

Cybersecurity in the Electoral Sphere: Legal and Technical Considerations on a Hybrid Threat*

Tamara Álvarez Robles

Table of Contents

1. Introduction. - 2. The Venice Commission Facing the Challenge of Cybersecurity Election. - 2.1. Joint Report on Digital Technologies and Elections. - 2.2. Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes. - 2.3. Interpretative Declaration of the Code of Good Practice in Electoral Matters as Concerns Digital Technologies and Artificial Intelligence. -3. Reflection on Electoral Cybersecurity in the Context of Crisis. - 4. Conclusion.

1. Introduction

Cybersecurity in the electoral sphere has become a key element to ensure transparency, public trust, and the legitimacy of democratic processes. In this regard, the Venice Commission, as the Council of Europe's advisory body on constitutional matters, has emphasized in multiple reports the need to strengthen the digital protection of electoral systems against threats such as cyberattacks, information manipulation, or external interference. Safeguarding voter registries, securing the transmission of results, and protecting digital communication platforms are essential components to prevent vulnerabilities that could undermine the course of free and fair elections.

Recent elections in different parts of the world have shown that this threat is far from hypothetical: the digitalization of electoral processes, from voter rolls to vote counting, expands both opportunities for participation and risks of interference. Cases of disinformation spread through social media, hacking attempts against electoral authorities, and growing geopolitical tensions have highlighted the urgency of establishing solid regulatory and technical frameworks. In this context, the recommendations of the Venice Commission serve as a key reference for strengthening the digital resilience of electoral systems and, consequently, safeguarding one of the most sensitive pillars of contemporary democracy.

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

2. The Venice Commission Facing the Challenge of Cybersecurity Election

The Venice Commission, as an institution of reference in democratic matters, has carried out a solid analysis of the electoral situation in the 21st century, examining both the opportunities and challenges posed by the use of technology. Among the various documents produced, three in particular stand out, not only for the specificity of their approach, but also for their recent publication and the high quality of their contributions: the Joint Report on Digital Technologies and Elections; Principles for a Fundamental Rights-Compliant use of Digital Technologies In electoral processes, and Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence. While it is true that, there are other reports where some security and/or cybersecurity guidelines are also collected, especially those focused on specific technologies, such as electronic voting systems, as well as relevant updates to the Code of Good Practices or the 2020 Electoral Compendium, the three reports mentioned above are particularly useful to understand the current state of cybersecurity in the electoral field and its evolution in a short period of time, specifically in the last six years.

2.1. Joint Report on Digital Technologies and Elections

One of the most relevant Venice Commission reports dedicated to digital technologies during the electoral process is the Joint Report on Digital Technologies and Elections in 2019. That could be an example of lessons learned after the American elections and Brexit in 2016, the hacking of Emmanuel Macron's email and the dissemination of information on the day of reflection of the French presidential elections in 2017, the use of WhatsApp in the Brazilian elections of 2018 or the presence of bots and trolls in the Mexican elections of the same year. It is the consequence of information manipulation, the misuse of social networks and several cybersecurity events in the electoral field.

The report focuses on analyzing the problems generated by the large technological companies that control the contents of the Internet and, in particular, social networks, given that the massive use of the Internet and social networks is changing various aspects of social and political life, which are reflected in the electoral process. Several problems emerge, among which the following stand out: monopolies, hacktivism, disinformation, misinformation, malinformation, foreign interference and hybrid threats. Therefore, the objective is to identify the most relevant legal problems generated by the use of these technologies, describe their logic and possible parameters of solution, point out the deficiencies identified so far and suggest a general set of principles and guidelines that can help to adapt democracy and its laws to the new technological realities.

It is true that the document analyzes the phenomenon of information manipulation in detail, and that in certain sections it analyzes information

security, cybersecurity and cybercrime. Thus, one of the first references to cybersecurity refers to the use of cyberattacks, malware, espionage by third countries and “cyberwarfare” (para. 40- 44), a growing trend, as will become clear. It then points out the problem of prosecuting these practices due to the lack of regulations or as a result of jurisdiction (para. 45), the existence of different regulatory frameworks makes investigation and punishment difficult and therefore calls for a transnational perspective to overcome these difficulties.

The report analyzes in three sections the rights to free elections and freedom of expression; privacy and protection of personal data; and protection against cybercrime, in which we will find different references to cybersecurity.

Beginning with the right to free elections and freedom of expression. We must point out the obligation of the States to ensure an uninterrupted communicative context of the elections (para. 50). It would therefore be a matter of preventing supply cuts caused by cyber-attacks, physical sabotage, both by public and private actors, which would be achieved through the observance of information security standards and policies, cybersecurity. This uninterrupted of the communication channels reaches the electoral campaign (para. 51). That is why we take this opportunity to point out to national legislators the need to review this aspect in their rules, especially in criminal law, in order to avoid legal loopholes and the application of analogical or extensive interpretations. In the same way that the communication channel must be guaranteed, i.e., that infrastructures are not affected, that a service is not blocked or interfered with by unauthorized third parties, it must be guaranteed that there is no censorship, removal or moderation of content, except those authorized by the judiciary in strict compliance with international standards (para. 54).

At the same point, the document analyzes electronic voting systems, highlighting the principles of reliability, accountability and security, in addition to the principles of universal, equal, free and secret suffrage (para. 57). Furthermore, it takes the opportunity to recall that the Council of Europe remains the only organization that has established intergovernmental standards in the field of electronic voting. It also takes up the words of researchers from the University of Michigan and the Open Rights Group who state that «there are fundamental advances in computer security, the risk profile may be more favorable for Internet voting, but we do not believe that the Internet voting system can be made secure today» (para. 119).

Next, attention is given to the right to the protection of personal data and privacy (para. 73-83) where we can highlight the adaptation to the framework of the European General Data Protection Regulation (going beyond Convention 108 and recognizing the Brussels effect), promoting the incorporation of its principles.

This point includes the state’s obligation to guarantee privacy and the protection of personal data. This State obligation is twofold: negative, to refrain from interfering with human rights; and positive, to actively protect these rights, which includes protecting individuals from the actions of non-State actors (para. 81). This is because privacy is a necessary element

of human life and of the human functioning of a democratic society, and its violation affects the dignity, freedom and security of the individual (para. 78).

In this sense, it is essential to link once again the protection of information with strict compliance with information security and cybersecurity regulations. Said regulation establishes adequate and proportional measures to the type of information to be protected, applicable both to electoral bodies and to political parties, candidates and other actors who, in their capacity as holders or responsible for data processing, must guarantee its integrity, confidentiality and availability. The adequate protection of this information, which may be of a sensitive nature, personal data or with electoral value, is crucial, since its improper use or unauthorized access could be exploited by different actors in order to influence the development of the electoral process. Examples include the hacking of Macron on the eve of the elections, on the day of reflection, one of the most fragile or sensitive electoral moments; the data breach suffered by the UK Electoral Commission published in 2023 or personalized phishing attacks directed against a candidate, such as the hacking of the X account of the Dominican presidential candidate Abinader in 2024.

Thirdly, it focuses on protection against cybercrime, which, as far as we are concerned, is one of the most relevant sections. Starting by identifying the normative basis of the Budapest Convention on Cybercrime (The Council of Europe Convention on Cybercrime ETS 185 of 2001- “Budapest Convention”) to which the two protocols are incorporated.

Two types of threats derive from the Budapest Convention, which are identified in the document as follows (para. 84): First, attacks against the confidentiality, integrity and availability of computers and election data, which constitute forms of cybercrime, such as illegal access to computer systems (art. 2), illegal interception (art. 3), interference with data and systems (arts. 4 and 5), among others. Secondly, disinformation operations in which the rules on personal data protection, political financing, media coverage or election broadcasting, i.e. the rules to ensure free, fair and clean elections, are violated. As a whole, they will form part of the hybrid threats (which are also combated from the international scope of NATO, para. 91) but they have, as can be seen, their own distinct entity.

The document at this point focuses on misinformation and the difficulties in obtaining evidence due to several aspects: jurisdiction and procedures, the typology of the crime itself, the agents involved.

With regard to cybersecurity incidents, the work carried out by the European Commission is given as an example, which in 2018 formulated specific recommendations with the aim of protecting Europe’s democratic processes from manipulation by third countries or private interests, and proposed new rules on electoral cooperation networks, online transparency, protection against cybersecurity incidents and measures to counter disinformation campaigns in the context of European elections (para. 97). In this order of ideas, it is also worth highlighting several sections that are linked to “electoral democracy” and that are related to electoral cybersecurity.

Starting with the concept of “electoral democracy” which refers to the

activities and institutional infrastructures that make elections possible. From the organization of elections to the creation and administration of the electoral roll or the implementation of electronic voting and Internet voting, the electoral aspect of democracy establishes the material and institutional conditions necessary for popular suffrage to translate into the appointment of representatives or the approval of laws and public policies (para. 109). This is the time to call for it to be categorized as critical infrastructure, if it has not been identified as such by the States, as this will have an impact on the criminal law applied to cybercrime types.

The document states that the correct maintenance of the electoral roll is crucial for the realization of the principle of universal suffrage; the strict observance of voting and counting procedures is crucial for the realization of the principle of free suffrage (para. 109). Let us recall the example of the exfiltration of data from the electoral roll in the United Kingdom, or the cyber-attacks suffered in the elections to the telematic voting system abroad in Ecuador's elections in seven countries in 2023.

In addition, attention is drawn to how different actors try to intervene in elections such as those in Arizona, the Netherlands, Ghana or the United States of America. «According to the Government of Canada's Centre for Communications Security (CSE), «[d]enemies around the world use cyber capabilities...against elections...to suppress voter turnout, manipulate election results and steal voter information.... against political parties and politicians... to conduct cyber-espionage for coercion and manipulation, and to publicly discredit individuals... [and] against traditional media and social networks... to spread disinformation and propaganda, and to shape voter opinion» (para. 111)».

And a future and upward trend is evident based on several reasons: effective cyber capabilities are accessible, inexpensive and easy to use; the expansion of social networks and the loss of reliable sources of information facilitate the spread of disinformation; moving electoral services to the Internet increases their vulnerability to cyber threats; the difficulty to detect, attribute and respond to cyber threats favors attackers over defenders; and the success of previous attacks motivates adversaries to repeat them and inspires copycats. A trend that has been confirmed over the years.

Again, the two types of cybercrime, which were derived from the Budapest Convention, focusing on those that affect the principles of information security, those attacks against the confidentiality, integrity and availability of computers and electoral data, the following practices are pointed out (para. 113):

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

According to the Budapest Convention, these attacks are cybercrimes: illegal access to computer systems (art. 2), illegal interception (art. 3), in-

interference with data and systems (arts. 4 and 5), among others. Although it is pointed out that more than sixty States Parties to this treaty have transposed these provisions into their domestic law, there is no analysis of how they have been transposed, and the fact is that to a large extent criminal offenses have been configured within the Criminal Codes that do not contemplate an aggravated type in the event that these conducts are carried out at election time, the legal property protected is not democracy, but patrimony (crime of computer damage or illegal interference in data; also in crimes of attacks on computer systems or unlawful interference in systems). *Sensu contrario*, in the framework of the special electoral criminal laws, these criminal offenses are not usually contemplated and remain obsolete. This scenario generates legal uncertainty. The protection of the legal good of democracy would be achieved, as we have pointed out, by means of a concurrence of crimes.

As a result, States are asked to make a greater effort and commitment and it is emphasized that, according to the ECHR, States have a positive obligation to guarantee free and secure elections and to guarantee human rights such as the right to privacy and freedom of expression (para. 115). In this sense, it is necessary to strengthen the international framework to establish more efficient mechanisms for transnational cooperation between nations and private actors and, if possible, to achieve greater uniformity among national legislations. In short, the solution lies in adapting the constitutional framework of modern democracies to the new electronic environment in which cybercrime thrives and in which governments, businesses and citizens interact and make democracies possible (para. 121). Public-private, interstate cooperation and harmonization of regulatory frameworks will be key to electoral resilience.

In short, it reaffirms the commitment to security, which we must understand as cybersecurity by stating that «digital technologies must not be allowed to undermine public confidence in the electoral process, hence the need to guarantee the security of such technologies to the citizenry. To this end, digital technologies must be introduced gradually and can be combined with traditional methods. Innovation cannot be to the detriment of legal requirements, including security» (para. 120).

Among the proposals made to face these challenges related to electoral democracy (para. 149) are:

- Classify in the criminal code cyber-attacks against the confidentiality, integrity and availability of computers and electoral data, in accordance with the Budapest Convention on Cybercrime;
- Provide criminal justice authorities with the necessary powers to obtain electronic evidence of violations of rules on personal data protection, political financing, media coverage or election broadcasting;
- Prepare EMBs for emergency situations and have a crisis management organization in place; EMBs should be adequately resourced and trained to adopt digital technologies and address related cybersecurity risks.

To this we must add: revision of the electoral laws and penal codes in accordance with what has already been indicated.

Finally, we can show the measures they advocate within the framework of

deliberative democracy (para. 149):

- Recognize the transnational nature of the problem and the essential role played by internet intermediaries (i.e. internet service providers and search engine and social networking companies);
- Strengthen the international framework to establish more efficient mechanisms for transnational cooperation between nations and private actors and, if possible, to achieve greater uniformity among national legislations;
- Work on a regulatory and adjudicative model based on the co-responsibility of private and public actors, and on multiple regulatory and conflict resolution approaches. Such a model could include at least four strategies, all capable of constantly adapting to the constantly evolving environment of the Internet and communication technologies:
 - Promote research and cooperation among electoral authorities, academics and practitioners to assess the real impact of digital technologies on electoral processes and the effectiveness of the measures adopted;
 - Promote education to strengthen the legal and democratic culture among citizens;
 - Promote self-regulation, such as the mandatory adoption of codes of ethics and corporate social responsibility, among Internet service providers and search engine and social networking companies; and

Establish remediation mechanisms in laws, policies and alternative dispute resolution mechanisms.

In conclusion, the commitment demonstrated by the Venice Commission in adapting electoral procedures to current requirements is to be commended, as well as its ability to anticipate the challenges that will arise in the short term in the area of cybersecurity. Among the most relevant contributions are the adherence to the principles of the Budapest Convention, the rigorous analysis of cybersecurity incidents, the priority attention to the protection of personal data and the comprehensive consideration of hybrid threats. These actions reflect a proactive and conscious approach to the need to strengthen electoral processes in the face of emerging risks in the technological-digital environment.

2.2. Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes

The second of the documents, Principles for a Fundamental Rights-Compliant use of Digital Technologies In electoral processes, that is of interest to us is published a year later, in 2020, and is dedicated to the heart of the law, to the principles, the bases that support the electoral system reflected in attention to the new social, technological-digital reality, and the challenges it faces.

The importance of this report is that it provides a rigorous analysis of the

threats we face (para. 8):

- At various levels: international, national, local.
- Conditioned by the time factor: immediate effects, rapid spread.
- Involving different public and private actors: States, governments, political parties, media, companies, citizens.
- Realized through infrastructures and technological-digital services using their potential.

In addition, the importance of the electoral infrastructure in a broad sense (internet, e- government), on which electoral cyber threats are projected in their different forms, is taken into account and analyzed in relation to the two types of democracy: electoral democracy - through attacks on the integrity, confidentiality and availability of computers or data - and deliberative/monitory democracy - through information operations with violations of the rules that guarantee fair, free and clean elections.

In this sense, we could deduce that the former would be those that fit into criminal types such as attacks on computer systems or unlawful intrusion into systems; computer damage and illegal interference in data; while the latter would be related to the concept of disinformation and traditional electoral crimes.

We must recognize that the report not only analyzes the technologies from a negative point of view, but also alludes to the benefits they can bring. However, the approach to risks and threats appears to a greater extent, for example the references to “Algocracy”, “Dictadata” or “Weapons of Maths destitution” (para. 17).

As in the previous report, attention is focused on the difficulties that make up the technological-digital ecosystem: extraterritoriality and temporality or immediacy (para. 37).

In short, attention is paid to the subjects that are part of the electoral procedure. These are no longer only the traditional state actors -who have the role of watchdogs and organizers of the electoral process- (para. 22) and are expanded to include other public and private actors (para. 24-31), service providers, ISPs, to whom we must add cybercriminals and those who try to interfere in the electoral procedures.

The prevention of cybercrime is again analyzed on the basis of the well-known Budapest Convention, following the guidelines of the previous report and devoting to it one of the eight principles, specifically the sixth, which is the main contribution of this report:

- Principle 1: The principles of freedom of expression that imply a robust public debate should be transferred to the digital environment, particularly during election periods.
- Principle 2: During election campaigns, an impartial and competent Electoral Management Body (EMB) or judicial body should be empowered to require private companies to remove clearly defined third-party content from the Internet, based on election laws and in accordance with international standards.
- Principle 3: During election periods, it is necessary to protect the open internet and net neutrality.
- Principle 4: Personal data should be effectively protected, especially during the crucial election period.

- Principle 5: Electoral integrity should be preserved through the periodic review of rules and regulations on political advertising and on the liability of Internet intermediaries.
- Principle 6: Electoral integrity must be ensured by adapting specific international regulations to the new technological context and by developing institutional capacities to combat cyber threats.
- Principle 7: The international cooperation framework and public-private cooperation should be strengthened.
- Principle 8: The adoption of self-regulatory mechanisms should be promoted.

However, we are going to focus only on the description of two of them, principles 6 and 7, not only because of the space available, but mainly because they are closer to the subject we are trying to analyze, cybersecurity. Beginning with Principle 6 that analyzes electoral integrity, which must be guaranteed by adapting specific international regulations to the new technological context and developing institutional capacities to combat cyber threats.

As can be seen from the title, there are two lines of action to be undertaken: regulatory adaptation, on the one hand, and training or education, on the other.

This principle reanalyzes the threats according to the type of electoral or deliberative democracy, within the electoral framework of the Council of Europe, the Council of Europe Convention on Cybercrime ETS 185 of 2001 (Budapest Convention) and in terms like those of the previous report (para. 79).

First, threats to electoral democracy are identified, which have been related to attacks against the confidentiality, integrity and availability (basic principles of information security, cybersecurity) of computers and electoral data, the violation of voter databases or registration systems; the manipulation of voting machines to manipulate results; interference with the operation of systems on election day; and illegal access to computers to steal, modify and disseminate sensitive data. We have related these threats on several occasions with crimes such as attacks on computer systems or unlawful intrusion into systems; computer damage and illegal interference in data, which in the Budapest Convention are established generically and not thinking only and exclusively in electoral procedures, which is why the legal property protected in these criminal offenses is usually the patrimony, as opposed to democracy in the special electoral criminal laws.

Secondly, it contemplates threats to deliberative democracy, that is, information operations that violate the rules for guaranteeing free, fair and clean elections, related to data protection, political financing, media coverage of electoral campaigns, broadcasting and political advertising, which are usually found in special criminal regulations, or in those sections of the criminal code dedicated to the electoral field.

Once again, the volatility of digital evidence and extraterritoriality and jurisdiction problems are some of the concerns reflected in the report. To counteract these deficiencies, the need to implement the mechanisms provided for in the Budapest Convention (and its two protocols), which are based on the principles of international and public-private cooperation

and coordination, is again emphasized.

The three basic measures to be implemented to ensure free elections are repeated (para. 81):

- Classify in the criminal code cyber-attacks against the confidentiality, integrity and availability of computers and electoral data, in accordance with the Budapest Convention on Cybercrime;
- Provide criminal justice authorities with the necessary powers to obtain electronic evidence of violations of rules on personal data protection, political financing, media coverage or election broadcasting;
- Prepare EMBs for emergency situations and have a crisis management organization in place; EMBs should be adequately resourced and trained to adopt digital technologies and address related cybersecurity risks.

And relevant measures are established in the framework of cybersecurity (para. 86):

- It is necessary to strengthen institutional capacities to prevent cyber threats to democracy and electoral processes.
- Elections should be declared a critical infrastructure.
- The technological capabilities and legal powers of the electoral authorities to control, investigate and criminally prosecute illegal online conduct must be strengthened.

In conclusion, this principle allows for important advances in various strategic areas. Among its main contributions are the approach to electoral cybersecurity based on the risks and threats it faces, the strengthening of institutional capacities and the review and updating of regulatory frameworks and cybersecurity policies, as well as the declaration of the electoral process as part of the critical infrastructure.

Finally, we must refer to Principle 7 dedicated to strengthening the framework for international cooperation and public-private cooperation.

As the United Nations has been maintaining with its Global Programme against Cybercrime or the Venice Commission itself, in the previous report, it is necessary to strengthen the international framework to establish more efficient mechanisms for transnational cooperation between national authorities and private actors and, if possible, to achieve greater uniformity between national legislations. It is also necessary to respond more effectively and efficiently at the public policy level to a problem that is characterized as transnational.

This cooperation can be made more efficient through the standardization and implementation of homogeneous protocols and norms, such as those provided by ISO norms, NIST or ESN standards, with information security policies such as MAGERIT, SP800-30, CRAMM or OCTAVE: standardized request formats; legal clarity of procedural rules; authentication of the identity of the requester and the recipient; establishment of transparency standards in reporting; determination of the rules that should guide decision-making; a transnational appeals system; and establishment of formal and efficient channels of dialogue between stakeholders (para. 89). Or with the provision of a “Certificate of Digital Corporate Responsibility” similar to ISO standards (para. 91).

Citizen education and quality journalism (which must be protected) are

presented as the solution to most of the problems in this principle (para. 92-95), transcending from a vision of institutionalized security to a true culture of security.

In relation to education the Commission recommends:

- Promote education to strengthen the legal and democratic culture of citizenship, based on the co-responsibility of private and public actors; and
- Empower voters to critically evaluate election communication and take specific steps to prevent exposure to false, misleading and damaging information through education and advocacy.

Thus, education must enable citizens to face the new digital reality, not only in terms of the functions of technology, but also its effects, teaching them to distinguish between what is important and what is irrelevant, between truth and lies, and to protect themselves from cyber threats. This education transcends the educational strategies of the State, of education in a strict sense, and reaches the private sphere, companies and civil society organizations, which could establish partnerships both to educate Internet users and to evaluate the effectiveness of the controls implemented by companies (para. 93).

In short, this principle underscores the need for a comprehensive and transnational review of regulatory frameworks and cooperation protocols, defends quality journalism, and promotes the strengthening of training processes and education in cybersecurity, essential elements to face the current challenges in the changing and disruptive technological- digital environment.

2.3. Interpretative Declaration of the Code of Good Practice in Electoral Matters as Concerns Digital Technologies and Artificial Intelligence

The period from 2023 to 2024 was characterized as the year in which 80% of the world's population was called to participate in elections (local, national, regional). In this context, not only the challenges of a prolonged political and democratic crisis, but also a growing geopolitical instability, the dangers associated with technological progress and a marked increase in cyberattacks. Consequently, a technological-digital concern arises on the one hand, disinformation campaigns, on the other, cyber-attacks on infrastructures (mainly DDoS and ransomware), both known; to which is added the perverse use that could be made of Artificial Intelligence in the electoral field.

This concern is the subject of the third of the Venice Commission's reports, which we are going to outline and which focuses to a large extent on a technology that, although it has been with us for decades, is beginning to become more popular: Artificial Intelligence.

The report aims to guide us in the interpretation of the 2002 Code of Good Electoral Practices from a technological-digital approach, for which it analyzes free and equal suffrage, the positive obligations of public authorities and the principle of co- responsibility of private actors, the re-

spect for fundamental rights and some specific considerations regarding the use of technologies in electoral bodies.

Beginning with free suffrage (paragraphs 5 to 11), it starts with some of the contributions made in previous reports, such as the aforementioned right to confidentiality of communications on the Internet, the right of access to the Internet, and the right to receive and share information (para. 37). The approach to the right of access to the Internet (para. 39) is broad, as it includes the protection of the infrastructure, the principle of neutrality, in order to guarantee the principles of equality and non-discrimination (para. 40).

In its analysis it is mentioned that freedom is lost, among some of the bad practices, with the monitoring of people's activity without consent (para. 36). That is why, when we try to implement mainly preventive cybersecurity measures consisting of monitoring behavior patterns, we must consider the impact on this right. This right is also affected by personal data breaches, which we can identify with failure in preventive information security systems and with the implementation of incident management plans. It is therefore relevant that in the information security system, when performing the risk analysis and impact assessment, attention is paid to this right in its relationship with the protection of personal data. Thus, in the incident management plans, we will have been able to establish some safeguards to minimize the impact of a cybersecurity incident. Therefore, it is necessary to know the electoral regulations, information security regulations, personal data protection regulations and the actual framework of application of these information security management systems. Let us recall that the certification of international standards has been presented as good practice in the matter.

Equal suffrage, understood as equal opportunities (para. 9 to 11) is presented as equal access to technologies, to Artificial Intelligence, to the media, and to the Internet. In this order of ideas, we must focus not only on access to these media and communication channels but also on their protection from the point of view of cybersecurity. This equality in cybersecurity protection (understood in a generic sense) must reach subjects such as candidates, political parties, electoral institutions, to avoid inequalities and discrimination in cybersecurity (digital gaps). It is here where the principle of neutrality, a principle that guarantees equality and non-discrimination, must again be alluded to.

Of great relevance are the considerations made regarding the positive obligations of public authorities and the principle of co-responsibility of private actors (para. 12- 19), to protect against cybercrime or disinformation campaigns (para. 48 and 49). The need to strengthen the integrity of the electoral process is reiterated, with specific rules on cybercrime, including sanctions (para. 12-17), as well as the provision of mechanisms for collaboration and international cooperation (para. 18- 19).

Integrity can be ensured by establishing cybersecurity rules, specific standards, principles and values to prevent and combat cyber threats. To this end, international cybersecurity standards are taken as references: the Budapest Convention and, in particular, T-CY Guidance Note No. 9 on the aspects of election interference through computer systems covered

by the Budapest Convention, adopted by the Committee of the Convention on Cybercrime (T-CY); and Principle 5 of the 2020 report CDL-AD(2020)037.

The need for cooperation between the various public authorities at the international level is reiterated (para. 53). Among which we should highlight the CERTs/CESIRTs, in a similar way to what happened in the elections to the European Parliament, but also internally reinforcing the cooperation mechanisms between the SOCs of the institutions with the CERTs/CESIRTs of reference in the States. We could conclude that this section is dominated by the principle of accountability.

In the fourth point, dedicated to respect for fundamental rights (para. 20 to 22), it is established that the State has a positive responsibility to protect the principles of the European electoral heritage. To this end, the following rights, among others, must be guaranteed: freedom of expression and freedom of the media; and any restriction on these rights must be based on law, be necessary, respond to the public interest and respect the principle of proportionality. Finally, it is noted that sanctions must be imposed by an independent and impartial body and be subject to an effective system of remedies/appeals (para. 57-60).

The report concludes with the analysis of specific provisions on the use of digital technologies by electoral management bodies, electoral administration (para. 23 to 27). It begins by stating that nothing prevents (neither in the report, nor in the Code of Good Electoral Practices) the incorporation of digital technologies into the electoral process. However, a limit to this incorporation is established: technologies must always respect human rights, democracy and the rule of law (para. 23). These technologies must be introduced provided that they guarantee an equal or higher level of protection to the rights we enjoy in this area (as is the case with the example of people with disabilities contained in para. 25).

In sum, its adoption must be carried out in a transparent manner, through broad consensus after extensive public consultations with all stakeholders, and with a political commitment to implement it fully and in good faith, with due process and judicial guarantees, with the means to timely assess any alleged non-compliance, and with full respect for the principles of individual autonomy, privacy, equality and non-discrimination (paragraphs 23 and 24).

The report states that when digital technologies are used in electoral processes, specific provisions must be established to ensure respect for the procedural guarantees provided for in the Electoral Code. First, the impartiality, independence and professionalism of the electoral management bodies, the electoral authorities, must be reinforced. Likewise, the use of digital technologies and artificial intelligence must be transparent, in order to safeguard electoral integrity and fairness, especially in the processing of votes, considering that the access of election observers to these processes must be balanced with the need to protect cybersecurity and sensitive personal data. Likewise, the digital technologies used should be subject to independent audits, the results of which should be made public. Finally, there must be the possibility of challenging, before an independent body, both the procedure for the adoption of these tools by electoral bodies and

specific decisions based on recommendations from artificial intelligence systems (para. 27).

In this vein, additional standards and requirements should be met as new knowledge emerges about the impact of digital technologies and artificial intelligence on electoral processes (para. 64), which could be achieved through a rigorous risk assessment.

At the normative level, the three elements necessary for the modification of electoral laws are noted (para. 65):

- Clear and comprehensive legislation that complies with international obligations and standards and addresses the above recommendations.
- The adoption and implementation of legislation by broad consensus after extensive public consultations with all relevant stakeholders.
- The political commitment to fully implement such legislation in good faith when using digital technologies and artificial intelligence, with adequate procedural and judicial safeguards and means to timely assess any alleged non-compliance.

It concludes with a discussion on security, cybersecurity, which becomes more prominent in each report (para. 69 to 71). The integrity and security of election technologies must be addressed with special care. Arguably, they are a *sine qua non* for legitimate elections. This special care is because risks and threats change rapidly, hence the need for regular review and updating, especially of the special procedures for risk assessment and management (para. 69).

The report confirms that new provisions adapted to the risks and threats faced by electoral authorities may be necessary and focus on accountability, cooperation, transparency and control of the technologies used (para. 71):

- The impartiality, independence and professionalism of electoral management bodies are essential when digital technologies imply a greater number of tasks and their centralization in these bodies, who must be accountable for their use. In turn, electoral authorities will also need the cooperation of cybersecurity, data protection and law enforcement agencies, as well as citizen organizations and businesses.
- EMBs should disclose the use of digital technologies, including algorithms and artificial intelligence systems. Legislation should contain clear rules on observer access to digital systems or algorithms. While digital technologies and artificial intelligence systems are in continuous development and, therefore, security mechanisms and needs are constantly changing, election legislation should establish, in as much detail as possible, what data is publicly accessible. Observation missions, in turn, should consider incorporating specialists and resources dedicated to addressing these specific issues within their teams.
- If public access to some processes or contents of digital systems is limited for security reasons, an independent audit should be provided for. The conclusions of these audits must be made public.

In summary we have been able to see how the Venice Commission in this report, responds to the risks and threats to electoral procedures that occur with technological advances. So, it transcends more or less known technologies -electronic voting systems, internet- and focuses on artificial

intelligence. In addition, we can witness a growing prominence of aspects related to cybersecurity, which, despite not being the central object of the reports, permeate a large number of the points analyzed.

3. Reflection on Electoral Cybersecurity in the Context of Crisis

Initially, the approach to security within the electoral framework was predominantly analogical. Legal provisions emphasized the intervention of security forces only in the event of incidents, while explicitly recommending that the president of the polling station be the sole authority empowered to summon the police. In addition, the Code of Good Practices in Electoral Matters (2002) highlighted the presence of security forces in electoral offices and institutions, at polling stations, and in the safeguarding of ballot boxes as central components of maintaining order and legitimacy in the process. This framework reflected an understanding of electoral security primarily as a matter of physical integrity and institutional control.

Over time, however, the introduction of technology into electoral procedures shifted the focus toward new dimensions of security. Academic and institutional analyses increasingly examined how technological tools were integrated into processes such as voter registration, census management, ballot counting, and the transmission of results. Much of this interest stemmed from debates surrounding the adoption of electronic voting systems. Within this stage, security concerns were no longer confined to physical spaces or actors, but also extended to digital vulnerabilities, including the hacking of voting machines, the theft of sensitive electoral data, and the illegal transfer of voter databases. Consequently, the notion of electoral security expanded to encompass both traditional physical safeguards and emerging cybersecurity challenges. From this perspective disinformation, information manipulation, hybrid threats are gaining space in the reports of the Venice Commission and in the rest of electoral organizations, as we have seen in the previous sections.

In addition to the above, we must consider a context marked by geopolitical uncertainty and rapid digital transformations in which ensuring free, transparent, and secure elections requires not only attention to democratic quality but also to cybersecurity, conceived broadly as the comprehensive safeguarding of electoral processes and participants from both external and internal risks and threats.

In the course of this paper, we have exemplified how cyberattacks and security breaches are making us increasingly aware of the interdependence of systems and societies (including electoral administrations) and have highlighted the crucial role of the time factor, both in the rapid propagation of these events and in the urgency of their resolution.. Specifically, cyber-attacks on electoral infrastructures, public administrations and the different subjects or actors involved in elections combined with disinformation campaigns make up a hybrid threat scenario that concentrates part of the main current concerns (ENISA, 2024). Effectively addressing this

phenomenon will require a rigorous analysis and an articulated response that will only be possible through a collaborative effort and a comprehensive commitment on the part of all those involved, with the aim of strengthening democratic resilience in the face of present and future challenges. However, it is essential to develop a cybersecurity that, in addition to protecting critical and strategic infrastructures, focuses on the rights of individuals and guarantees a peaceful and harmonious relationship with public administrations, a cybersecurity that transcends the administration-state vision to the citizenry, which is a true culture of democratic cybersecurity. This will therefore constitute one of the challenges that future reports of the Venice Commission will be required to address.

From this perspective, it is essential to foster a true culture of cybersecurity, a culture of democratic- electoral cybersecurity, that strengthens resilience and contributes in a comprehensive manner to the protection of democracies. This effort must transcend one-off actions to become a structural element of electoral processes, encouraging electoral administrations to assume a more active role and to consolidate a firm and sustained commitment to cybersecurity. Only through this cultural transformation will it be possible to effectively confront emerging threats, preserve citizen confidence and guarantee the integrity of democratic systems in the face of the risks of the digital-technological environment.

Therefore, the future challenge facing the Venice Commission could be to carry out a more concrete and detailed analysis of cybersecurity in the electoral framework. This challenge implies addressing not only general issues, but also technical aspects, such as information security management systems, cybersecurity plans and incident response protocols. It will also be necessary to pay attention to the required regulatory adaptations, including the development and implementation of specific criminal and cybersecurity rules for electoral periods, in order to strengthen the protection of democratic processes against digital threats, going beyond the Budapest Convention by protecting democracies as a legal asset. Finally, the observance of the culture of democratic cybersecurity that transcends from the institutional to the citizenry.

Based on these ideas, in the following lines, we will attempt to outline certain guidelines to be incorporated into future reports of the Venice Commission. In doing so, we will focus on key aspects that are increasingly critical in the current electoral context, particularly in light of the geopolitical developments that have shaped elections from 2023 to 2025. These aspects include the strengthening of cybersecurity frameworks as a fundamental pillar of democratic systems; the standardization of procedures, protocols, and technical norms to ensure uniformity and resilience across electoral processes; the adaptation of criminal law to address electoral offenses in the digital era, and the promotion of a robust culture of democratic cybersecurity among all stakeholders. By addressing these interrelated areas, it is possible to provide a comprehensive approach that reinforces the integrity, legitimacy, and trustworthiness of elections in an evolving and technologically complex environment.

Beginning with the adoption of comprehensive cybersecurity regulations within electoral processes is essential to review them to ensure the pro-

tection of all stakeholders—electoral institutions, citizens, political parties and their candidates, as well as private sector actors—throughout every stage of the electoral cycle. This will mean that the legal framework must take care of insert some obligations to ensure that prior to voting, this encompasses the establishment and maintenance of the electoral roll, the conduct of electoral campaigns, and the observance of the reflection period. During the voting phase, both the physical and digital infrastructures, including electronic voting machines, must be secured against any potential compromise. In the counting or scrutiny phase, the integrity and reliability of voting systems must be guaranteed. During the transmission of results, electronically managed tables should be protected to prevent unauthorized alterations of official electoral data. Finally, in the retransmission of results, it is imperative that institutions implement measures to mitigate denial-of-service attacks, ensure the resilience of communication channels, and safeguard the authenticity and accuracy of published outcomes.

Accordingly, it is essential to design, implement, and systematically review comprehensive frameworks, including systems, plans, and protocols for information security management and cybersecurity, in full compliance with international standards on electoral integrity, data protection, and information security. Such approach is critical to uphold the transparency, legitimacy, and resilience of electoral processes in the digital era, and to mitigate both internal and external threats to democratic governance. As recommended by the Venice Commission in its latest reports.

In this order of ideas, and as a proactive measure that helps to face the risks and threats in electoral cybersecurity, it is recommended to introduce certifications of ISO standards or of similar value since they can contribute to obtain greater confidence in the electoral institutions, as they help to implement and document procedures that facilitate the management of the processes within the institutions. As an example of these technical standards and regarding cybersecurity in the electoral field we can highlight ISO27000 standards on information security, ISO 28000 in charge of supply chain security, or ISO/TS 54001:2019 known as electoral ISO. It is important to establish Information Security Management Systems that contemplate action protocols, definition of roles and functions, standardized documents in order to prevent, or if necessary, to respond effectively and efficiently to a cybersecurity event in the electoral context. These systems must involve all the actors that participate in it, from the citizens to the State security bodies and forces, including those who form the polling stations or make up the electoral administration (Electoral Management Boards).

In addition to the above, it is essential to promote independent and comprehensive audits that evaluate not only the compliance with the electoral legal norms or, if necessary, the adaptation or reform, but also the effectiveness of the cybersecurity policies applied to the electoral processes in each of the institutions. The implementation and knowledge of cybersecurity plans at the institutional level are essential to strengthen resilience in this area. Likewise, the institution's technical bodies (SOC) must have clearly defined roles and functions and be fully aware of the communica-

tion channels established with the State's reference CERTs/CESIRTs. To ensure an effective response to cybersecurity incidents, it is essential that there is a prior relationship of trust, created and strengthened through regular joint exercises and the creation of bodies specially designed to understand the specific needs of electoral procedures, in place at.

At the same time, a new task is required: the adaptation of the normative frameworks and particularly the criminal ones, either the special criminal laws or the criminal codes, going beyond the Convention of Budapest and protecting the electoral procedure itself.

In some States there are special electoral criminal laws that regulate criminal offenses that are mainly designed in an analogical key or criminal codes that are not usually adapted to the technological electoral context, which leads to legal uncertainty and the application of analogies or analogical interpretations. This is why it is recommended to analyze: on the one hand, the categorization of the critical or strategic structure of the electoral procedure; on the other hand, the adaptation of the criminal offenses to the specific technological electoral context.

This adaptation can be done by aggravating the criminal offenses that are not designed for the electoral field if they occur during electoral periods (illegal access to computer systems, illegal interception, and interference with data and systems), or, if necessary, protecting democracy as a legal good within the framework of these criminal offenses. The vast majority of the criminal codes protect patrimony (computer damage and legal interference and data; attacks on computer systems or unlawful intrusion into systems) and with a concurrence of crimes (crimes of alteration of the order of the electoral act, against official electoral documents) could be reached to the protection of the legal good of democracy. In this context, the harmonization of electoral and cybersecurity regulations, as well as the standardization of practices and protocols, are two of the main shortcomings observed at the international level. Overcoming these shortcomings is essential to strengthen the integrity of elections and ensure effective protection against emerging challenges.

Finally, in this regard, another challenge highlighted by the Venice Commission concerns the establishment of a genuine culture of democratic cybersecurity that effectively reaches citizens and fosters a stronger commitment to institutionalized cybersecurity. Such a commitment entails public administrations—particularly those involved in the electoral process—allocating sufficient budgets and personnel to ensure the full implementation of cybersecurity standards. It is equally essential to obtain relevant certifications and conduct regular information security audits. Promoting a culture of democratic cybersecurity strengthens the resilience of electoral processes and safeguards democracy as a whole. This approach must be permanently integrated into electoral structures, encouraging administrations to adopt a proactive stance and demonstrate a robust commitment to digital and technological security. Only through the consolidation of such a culture will it be possible to prevent, mitigate, and respond effectively to risks and threats, reinforce trust in institutions, and protect the integrity of democratic systems in an increasingly complex and uncertain environment.

The development of a genuine culture of democratic and electoral cybersecurity must transcend the strictly institutional sphere to be fully embraced by citizens; only in this way will it be possible to achieve effective resilience and ensure adequate protection against the risks and threats inherent to the electoral techno-digital ecosystem.

4. Conclusion

The analysis of the Venice Commission's reports highlights the growing relevance of cybersecurity in safeguarding the transparency, legitimacy, and stability of electoral processes in the digital age. As elections increasingly rely on technological and digital infrastructure, the risks posed by cyberattacks, disinformation campaigns, and foreign interference have become critical challenges for modern democracies.

The reports reviewed demonstrate a comprehensive and forward-looking approach to addressing these threats. Through a set of guiding principles, the Commission emphasizes the need for adapting international regulations, enhancing institutional capacities, and fostering cooperation between public and private actors. Notably, Principles 6 and 7 underscore the importance of protecting electoral integrity by integrating cybersecurity measures into critical electoral infrastructure and promoting international collaboration and public-private partnerships.

Furthermore, the Commission's focus on emerging technologies, particularly artificial intelligence, reflects an awareness of the evolving nature of digital threats. By extending its analysis beyond traditional issues such as electronic voting and data protection, the Commission recognizes the potential misuse of advanced technologies to disrupt democratic processes. The future challenge facing the Venice Commission could be to carry out a more concrete and detailed analysis of cybersecurity in the electoral framework. This challenge implies addressing not only general issues, but also technical aspects, such as information security management systems, cybersecurity plans and incident response protocols. It will also be necessary to pay attention to the required regulatory adaptations, including the development and implementation of specific criminal and cybersecurity rules for electoral periods, in order to strengthen the protection of democratic processes against digital threats. Finally, the observance of the culture of democratic cybersecurity that transcends from the institutional to the citizenry.

Strengthening cybersecurity in electoral processes requires a comprehensive approach that encompasses institutions, citizens, and public-private actors. This involves fostering a cybersecurity culture within electoral management bodies (EMBs) and among voters, developing robust regulatory frameworks that include everything from criminal codes to cybersecurity, information security, and data protection laws, as well as recognizing and protecting critical electoral infrastructure. Equally essential is the establishment of information security management systems with international standards and certifications such as ISO, which provide trust and transparency, along with the implementation of independent and thorough audits

to evaluate plans and strategies in this field. Only through this combination of culture, regulation, standards, and external oversight will it be possible to consolidate resilient, trustworthy, and legitimate elections in the digital era.

In light of the current challenges facing electoral cybersecurity, it becomes clear that the framework provided by the Budapest Convention is no longer sufficient. While the Convention defines cybercrimes such as illegal access to computer systems (art. 2), illegal interception (art. 3), and interference with data and systems (arts. 4 and 5), among others, its provisions have been transposed into domestic laws of more than sixty States Parties without a uniform or comprehensive approach. In many cases, these offenses are addressed within general Criminal Codes that fail to establish aggravated categories for conduct occurring during electoral periods. As a result, the protected legal interest remains limited to property or system integrity — such as computer damage or unlawful interference with data — rather than the safeguarding of democracy itself. Conversely, special electoral criminal laws often omit these offenses entirely, rendering them obsolete and creating a significant degree of legal uncertainty. Therefore, it is imperative to revise and modernize criminal provisions to explicitly protect democracy as a fundamental legal interest, moving beyond a narrow focus on computer damages or intrusions and ensuring the resilience of electoral systems in the digital era.

To effectively confront these challenges, it is essential to establish a strong culture of cybersecurity at all levels — institutional, governmental, and civic. This requires implementing robust cybersecurity policies, conducting regular independent audits, and ensuring that electoral authorities have well-defined roles and communication channels with national and international cybersecurity organizations. Ultimately, safeguarding electoral processes demands a structural transformation that embeds cybersecurity into the very foundation of democratic systems. Only through sustained commitment, comprehensive regulatory frameworks, and active participation of all stakeholders can trust in electoral systems be preserved and the resilience of democracy strengthened in the face of evolving digital threats.

Abstract

This article analyzes the challenges and responses related to cybersecurity in the electoral sphere, with special attention to the role of the Venice Commission and its most recent reports (2019, 2020, 2024). The study examines how technological advances, cyberattacks, disinformation campaigns, and hybrid threats pose serious risks to electoral integrity, transparency, and trust. It highlights the need to adapt criminal law and electoral legislation, recognize elections as critical infrastructure, and establish robust frameworks for cooperation between states and private actors. Moreover, it stresses the importance of fostering a democratic cybersecurity culture that extends from institutions to citizens, supported by international standards such as ISO certifications, information security management systems, and independent audits. By combining legal, technical, and cultural measures, democracies can strengthen their resilience and safeguard the legitimacy of elections in the digital era.

Keywords

cybersecurity – Electoral integrity – Venice Commission – hybrid threats – disinformation