EUROPEAN CONVENTION ON HUMAN RIGHTS
CONVENTION EUROPÉENNE DES DROITS DE L'HOMME
1950 - 2025 75

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

CDDH-IA(2025)12
07/10/2025

STEERING COMMITTEE FOR HUMAN RIGHTS

COMITÉ DIRECTEUR POUR LES DROITS HUMAINS

(CDDH)

DRAFTING GROUP ON HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE

GROUPE DE RÉDACTION SUR LES DROITS HUMAINS ET L'INTELLIGENCE ARTIFICIELLE

(CDDH-IA)

Compilation of written contributions and presentations received from experts of the exchange of views of the 4th meeting of CDDH-IA

Compilation de contributions écrites et présentations reçues des experts de l'échange de vues de la 4e réunion du CDDH-IA

TABLE OF CONTENTS / TABLE DES MATIÈRES

AI and Elections – Rafael BUSTOS GISBERT

***Elections, AI, and Human Rights*.**
Rafael Bustos Gisbert (professor in Constitutional Law, UCM, Spain. Member of the Venice Commission) Text following the exchange of views with the Council of Europe CDDH Drafting Group on Human Rights and AI (CDDH-IA). 2 April 2025.

0.- Background: the work of the Venice Commission on elections and AI

In recent years, the Venice Commission has carried out several activities related to the use and impacts of digital technologies and Artificial Intelligence in electoral processes.

1) In June 2019, the Venice Commission adopted a Report on digital technologies and elections. This report provided an overview of potential benefits and challenges and of existing and emerging standards and fundamental rights protected at European and universal level[1].
2) In December 2020, the Venice Commission prepared a Set of principles for a fundamental rights-compliant regulation of the use of digital technologies in electoral processes, which should be respected by law-makers, regulators and other actors involved in the use of digital technologies in elections[2]. They emphasise the need for a human rights-compliant approach: namely, that human rights and fundamental freedoms must be translated into the digital environment.
3) The 19th European Conference of Electoral Management Bodies, which was organised by the Venice Commission in November 2022. The topic of the Conference was “Artificial intelligence and electoral integrity”[3].
4) More recently, the Venice Commission has adopted an interpretative declaration of the Code of Good Practice in Electoral Matters as concerns digital technologies and artificial intelligence[4]. It must be underlined that the Code of Good Practice in Electoral Matters, the reference document on electoral matters for the 61 member States of the Venice Commission, if not worldwide. The usefulness of the Interpretative Declaration was demonstrated when the Venice Commission adopted the Urgent Report concerning the annulment of the election results by the Constitutional Court on 14-15 March 2025[5].

1.- A complex scenario

The scenario of AI and elections is extremely complex from different points of view.

[1] Joint Report of the Venice Commission and of the Directorate of Information Society and Action Against Crime of the Directorate General of Human Rights and Rule of Law (DGI) on Digital Technologies and Elections, adopted by the Venice Commission at its Plenary Session 21-22 June 2019

[2] Principles for a Fundamental Rights-Compliant use of Digital Technologies in Electoral Processes, adopted by the Venice Commission at its Plenary Session 11-12 December 2020

[3] See the conclusions of the Conference in https://www.coe.int/en/web/electoral-management-bodies-conference/conclusions-2022

[4] Interpretative declaration of the Code of Good Practice in Electoral Matters as concerns digital technologies and artificial intelligence, adopted by the Venice Commission at its Plenary Session 6-7 December 2024

[5] Urgent Report concerning the annulment of the election results by Constitutional Courts adopted by the Venice Commission at its Plenary Session 14-15 March 2025

1.1.- From the point of view of the **actors** involved: we need to distinguish between public and private actors involved in elections. A nuanced approach is needed:

i) Private actors: but among them we must distinguish: a) individuals, b) political parties/candidates, c) platforms (VLOs and VLOSEs)
ii) Public Authorities: an again the nature of public actors involved is rather diverse: a) Electoral Management Bodies (EMBs), b) Judiciary, c) other Agencies (in particular, data protection agencies).

1.2.- From the point of view of **Human Rights** (HRs) involved

i) Right to vote and to be elected, and more particularly the principles of free, equal, and universal suffrage. But elections depend on the respect of other rights (see the Code of Good Practice, guideline II.2)

ii) ii) Freedom of speech, freedom to impart and receive information, media freedom, pluralistic information, right to property.

iii) Privacy, data protection rights, non-discrimination. Even property might be important when we came to the rights of designers or providers of AI systems.

iv) Access to courts when applicable

v) In the case of digital technologies and AI, their distinction becomes blurred. For example, free suffrage (right to form an opinion: i) right to access any kind of information, ii) right to private internet browsing, iii) right to private internet communications) and equal (equal opportunities) suffrage. The right of voters to freely form an opinion may also be damaged if contestants do not have a levelled playing field.

1.3. From the point of view of the **viability** of issuing legal rules on the topic: a global, cooperative and multilevel approach. The European panorama is rather complex. From the CoE we now have the Framework Convention on AI. At the EU a strategic approach has been followed. The work of the CoE and the UE must be understood not as a competing approach but as complementarity one as Mario Hernández Ramos; current President of the Committee on Artificial Intelligence within the CoE CAI), has underlined[6]. The EU seems to be the most developed example of a global regulation of AI and elections: General Data Protection Regulation (GDPR, 2016/679), Artificial intelligence Act (AIA, 2024/1689), Directive 2022/255 on measures for a high common level of cybersecurity across the Union, Code on practice on disinformation (2022, a text considered as a Code of Conduct on disinformation since 2025 within the framework of the DSA), Regulation on the transparency and targeting of political advertising (2024/900), Digital Services Act (2022/2065), Commission Recommendation (EU) 2023/2829 of

[6] M. Hernández Ramos, “El marco regulatorio europeo de la inteligencia artificial. La relación de complementariedad entre el Reglamento de la UE y la Convención Marco del Consejo de Europa” (“The European regulatory legal framework for artificial intelligence. The complementary relationship between the EU Regulation and the Council of Europe framework convention”), Revista Española de Derecho Europeo, 92, 2024.

12 December 2023 on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament

But the CoE may have set the path, i.e., under the Convention 108//108+ (in particular Art. 9(1) and Art 11), the Budapest Convention, and most importantly through the case-law of the European Court of Human Rights (Animal Defenders Intl v. UK, App 48876/08).
In addition, several other non-binding standards with are key, particularly in the electoral field:

- Venice Commission – documents mentioned above.
- Committee of Ministers: Recommendation CM/Rec(2016)1 on network neutrality; Recommendation CM/Rec(2018)2 on internet intermediaries, Recommendation CM/Rec(2017)5 on standards for e-voting and the Guidelines on the use of information and communication technology (ICT) in electoral processes
- Convention 108 (Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data): Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, Guidelines on the protection of individuals with regard to the processing of personal data for the purpose of voter registration and authentication – ongoing work on neurorights.
- Cybercrime Convention Committee: T-CY Guidance Note #9 on aspects of election interference by means of computer systems covered by the Budapest Convention.

1.4. A **two-pronged process**: risks (it can jeopardise the electoral process) and opportunities (it can improve electoral rights and the administration of the electoral process - registration, e-voting, vote counting, certification of signatures, continuous monitoring of polling day and vote counting, etc.).

2. **The risks posed by AI on free elections**[7]**.**

2.1. *Direct attacks to the electoral process*

i) Attacks on electoral infrastructure – supporting already existing cyberattacks (registry, DoS on electoral web pages, etc)

ii) Attacks on public confidence in the electoral process (massive disinformation strategies, questioning the integrity of elections, questioning the fairness of voting or vote counting, unjustified allegations of fraud, etc.).

iii)

iii) These two risks are even higher when third States attack on electoral processes (*astroturfing*, bots to disseminate misinformation or to favour ideas or candidates, etc)

[7] On these risks, see the conclusions of the Seminar "Private Powers and the Rule of Law" organised by the Venice Commission and the Centre for Political and Constitutional Studies in Madrid 28-29 November, 2024: https://www.cepc.gob.es/blog/seminar-private-powers-and-rule-law-conclusions and Rafael Rubio Nuñez (former substitute member of the Venice Commission): "El uso de la inteligencia artificial en las campañas electorales y sus efectos democráticos" ('The uses of artificial intelligence in election campaigns and their democratic effects'), Revista de Derecho Político, 122, 2025.

2.2. *Negative effects form the use of AI in electoral processes*.

i) *Disinformation*: understood as the dissemination of false information with the intention of undermining the electoral process, which enjoys increased possibilities for strategic and coordinated dissemination of fake news and/or deep fakes. This type of disinformation is even more worrying because of its virality (the ability to spread quickly and widely from one Internet user to another) and scalability (the ability to artificially increase the importance of a particular idea or the popularity of a candidate - or vice versa). It can be carried out by "human-like" bots, which are able to fool the recipients of the information into thinking that they are interacting with humans.

ii) *“Cognitive” hacking through microtargeting* (“Plato’s Cave”): The ability to condition the way voters form their opinions on the basis of personalised information built from their personal data. In this way, the citizen is only presented with information that is tailored to condition his or her political views, creating a 'Plato's cave' effect.

iii) *Fragmentation and polarisation* (“Tribalism”): public conversation due to the use of AI systems can be oriented to take place only among those that share similar political views fragmenting the public sphere in “echo chambers” were polarisation appears as an inevitable consequence[8]

iv) *Online harassment, discrimination and political violence against candidates (especially women)* can become widespread and take new and extremely dangerous forms through the use of AI systems*.*

v) *Communication inequalities* in access to online platforms and AI systems between candidates/political parties, but also between voters, can undermine the existence of a fair playing field for election candidates.

vi) *Simplification of political debate*: AI-generated content, personalised political propaganda and new AI dissemination techniques are based on emotional messages rather than rational discourses. Thus, the political debate becomes not an in-depth discussion of shared concerns, but a competition for immediate attention based on the ability to arouse the emotional interest of the information receiver/voter.

vii) Strategies used by AI systems to condition electoral processes are often *undetectable and unnoticeable*. This makes it extremely difficult to control them.

2.3.- *General challenges*:

[8] On “Plato’s cave” and “tribalism” effects see the conclusions of the Seminar “Private Powers and the Rule of Law” organised by the Venice Commission and the Centre for Political and Constitutional Studies in Madrid 28-29 November, 2024: https://www.cepc.gob.es/blog/seminar-private-powers-and-rule-law-conclusions

Summarising the risks on electoral processes, the main challenges raised by the use of Ai Systems are:

i) Loss of confidence in electoral integrity
ii) General disinformation
iii) Aggressive dissemination techniques
iv) Excessive allocation of "electoral" power in private actors

3. The European Approach to address the risks raised by AI in electoral processes

3.1.- **Premises**: a) Free speech and public debate as the foundation of democracy. b) Free access to internet and all the services as the essential rule (see, ECtHR Ahmed Yildrim vs Turkey, App 311/10, and Cengiz and Others v. Turkey, Appl nos. 48226/10 and 14027/11); c) General principle: internet neutrality (not to be understood as an absolute "shield" for internet intermediaries). d) To approach the risks from a human rights perspective we may use the distinction within the ECtHR case law between a *negative obligations* (on the use of AI by public authorities) and *positive obligations'* approach (mainly, but not only for private actors).

3-2- **Negative obligations of public authorities** when using AI in electoral processes public authorities must not undermine human rights. Thus, procedural and judicial guarantees must be put in force on the use of AI systems by public authorities (EMBs in particular) not to undermine HRs, nor the integrity of the electoral process, In particular the Venice Commission has underlined: a) reinforcement of the impartiality, independence and professionalism of EMBs, b) transparent use of AI; c) auditability of AI systems, d) right to challenge before an independent body both the process of adoption of an AI system and the concrete decisions taken on the basis of a recommendation by an AI. AI systems used in the electoral process by public authorities should respect the rule of law principles related to, *inter alia*, transparency, accountability, and responsibility in the decision-making process regarding the purchase, implementation, monitoring, and use of digital technologies and artificial intelligence

3.2.- **Positive obligations**: The three steps test on limits on Freedom of speech (art. 10 ECHR) linked with the positive obligation by public authorities to protect electoral rights

i) *Stablished by law*: this is probably one of the most urgent aspects. There must be a previsible, accessible and clear legal basis to limit any human right (in particular, but not only, freedom of speech) to defend electoral processes. Some problems have already arisen from the lack of legal rules. The need of a specific, effective and complete regulation has been pointed out by the Venice Commission in its Report on the cancellation of electoral results by Constitutional Courts: "States should regulate the consequences of information disorders, cyber-attacks and other digital threats to electoral integrity; candidates and parties must be granted fair and equitable access to online media, and regulations should be implemented to ensure that artificial intelligence systems by internet intermediaries do not favour certain parties or candidates over others" (par. 78.F).

ii) *Legitimate aim*: protection of democracy

iii) *Necessary in a democratic society*: in assessing the necessity of an interference in a human right a risk-based approach seems to be appropriate. Thus, the distinction between unacceptable risks, high risks, limited risks is recommended.

Electoral processes are high-risk situations which provides justification of stronger positive obligations on public authorities and thus on the activity of private actors. But, as the Venice commission has stated, generic bans on the operation of certain sites and systems are not compatible (with exceptions) with the provisions of the European electoral heritage. Permissible restrictions generally should be content-specific

3.3.- **Justified measures**. Examples:

a) *Substantive positive obligations for ensuring election integrity.* Based on clear, previsible and accessible laws and entrusted to public authorities with enough capabilities and resources.

b) *Procedural positive obligations to investigate attacks on elections:* as Mr. Brezmes pointed out during the exchange of views with the Council of Europe CDDH Drafting Group on Human Rights and AI (CDDH-IA), the positive procedural obligations under *i.e.* arts 2 and 3 ECHR to investigate violations of human rights could be, *mutatis mutandis*, be transposed to the right to free elections under art. 3 protocol 1. Therefore, a duty to investigate attacks on electoral processes using AI systems may be theorised with the same requirements of promptness, independence, efficacy and full participation of victims.

c) *Prohibitions* (examples): Importance of full respect to the right to data protection regulations (most of the use of AI systems to undermine electoral integrity imply a violation of personal data protection). Other prohibitions: a) systems able to manipulate human behaviour, b) biometric categorisation, c) massive surveillance during elections, d) political microtargeting based in personal data related to race, ethnic origin or political ideas, e) contracting of political propaganda by third country organisations in a period of time prior to the elections. *Venice Commission specific standards*: a) Political “deep fakes”, namely the distribution of deceptive artificial intelligence-generated content to influence an election or to infringe voters’ freedom to make informed decisions, should be prohibited and sanctioned. b) It could be banned certain forms of paid political advertising on social media during electoral periods particularly when automated mass dissemination or micro-targeting, techniques based on artificial intelligence are being employed. c) It could be banned anonymously campaigning by political parties and candidates.

d) *Implementation of AI Governance*: risk and impact assessment, certification procedures,

e) *Private actors’ obligations* (examples):

   i. General cooperation duty: including
      1. Self-assessment: increasing obligations of monitoring, auditability and response in electoral periods;
      2. Cooperation with public authorities (in particular EMBs)

ii. Equal access of parties and candidates including:
    1. Minimum access right to internet intermediaries and to AI systems to manage their campaigns and
    2. Ensuring AI systems used by internet intermediaries do not favour certain parties or candidates over other, maintaining a balance in the visibility of electoral content;

iii. Content moderation (specific requirements related to the respect of freedom of speech of platform's users);

iv. Labelling AI generated content,

v. Labelling AI dissemination techniques used in political propaganda,

vi. Transparency on the political nature of a content and

vii. Identification of the sponsors