modern political campaigns often rely on harvesting and analysing vast quantities of personal data – from voter rolls and social media profiles to browsing histories and consumer habits – to micro-target messages and predict voter behaviour. While data-driven techniques can increase efficiency, they pose significant risks to individuals' privacy and the fairness of elections. The VC underscores that Article 8 of the ECHR (right to privacy) and data protection principles must be rigorously upheld during electoral processes[93]. Voters should be able to participate in elections without fear that their personal information will be misused, and they should be free from undue surveillance or manipulation based on hidden data profiles.

The Commission's 2020 Principles devote an entire principle to data protection (Principle 4), stating succinctly: «Personal data need to be effectively protected, particularly during the crucial period of elections»[94]. This emphasises that election times are especially sensitive – political actors have heightened incentives to exploit data, and citizens are often required to share data (e.g. when registering to vote). Key elements of the Commission's doctrine on data protection include:

- Compliance with international standards: All processing of personal data for electoral purposes must comply with established data protection principles, notably those in Convention 108+ (the Council of Europe's modernized Data Protection Convention) and, where applicable, the EU GDPR. Convention 108+ is highlighted as the "universal treaty for data protection" that states worldwide should adopt[95] and the Commission urges that its robust standards (lawful basis for processing, data minimisation, purpose limitation, etc.) be the baseline for handling voter data[96]. The VC even suggested that the Council of Europe might develop a specific legal instrument to address the high risks of digital tech in political campaigns with regard to personal data[97].
- Limitations on automated decision-making: The use of algorithms and artificial intelligence to make decisions that significantly affect voters – for example, profiling individuals to determine who should receive which political ads, or decisions like removing people from voter rolls

[93] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 66.

[94] *Ibid.,* 16.

[95] *Ibid.,* 65.

[96] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 67.

[97] *Ibid.,* 152.

– is of particular concern. The 2024 Interpretative Declaration asserts that individuals «should not be subject to a decision based solely on automated processing of data which significantly affects them», unless certain safeguards are met. In the electoral context, this could apply to automated voter registration systems, automated content curation shaping someone's political information diet, or AI-driven moderation of political content. The Commission insists that human oversight and the possibility to contest such decisions are essential. Specifically for voter registration, the declaration adds that removal from electoral lists must not be decided solely by algorithms – except if the law expressly permits it with appropriate safeguards or the person has explicitly consented[98]. This ties into the broader data protection principle (in Convention 108+ and EU law) that individuals have the right not to be subject to purely automated decisions with legal or similarly significant effects on them, unless certain conditions (like explicit consent) apply[99].

- Consent and sensitive data: Political opinion data is classified as highly sensitive. The Commission notes that when data revealing political views is processed (for instance, inferring someone's political leanings from their Facebook activity), often the explicit consent of the individual is required as an extra layer of protection.[100] Moreover, voters should be able to easily withdraw consent if they later object. The Commission echoes recommendations that users be provided straightforward privacy controls – for example, the ability to "opt out" of political micro-targeting altogether[101].
- Purpose limitation and data minimisation: Data collected for one purpose (say, social networking) shouldn't be repurposed for electioneering without permission. The Commission reminds that under Convention 108+ principles, personal data in elections should only be processed for specified, legitimate purposes and not excessively. For instance, electoral rolls are collected to administer voting; using them to target campaign messages might go beyond the original purpose, unless the law explicitly allows some use while balancing privacy. There is often a tension between transparency and privacy here: making voter lists public can aid transparency and canvassing, but can also expose personal information. The Commission suggests privacy must be «balanced against the transparency required for electoral integrity» in such cases[102].
- New privacy rights for the digital age: The Commission posits that the traditional privacy right of the secret ballot should be conceptually expanded in the digital age. Beyond just keeping one's vote secret, voters

[98] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 26.

[99] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 69.

[100] *Ibid.,* 66.

[101] *Ibid.,* 67.

[102] *Ibid.,* 66.

should have a right to privacy in the pre-voting phase – i.e. the right to gather information and deliberate without undue monitoring[103]. This implies a right to private online browsing of political material and private communication regarding one's political opinions[104]. If a voter is being tracked across websites and then bombarded with tailored political ads or misinformation, their freedom to form an independent opinion is compromised. Therefore, the Commission underscores that online surveillance of voters' activities for campaign purposes should be tightly regulated. Voters should, for example, be free to research issues or interact in forums without fear that all those digital traces will be compiled to manipulate them.

The misuse of personal data for electoral gain is singled out as a major threat in the 2019 report and outlined in the 2020 Principles for a fundamental rights-compliant use of digital technologies in electoral processes. It warns that «the use and abuse of personal data for electoral purposes, cloaked as freedom of commerce, might pose a serious threat to free elections and electoral equity»[105]. Three specific dangers are noted: (1) Private actors using detailed personal information to exert undue influence on voters (for instance, micro-targeting susceptible individuals with manipulative messages tailored to their psychology); (2) Internet and social media companies, under the guise of their business freedom, potentially restricting access to certain political information in a non-transparent way (e.g. algorithmically down-ranking content from certain candidates), thus giving an opaque advantage to some; and (3) The commodification of personal data undermining campaign finance rules – data about voters is bought and sold as a commodity, which can be a form of unmonitored campaign expenditure or even facilitate foreign interference. All these practices, the Commission notes, «could facilitate, conceal or even constitute offenses against democracy», and should be prosecuted and sanctioned where they violate laws[106].

To strengthen personal data protection in elections, the VC recommends states take measures such as:

- Empowering Data Protection Authorities (DPAs) to actively supervise political campaigning. In some countries, DPAs have issued guidelines or sanctioned parties for unlawful data use. The Commission favours close cooperation between electoral authorities and DPAs during election periods[107]. For example, if a breach of voter data occurs or a party obtains data illicitly, there should be swift investigation.
- Mandating transparency from campaigns and platforms about how they use personal data. Voters should be informed if they are being

[103] *Ibid.,*

[104] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence,* cit., 5.

[105] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 152.

[106] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 58.

[107] *Ibid.,* 57.

micro-targeted and on what basis (e.g. "You are seeing this ad because you were identified as a young urban voter interested in environmental issues"). Such transparency allows voters to understand when their data profile is influencing the content they see.

- Ensuring effective remedies: Individuals should have the ability to access their personal data held by political parties or platforms and to correct or delete it. This ties into general data subject rights in privacy law, which should be operational even during campaigns.
- Considering new rules on surveillance technologies: The 2019 report floated the idea that the Council of Europe could develop guidelines on restricting surveillance tech during elections[108]. This includes not just state surveillance, but also private companies using invasive tracking. For instance, the use of spyware or excessive tracking cookies for campaign purposes should be off-limits.

In practical terms, the Commission applauds efforts like the Global Network Initiative's principles on freedom of expression and privacy, which aim to guide the ICT industry in respecting privacy rights. It also notes that some countries have begun to ban certain data practices – for example, several jurisdictions prohibit political parties from using personal data that reveals ethnic origin, health status or other sensitive traits for campaigning, as this could be discriminatory.

In conclusion, the VC's doctrine places data protection at the forefront of fair elections in the digital era. It recognises that if voters are micro-targeted in a manipulative way or if their personal lives are data-mined without consent, both their individual dignity and the collective freedom of the election are at stake. As such, robust data protection rules – grounded in Convention 108+, requiring consent, transparency, and data security, and giving individuals control – must be rigorously enforced when digital technologies intersect with electoral campaigns. The Commission's guidance urges states to treat abuses of voter data as serious electoral offences and to continually adapt their laws to confront emerging threats such as AI profiling or cross-border flows of voter information.

3.4. Transparency in Digital Campaign Financing

Transparent and fair campaign financing is a cornerstone of democratic elections. Voters have the right to know who is funding political messages and how much money is being expended to influence their vote. Moreover, rules on campaign finance (such as spending limits, donation caps, and disclosure requirements) aim to prevent excessive or opaque money from undermining the principle of equal opportunity. The VC notes that digital campaigning has upended traditional campaign finance controls, creating loopholes that must be closed to preserve transparency and accountability. Many campaign finance regulations were designed for

[108] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 151.

an offline world and thus «their applicability and efficacy turned out to be severely limited in the information age», as mentioned in the Principles for a fundamental rights-compliant use of digital technologies in electoral processes[109]. Campaigns can now raise and spend money online in ways regulators might not easily trace – for instance, through decentralized online donations or purchasing targeted ads from foreign companies. Also, in-kind contributions like data analytics or influence operations provided by third parties (sometimes from abroad) complicate the picture of who is financially behind a campaign. For example, laws might cap TV advertising purchases but impose no limits on social media ads, or require reporting of expenditures on official campaign materials but not on hiring online influencers or running a bot network.

To address this, the VC calls for a comprehensive revision of campaign finance rules to cover digital campaigning. In its conclusions, the 2019 report specifically recommended action in the following areas[110]:

- Updating legal definitions of campaign expenditure to include online communication costs. Legislation should make it explicit that money spent on Facebook ads, Google search promotions, mass SMS messages, campaign mobile apps, etc., counts as campaign spending subject to limits and disclosure.
- Expanding disclosure obligations to new categories: Parties and candidates should report not only classical expenses (rallies, posters, TV spots) but also digital services – for instance, fees for data mining, consulting payments to social media firms, or outsourcing of digital campaign strategy.
- Requiring detailed transparency for online ads: The Commission urges that Internet intermediaries be obliged to maintain and publish *ad libraries* for political advertisements. These archives would show each political ad, its sponsor, cost and the audience targeted. This allows both the public and oversight agencies to scrutinise how campaigns are using online ads and to detect anomalies such as foreign-funded ads or disproportionately large expenditures aimed at narrow groups.
- Ensuring foreign funding bans extend online: Many countries ban or restrict foreign donations to domestic campaigns. However, without specific rules, a foreign entity could simply purchase online ads or pay influencers to support a candidate, evading donation routes. The Commission notes that prohibiting or tightly controlling foreign or anonymous online campaign spending is necessary. Campaigns should not be able to hide behind Internet anonymity to receive illicit support. Measures like requiring payment for political ads to come from a domestic account, or cooperation with platforms to flag foreign-sponsored content, can enforce this.

Also, in the Principles for a fundamental rights-compliant use of digital technologies in electoral processes, the Commission places strong emphasis on the responsibility of Internet intermediaries (social media compa-

[109] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 72.

[110] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 152.

nies, ad networks) to contribute to transparency. Under Principle 5 of the 2020 guidelines, recalling the Joint Report, «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»[111]. In practice, this means companies like Facebook or YouTube need to share information about political ads with regulators and researchers: who paid for the ad, how much was spent, whom it reached, etc. Some major platforms have begun doing this via voluntary transparency archives, but the Commission's position implies it should be a legal requirement backed by regulation.

The VC cites the lack of transparency in digital spending and the «difficulties in tracking the sources of campaign financing» as pressing problems[112]. For instance, if a political party contracts an overseas data analytics firm that runs social media campaigns on its behalf, tracing that money flow can be hard under current rules. The Commission encourages states to impose clear record-keeping and reporting duties on parties for all services procured, including those online and abroad. Additionally, cross-border cooperation may be needed: election authorities might have to coordinate with foreign counterparts or international bodies if money is moving transnationally (linking to a later point on international cooperation).

Transparency is also needed for issue-based advertising. Modern online campaigns often involve not just direct candidate ads, but also third-party groups running campaigns on wedge issues (e.g. immigration or healthcare) that indirectly favour one side. These might not be covered by narrow definitions of campaign advertising. The Commission recommends broadening transparency to cover «sponsored content on social media» related to elections[113]. The public should know if a viral article or meme on a political issue was in fact paid for by a campaign or an allied organization. By extending sponsor-identification requirements to social media content, voters can better evaluate the material they see.

Beyond rules and disclosure, the Commission acknowledges a deeper question: is transparency enough to tackle the outsized influence of money in online campaigns? It notes in the 2020 principles that while transparency is critical, it might not alone prevent the problem that «financial power can manipulate the electoral process to the extent that democracy is severely threatened»[114]. In the online arena, targeted ads can enable wealthy actors to proliferate «highly targeted and often misleading messages», raising concerns that even fully disclosed spending could still skew an election[115]. Some have argued that more direct restrictions on online political advertising are needed – for example, banning certain forms of paid political ads, at least during the immediate campaign period. The Interpretative Declaration reflects this by mentioning that «banning certain forms of

[111] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes*, cit., 73.

[112] *Ibid.,* 72.

[113] *Ibid.,* 74.

[114] *Ibid.,* 77.

[115] *Ibid.*

paid political advertising on social media during electoral periods may be an option, particularly when automated mass dissemination or micro-targeting techniques based on AI are being employed»[116]. This suggests that if transparency and self-regulation do not suffice to curb the pernicious effects of micro-targeted propaganda, states could consider temporarily prohibiting micro-targeted political ads in the run-up to elections. Some jurisdictions have indeed experimented with such bans or moratoria, given that micro-targeting can be used to spread tailored falsehoods in ways invisible to the broader public.

Another aspect of campaign finance in the digital age is in-kind contributions by platforms. For example, a social network might offer free promotional tools to one campaign (perhaps as part of a commercial partnership) or fail to enforce its terms evenly. The Commission implies that regulators should watch for any indirect subsidies or unequal treatment by platforms that could count as a contribution in kind. If a company's algorithm change suddenly boosts the visibility of a candidate's posts without explanation, is that a neutral business decision or a hidden contribution? These are complex questions, but the principle is that any such advantages should be transparent and ideally neutralised.

In concrete terms, the Commission's recommended steps for transparency in digital campaign finance can be summarised:

- Mandate disclosure of all online campaign expenditures.
- Enhance real-time transparency: In fast-moving online campaigns, reporting once after the election is too late. Mechanisms for more frequent or continuous disclosure (e.g. within 24 hours of an online ad purchase) could be instituted.
- Ensure equal opportunity in fundraising, if relevant: while not explicitly covered by the Commission, by extension equality concerns mean crowdfunding or online fundraising platforms should be equally accessible and not biased.
- Strengthen oversight bodies: Give electoral commissions or other oversight agencies the technical tools and legal authority to monitor online spending and enforce rules in cyberspace. This may involve new units staffed with data analysts or cooperation with tech companies.

The "Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence" adds an important point: «online electoral advertising must always be clearly identified as such and be transparent regarding the identity of its sponsor and the dissemination technique used»[117]. This encapsulates the transparency ethos – no political ad should masquerade as organic content or hide who paid for it; and if an ad is being micro-targeted or boosted by AI algorithms, that fact should be openly disclosed.

By implementing such measures, the overall aim is to prevent a situation where dark money or clandestine advertising warps the electoral playing

[116] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 11.

[117] *Ibid.*

field. Transparency shines light on attempts to flood social media with paid influence, enabling voters and authorities to react appropriately (whether through public pressure or sanctions for illegal funding). The VC's doctrine clearly views financial transparency and updated regulation as indispensable for maintaining trust in elections: voters should be confident that they are choosing their representatives in a contest of ideas, not one of hidden purses.

3.5. Responsibilities of Internet Intermediaries and Platforms

Perhaps the most novel aspect of the VC's doctrine on digital elections is its focus on the role of Internet intermediaries – primarily social media companies, search engines, online content platforms, and Internet service providers. As stated in the joint report on digital technologies and elections, these private actors have become the key gatekeepers of information in modern elections, effectively controlling the "information highways" over which political discourse travels[118]. Unlike traditional media (television, newspapers, radio), which are often bound by election regulations and journalistic standards, tech companies historically operated in a largely unregulated space with respect to political content. The Commission recognises that this new reality calls for rethinking responsibilities: the few dominant private companies in the digital sphere cannot be allowed to exercise unchecked power over democratic debate[119]. At the same time, the Commission is wary of simply handing control to the state – it advocates a model of co-responsibility where both public authorities and the platforms themselves work together to uphold democratic principles.[120]

The 2019 Joint Report vividly described the problem: «The small number of very powerful private actors that literally own the information highways have their own commercial interests and rights that tend to collide with both civil and political rights and electoral principles»[121]. These companies (think of major social networks or search engines) have assumed the role once played by editors and broadcasters in shaping public discourse, but «without however having adopted the ethical obligations of the media»[122]. In practice, platforms make decisions – through algorithms or content-moderation policies – about what political speech is amplified, suppressed or removed, yet they do so with minimal transparency or accountability. This can result in private censorship (removing content deemed "harmful" in opaque ways) or, conversely, tolerating abusive content that should be curtailed, all outside the framework of public law.

To address this, the VC suggests moving towards co-regulation and

[118] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit.,

[119] *Ibid.,* 143.

[120] *Ibid.,* 149.

[121] *Ibid.,* 145.

[122] *Ibid.,* 145.

self-regulation frameworks that impose greater responsibility on intermediaries. The Commission «reiterates the need to strengthen the international legal framework in order to establish more efficient mechanisms of transnational co-operation among nations and private actors», and to strive for uniform rules across jurisdictions. This implies developing international norms or agreements that set baseline duties for Internet companies during elections (further discussed under international cooperation). It also calls for regulatory models based on co-responsibility of state and private sector, combined with promotion of self-regulation. For example, states might set certain binding requirements (like transparency reports, data access for auditors, prompt removal of illegal content upon notice) while platforms themselves create and enforce codes of conduct that meet or exceed those requirements. An example cited is the idea of mandating corporate social responsibility and ethics codes for social media and tech firms[123]. Under such codes, a company might pledge to avoid algorithmic practices that unfairly favour one political viewpoint, or to voluntarily flag bot accounts and fake pages.

The Commission notes some progress: major firms have begun self-regulatory steps (Facebook, Google and Twitter signing an EU Code of Practice on Disinformation, creating ad archives, etc.). However, in the joint report on digital technologies and elections, it emphasises that these are «voluntary and unregulated» initiatives without a rule-of-law framework[124]. Ultimately, voluntary action is not enough; there must be oversight and potential sanctions to ensure compliance. The Commission cites that private companies' priority is profit, not protecting freedom of expression, so relying purely on their goodwill could leave fundamental rights vulnerable.[125]

Key responsibilities and actions for intermediaries that the VC highlights include:

- Transparency and accountability: Platforms should be transparent about their algorithms, content-moderation policies and business models as they affect political content[126]. For instance, if a platform curates news feeds, it should disclose the criteria. If it removes content or accounts (like disinformation networks), it should provide reasons and allow appeals. The Commission aligns with Council of Europe recommendations demanding transparency and accountability of intermediaries[127]. One concrete proposal is to develop a "Digital Corporate Responsibility Certificate"[128]. This concept, inspired by ISO standards, would certify companies that meet benchmarks for

[123] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes*, cit., 59.

[124] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 145.

[125] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes*, cit., 98.

[126] *Ibid*, 73.

[127] *Ibid.*

[128] *Ibid.,* 91.

accountability, transparency, ethical behaviour, human rights respect, etc., providing an incentive to uphold democratic values.

- Co-operation with authorities: Intermediaries should cooperate with election regulators and law enforcement (for cybercrime or foreign interference probes), as well as with oversight bodies. The 2024 declaration states that «provisions should be established to ensure the co-operation of Internet intermediaries and other private actors with governments, among themselves, and with academia and civil society»[129]. This multi-stakeholder cooperation could involve sharing data about disinformation trends, jointly developing tools to counter them, or collaborating in crisis situations (e.g. a major hacking or disinformation operation during an election).
- Rapid response to illegal content: While maintaining freedom of speech, companies should act quickly to remove or limit clearly illegal content (such as calls to violence, voter intimidation, or hate speech) when notified by competent authorities[130]. The intermediary has a duty to comply promptly[131]. Additionally, companies could proactively detect and curb blatantly unlawful activities (for example, foreign entities running ads in violation of law).
- Political advertisement policies: The Commission expects platforms to uphold strict standards for political ads – verifying the identities of advertisers, disallowing anonymous or falsely sponsored ads, providing libraries of ads, and possibly restricting micro-targeting. Some platforms have instituted such policies, but making them uniform and enforceable is key.
- Combating bots and fake accounts: Intermediaries have a responsibility to identify and eliminate inauthentic accounts or automated bots that spread disinformation or artificially amplify political messages. The 2020 principles note approvingly that platforms have taken steps like "deletion of fake accounts" and requiring authentication for political ads[132]. These efforts should continue and be strengthened, with due regard not to sweep up legitimate anonymous speech in the process.
- User empowerment: Companies should empower users with tools and information – e.g. explain "Why am I seeing this political content?" or provide options to report suspected disinformation. The Commission suggests that platforms should at least warn users «of potential risks implied by certain publications or sources»[133]. For example, if a news article trending on a platform is from an unverified source known for propaganda, the platform might label it or provide context.

The VC also underscores that any privatised regulation must not bypass

[129] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 19.

[130] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 56.

[131] *Ibid.,* 57.

[132] *Ibid.,* 99.

[133] *Ibid.*

the rule of law. There is concern about leaving too much content policing in the hands of tech executives or algorithms. As the Commission puts it, unaccountable private content regulation could turn companies into "semi-tribunals" without judicial oversight, which is unacceptable[134]. Therefore, it advocates for alternative dispute-resolution and appeals mechanisms for users whose content is removed or accounts suspended by platforms[135]. Users should have a right to challenge platform decisions and ultimately to access a court if needed. Transparency in company policies and moderation outcomes is also needed so independent observers can verify that fundamental rights (like non-discrimination and free speech) are not being unjustly curtailed.

The co-responsibility model is outlined in the 2019 recommendations: «Work on a regulatory and adjudicatory model based on the co-responsibility of private and public actors, and on multiple regulatory and conflict-resolution approaches»[136]. It then lists strategies like promoting self-regulation, providing remedial mechanisms, etc. The message is that governments alone cannot solve these problems, nor can companies be left alone to self-police – they must work in tandem, with civil society and experts contributing.

Finally, in the "Principles for a fundamental rights-compliant use of digital technologies in electoral processes" the Commission envisions continuous research and monitoring. It encourages cooperation with academics and experts to assess the real impact of digital tech on elections and the effectiveness of measures taken[137]. Platforms should share data (in privacy-compliant ways) with researchers so that society can gauge, for instance, how much disinformation is circulating or what effect a content policy change had. This knowledge is crucial to refining regulation over time.

In summary, the VC's doctrine assigns significant responsibility to Internet intermediaries to uphold democratic standards, but within a framework of law and shared oversight. Key expectations include transparency, fairness, proactive measures against malicious activities, and collaboration in safeguarding electoral integrity. While respecting their freedom to do business and innovate, these companies must recognise that with their immense power comes a duty not to harm the democratic process. The Commission essentially calls for bringing major platforms out of the legal grey zone and integrating them into the rule-of-law system governing elections – albeit in novel and flexible ways reflecting their global, fast-changing nature.

---

134 Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 96.

135 Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 97.

136 Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 149.

137 Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes*, cit., 90.

3.6. Safeguards in Electoral Administration and Cybersecurity

Elections rely not just on campaigns and media, but also on the administration of the voting process itself – voter registration, voting methods, vote counting, results transmission, and oversight mechanisms. The introduction of digital technologies into these administrative components (often termed "e-election" elements, such as electronic voting machines, online voter registers, or blockchain vote tallying) can offer efficiency and accessibility. However, it also raises serious concerns about security, transparency and trust. The VC insists that any adoption of digital tools by election management bodies (EMBs) must be accompanied by robust safeguards and guarantees, in line with the principles of its Code of Good Practice[138].

A fundamental point made in the 2024 Interpretative Declaration is that nothing in the Commission's Code or the new declaration prevents embracing new technology in elections – *provided that its use complies with human rights, democracy and the rule of law* (emphasis added). This is an important nuance: the Commission is not anti-technology; it recognises that properly implemented e-voting or digital tools can enhance participation (for example, enabling overseas citizens or persons with disabilities to vote more easily). However, the decision to implement such technologies should be taken carefully and inclusively. The declaration stipulates that any adoption of an electoral technology should be done «transparently, by broad consensus after extensive public consultations with all relevant stakeholders»[139]. This means changes like introducing Internet voting or electronic counting machines shouldn't be rushed or imposed by a slim majority – there should be cross-party agreement and expert input, reflecting the high stakes for democracy. Furthermore, there must be a political commitment to fully implement the technology in good faith and not to manipulate or underfund it. Adequate procedural and judicial safeguards must be built around it, including ways to evaluate and remedy any failures in a timely manner.

Concretely, the VC outlines specific provisions that should accompany the use of digital tech by EMBs[140]:

- Reinforcing EMB impartiality and professionalism: Digital systems should not undermine the independence of election organizers. If anything, extra measures (like independent technical commissions or multi-party oversight committees) should be in place to ensure impartial management of e-technology. EMB staff need proper training and resources to handle new systems. The Commission earlier recommended providing EMBs with adequate resources and training to adopt digital technologies and address related cybersecurity risks[141].

---

[138] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 24.

[139] *Ibid.,* 23.

[140] *Ibid.,* 23-27.

[141] Venice Commission, *Joint Report of the Venice Commission and the Directorate of Informa-*

- Transparency of digital processes: The use of technology – especially in vote casting or counting – must be transparent to stakeholders. The Commission insists that «the use of digital technologies and AI should be transparent to ensure electoral integrity and impartiality, especially in the processing of votes»[142]. In practice, this could involve open-source software, public testing, clear audit trails and allowing observers to scrutinize the digital aspects just as they would observe a paper ballot count.
- Election observation adaptation: Election observers (domestic and international) should be able to monitor digital processes. However, there is a recognition that cybersecurity considerations or protection of sensitive data might sometimes limit full access. The declaration notes that providing observers access to things like source code or real-time data flows might have to be balanced with security. Even so, some accommodation (such as inviting independent experts to certify the system, or conducting post-election audits) is necessary to maintain confidence.
- Independent audits: All digital technologies used in elections should undergo independent auditing, and the findings should be made public. Independent audits (by reputable tech experts or firms, possibly accredited by an international body) can verify that systems are secure, that there are no hidden backdoors, and that they function as intended. Publishing the audit results contributes to transparency and voter trust.
- Legal recourse: Voters, candidates or parties must have the possibility to challenge both the adoption of a digital tool and any specific decisions or outcomes produced by it. For example, if an online voting system malfunctions or is alleged to be compromised, there should be a clear process to bring a complaint before an independent body (like an electoral court or special commission). This includes challenging the initial decision to introduce the technology (perhaps if it was done without proper testing or consensus) and challenging results or operations (if, say, a software bug might have affected results). Ensuring judicial or quasi-judicial review of technology-related disputes is crucial, as it places these issues under the rule of law rather than leaving them solely to technical administrators.

Another critical aspect of electoral administration in the digital age is cybersecurity and resilience against cyber threats. Elections should be considered part of a nation's critical infrastructure, just as it was stated in the 2020 principles for a fundamental rights-compliant use of digital technologies in electoral processes[143].Consequently, they must be protected against cyberattacks with the same seriousness as one would protect power grids or banking systems. Cyber threats come in two main forms: (1) attacks on electoral infrastructure ("threats to electoral democracy") – e.g.

tion Society and Action against Crime (DGI) on Digital Technologies and Elections, cit., 149.

[142] Venice Commission, *Interpretative Declaration of the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence*, cit., 149.

[143] Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes,* cit., 86.

hacking voter registration databases, corrupting electronic vote tallies, taking down election websites, ransomware on EMB systems – which threaten the integrity and availability of the vote; and (2) attacks on deliberative processes – a kind of cyber-enabled disinformation or illegal intervention (overlapping with information disorder discussed earlier), e.g. hacking and leaking sensitive information about candidates, or using cyber means to violate campaign finance or data protection rules.[144]

To combat these, the Commission's recommendations include:

- Criminalizing election cyber-attacks: Ensure national law explicitly makes it a serious crime to attack election IT systems. Most countries have cybercrime laws (the Budapest Convention ETS 185 provides model provisions), but EMB-specific offences (tampering with voting machines, DDoS-ing election result servers) should be clearly covered.
- Empowering law enforcement for e-evidence: Give authorities powers to swiftly secure and obtain electronic evidence when investigating breaches of electoral laws. For example, if there's suspicion of foreign cyber interference, investigators may need logs from tech companies or servers abroad; laws and international agreements should facilitate that. The Commission notes the ongoing negotiation of a Second Protocol to the Budapest Convention to improve cross-border access to data.
- Crisis preparedness in EMBs: The Commission strongly advises EMBs to have contingency plans for cyber incidents. This might mean backup paper copies of electoral rolls, alternative communication channels if official ones are hacked, procedures to quickly switch to manual counting if an electronic system fails, etc. Also, training EMB officials in basic cyber hygiene and incident response is necessary[145]. Some countries conduct scenario exercises (simulating an election-day cyberattack) to test readiness – a practice others could adopt.
- Declaring elections "critical infrastructure": This designation (as the Commission suggests) can mobilise additional government resources and coordination. It ensures that national cybersecurity agencies or defence cyber units prioritise protecting election systems, especially during key periods.
- Regularly updating legal and technical frameworks: The Commission warns that technology evolves quickly, so laws and tools must be under constant review[146]. For instance, if quantum computing or new AI could break current encryption, security protocols must adapt. Similarly, if new forms of online manipulation arise, legal definitions might need expanding. A static approach will fail against dynamic threats.

Another emerging issue is jurisdiction and conflict of laws in cyber contexts. Cyberattacks and illicit online activities in elections often originate from abroad or involve actors in multiple countries. The Commission notes in the Principles for a fundamental rights-compliant use of digital

144 *Ibid.,* 79.

145 Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit. 150.

146 Venice Commission, *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes*, cit., 82.

technologies in electoral processes, that there is «no internationally established criterion» to resolve jurisdiction for cybercrimes affecting elections[147]. Various principles (location of act, location of effect, nationality of perpetrator/victim) are used by different nations, which can cause gaps or conflicts[148]. It suggests that an international approach or even an international court or tribunal might eventually be needed for transnational online election offences. In the meantime, enhanced cooperation via conventions (like the Budapest Convention's upcoming protocol) is the practical path[149].

Lastly, the Commission emphasizes public trust as the ultimate goal. Technical assurances alone won't suffice if the public doesn't believe in the system. That's why transparency, audits and inclusive decision-making about technology are so heavily stressed. Election officials should communicate clearly about how systems work and what is being done to secure them. If an incident occurs (like a hacking attempt), honesty and prompt information can actually shore up trust by showing that the response was effective.

In conclusion, the VC's doctrine on electoral administration in the digital era can be summed up as: innovation "with caution". Yes, use technology to improve elections (for accessibility, speed or accuracy), but do so methodically, with broad consensus, and with layers of safeguards (legal, technical and procedural). And treat threats from cyberspace as seriously as physical threats to ballots. By implementing these measures – from independent audits of e-voting to criminalizing cyber meddling – states can harness the benefits of digital tools without imperilling the integrity or credibility of their elections.

4. Doctrine in Action: Cancellation of Election Results

We have an opportunity to observe the practical application of the above doctrine in the *Urgent Report on the Cancellation of Election Results by Constitutional Courts*[150], requested by the President of the Parliamentary Assembly of the Council of Europe, regarding the recent specific case of Romania. This urgent report was prompted by the extensive use of technology in the election campaign of a candidate (Călin Georgescu) that resulted in the annulment of the election by the Constitutional Court of Romania. In it, the Commission offers a general analysis of the conditions that must be met to take such a momentous decision, and – relevant to our discussion – examines how online campaigns and an *uninformed campaign* can lead to this outcome, in light of the Romanian case that gave rise to the opinion[151].

147 *Ibid.,* 20.

148 *Ibid.,* 84.

149 Venice Commission, *Joint Report of the Venice Commission and the Directorate of Information Society and Action against Crime (DGI) on Digital Technologies and Elections,* cit., 149.

150 Venice Commission, *Urgent Report on the Cancellation of Election Results by Constitutional Courts*, CDL-PI(2025)001, (2025).

151 *Ibid.,* 52.

In this opinion, the VC itself summarizes its doctrine in a synthesis that serves as a useful recap. It emphasizes (1) that the freedom of voters to form an opinion includes the right to have access to all kinds of information that enable them to be properly informed before deciding (and that this freedom can be affected by online information disorders)[152]; (2) that 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[153]. The Code of Good Practice makes clear that candidates and parties must be granted fair and equitable access to online media, ensuring representation without discrimination. Legal provisions should also ensure 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 AI technologies to manage their campaigns[154]. The declaration adds that fairness in content dissemination and access should be observed: regulations should ensure that AI algorithms used by Internet platforms do not favour certain parties or candidates over others, maintaining balance in the visibility of electoral content, and that independent ongoing audits of such algorithms should be enforced[155].

The report goes on to note that the Commission calls on states to regulate online electoral advertising so that it is always identified as such and is transparent regarding the sponsor's identity and the dissemination technique being used; that funding of online campaign activities must be transparent, with potential limits on parties' spending on digital advertising; and that social media platforms should be required to consistently disclose data on political advertising and its sponsors. According to the Interpretative Declaration, 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, and prohibiting political parties and candidates from campaigning anonymously could also be justified.

The urgent report adds that in deciding to annul election results, considerations should include «whether the violation is so significant that it may have influenced the outcome of the election»[156] and that the mere existence of these campaigns «does not mean that the candidate has violated rules on campaign spending and transparency and thus obtained an unfair advantage»[157]. The report acknowledges the voluntary involvement of third parties in such online actions during the campaign, though obligations and restrictions may be established «to ensure transparency and accountability»[158].

---

152 *Ibid.,* 5.

153 *Ibid.,* 9.

154 *Ibid.,* 44.

155 *Ibid.,* 45.

156 *Ibid.,* 56.

157 *Ibid.,* 57.

158 *Ibid.,* 58.

It concludes by pointing out[159] that proving violations of the law through online campaigning and social media is particularly challenging, and safeguards are needed to prevent arbitrary decisions. The law must guarantee safeguards such as impartiality and precise norms to limit the authorities' discretion, as well as guarantees of fair, objective and well-reasoned decisions. Decisions to annul an election on such grounds must precisely indicate the violations and evidence; they must not be based solely on classified intelligence (which may only be used for contextual information), since that would not guarantee the necessary transparency and verifiability.

5. Conclusion

The VC has developed a comprehensive doctrine on how digital technologies should be reconciled with the fundamental norms of democracy. It is a doctrine that does not shy from naming threats – be it disinformation, big data abuse or cyber warfare – but remains fundamentally optimistic that, with prudent regulation and broad collaboration, digital technology can be harnessed in service of democracy rather than against it. Moving forward, the challenges will undoubtedly evolve. The Commission's doctrine, comprehensive as it is, acknowledges the need for constant review and adaptability. New developments like deepfake audio that indistinguishably mimics candidates, or the use of AI chatbots to flood debate forums, will test the resilience of these principles. The task now is implementation: it falls to national legislators, electoral authorities, courts, and indeed the tech industry and voters themselves to put these recommendations into practice. By doing so, they honour the spirit of the Commission's message: that the essential ideals of free and fair elections are not only compatible with the digital age, but can emerge from it strengthened and revalidated.
In formal opinions and principles, the Commission has articulated that while the digital revolution offers new avenues for political participation, it also demands renewed vigilance to protect the core values of electoral law – free expression, fair competition, transparency and security. The Commission's guidance is characterized by a dual commitment: an embrace of innovation's potential to enhance democracy, and an insistence that innovation not be allowed to undermine human rights, equality or the rule of law.
Several consistent themes run through this doctrine. First, fundamental rights are technologically neutral: the rights to freely form and express political opinions, to receive accurate information, to personal privacy, and to genuine choice in elections all continue unabated online. Any regulation of digital campaigning must therefore uphold these rights and meet the strict tests of legality, necessity and proportionality.
Secondly, the Commission underscores equality and fairness – the digital realm cannot become a Wild West where those with the most money, data or control over algorithms can skew the electoral playing field. Equal opportunity mandates transparency in political advertising, limits on exces-

[159] *Ibid.,* 59.

sive or opaque spending, and ensuring all voices can be heard.

Another prominent theme is accountability. The doctrine calls for accountability of both state and private actors, which has also been mentioned by several studies and academic resources[160]. States have positive obligations to update their laws, diligently enforce them, and not shy away from new duties like cyber defense of elections. Private companies, which now hold immense power over political discourse, must likewise be accountable – through transparency requirements, co-regulation schemes, independent audits and a culture of social responsibility. The Commission clearly rejects a laissez-faire approach; instead, it envisions a structured partnership where public authorities and Internet intermediaries work hand in hand, under agreed rules, to uphold democratic integrity.

Closely related to the previous point is the need for international cooperation. Digital threats to elections are transnational and cannot be tackled by individual states alone. Because the Internet is borderless and platforms operate globally, the Commission calls for strong international cooperation and broad multi-stakeholder engagement – including governments, private companies and civil society. The goal is to avoid regulatory loopholes, ensure mutual assistance, and maintain a united democratic front against cyber threats, disinformation and foreign interference. The Commission envisions an integrated network of states, companies and civic actors working together to safeguard electoral integrity in the digital age.

[160] T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, New Haven, 2018.

Abstract

This study examines the evolving doctrine of the European Commission for Democracy through Law (Venice Commission) regarding the impact of digital technologies on electoral processes. It focuses on the systematic approach adopted during 2019–2024, while also contextualizing the Commission's earlier work (2002–2018). A qualitative doctrinal analysis of key Venice Commission reports, opinions, and principles elucidates how the Commission has addressed challenges such as online political speech, fair campaigning in the digital sphere, voter data protection, transparency in digital campaign financing, the accountability of internet platforms, and cybersecurity in elections. The findings reveal a comprehensive framework emerging from the Commission's work. The Venice Commission reaffirms that fundamental rights—like freedom of expression and equality of opportunity—apply fully online; it calls for robust personal data protections and transparency measures in digital campaigning; it advocates co-regulatory responsibilities for internet intermediaries; and it insists on strong safeguards when implementing new voting technologies. The Commission's doctrine, reflected in a trilogy of major documents (2019 Joint Report, 2020 Principles, 2024 Interpretative Declaration) and related opinions, underscores the need to adapt electoral standards to the digital age to preserve democratic integrity while embracing innovation.

Keywords

Venice Commission – elections – freedom of expression – data protection – social media