A European human rights perspective on the use of ICT in election campaigns

Christina Binder[*] and Adam Drnovsky[**]

Abstract: As the EP elections approach, ICT present both opportunities and challenges for election campaigns. While a European regulatory framework for ICT usage is emerging, its adequacy is yet to be tested in the forthcoming elections. European human rights standards serve as a guide for the integration of ICT, allowing to leverage ICT's potential for democracy.

In the digital age, Information and Communication Technologies (ICT) have become essential tools shaping the landscape of politics and democracy. This is particularly evident in the dynamic and decentralised campaigns leading up to the 2024 European Parliament (EP) elections. As the political arena evolves, candidates, parties, and voters alike are using ICT like never before to engage,

---

[*] Christina Binder holds the Chair for International Law and International Human Rights Law at the Bundeswehr University Munich. Before, she was University Professor of International Law at the University of Vienna. Christina is a member of the governing Council of the Global Campus of Human Rights and former Vice-President of the European Society of International Law.

[**] Adam Drnovsky is an EMA alumnus, currently working as an Independent Electoral Consultant and pursuing a PhD in International Human Rights Law at the Bundeswehr University Munich. Before, he held the position of Election Observation Officer at the Council of Europe.

inform, and mobilize constituents. Social media platforms, mobile applications, and data analytics are just a few examples of the ICT arsenal used by campaigners to amplify their messages and connect with a diverse electorate across the EU.The increasing digitization of the campaign landscape brings both opportunities and challenges. While ICT enables unprecedented levels of outreach and engagement, it also raises concerns regarding privacy, disinformation and foreign interference. As we navigate this digital democracy, it is imperative to critically examine the implications of ICT on electoral processes, especially in election campaigns.

Opportunities and challenges of ICT uses

Numerous examples from EU countries demonstrate that throughout election campaigns, ICT serves as a catalyst for political mobilisation, communication, and outreach to voters. Campaign teams utilize digital platforms, social media, and data analytics to engage supporters. Interactive websites, and mobile apps facilitate the direct dialogue between candidates and constituents, enhancing citizen participation. Furthermore, ICT enables effective program communication, allowing campaigns to articulate policy positions and engage voters on critical issues, thus giving them broader possibilities to form their opinion.
However, the European Parliament and the Commission have both voiced concerns about cybersecurity threats and disinformation campaigns. Moreover, foreign interference during the campaign to the EP elections is a real issue that needs addressing. Therefore, the challenges posed by ICT in the context of elections need full recognition. One issue highlighted by the EP is the campaign's vulnerability to cyberattacks, including hacking, phishing attacks, and data breaches, aiming to compromise campaign websites or social media accounts. This can lead to disruptions of campaign operations, theft of sensitive information, or spread of disinformation. A breach of campaign data can damage the integrity of the electoral process and erode public trust in the campaign. Cyberattacks have the potential to cripple election campaigns, undermining the right to free elections by violating online freedom of expression. Breaching databases containing personal information and misusing it further constitutes a violation of privacy rights. The proliferation of disinformation on ICT platforms poses another risk to election campaigns, potentially involving foreign interference. As the European Commission recently highlighted, malicious actors may spread mis- or disinformation, including AI-generated content like deep fakes, to manipulate public opinion, discredit opponents, or undermine confidence in elections. Segments of society that possess lower digital skills may be particularly vulnerable. In this context, unequal access to ICT infrastructure and digital literacy skills can exacerbate existing disparities, raising questions of political equality. In addition, the spread of mis- or disinformation significantly affects voters' freedom to express their opinions by making informed choices at the polls. Moreover, AI-based algorithms employed on social media platforms

may exhibit bias in content distribution and audience targeting. This poses the risk of discrimination and negatively impacts on the equality of opportunity to participate in elections.

The European human rights framework

The use of ICT in election campaigns is regulated at two levels in Europe. Firstly, in the framework of the Council of Europe (CoE), the European Convention on Human Rights (ECHR) contains relevant standards based on the right to free elections and related rights, supplemented by ECtHR jurisprudence. This is further supported by a growing corpus of CoE treaties that address the wider application of ICT, including in elections.

Secondly, the EU is currently developing a regulatory framework for ICT in elections, most notably the Digital Service Act (DSA). The Act regulates online intermediaries and platforms in order to prevent illegal and harmful activities online and the spread of disinformation, also during election campaigns. While the DSA is effective already and will be applicable during the campaign period of the EP elections, other key instruments such as the EU AI Act and the Media Freedom Act are still in the process of adoption and will not be ready before these EP elections. Under the ECHR, the **right to free elections** (Article 3 of Protocol 1) establishes the right to vote and to stand for elections, under conditions where people can freely form and express their opinions and choose their representatives. Additionally, the right to freedom of expression (Article 10 ECHR) is especially relevant in the ICT context as it is closely interrelated with the right to free elections. In accordance with ECtHR case law, both rights mutually reinforce each other. For this reason, it is particularly important during the election campaign that opinions and information are permitted to circulate freely, including in the public digital sphere as Article 10 ECHR also protects the methods of dissemination. Ensuring an open public debate is pivotal: the ECtHR indeed highlighted the significance of 'the free exchange of opinions and ideas' (*Gillberg v. Sweden*), which is essential for fostering a democratic environment. Therefore, in its case law (*Observer and Guardian v. the United Kingdom*), the Court made clear that online media and bloggers are also protected under Article 10 ECHR. The ECtHR has also recognised individuals' **right to access the internet**. In its ruling against the wholesale blocking of online content, the Court asserted that:

> 'the internet has now become one of the principal means of exercising the right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest (*Cengiz and Others v Turkey*, para 49).

Therefore, measures blocking internet access will only be compatible with the ECHR if a strict legal framework is in place, regulating the scope of the ban and

affording the guarantee of judicial review to prevent possible abuses. Finally, the ECtHR has emphasised the state's responsibility to prevent inequality in media coverage during elections, also online (*Animal Defenders International v. the United Kingdom*) Another right of particular significance is the **right to respect for private and family life** (Article 8 ECHR). It has likewise been subject to extensive jurisprudence by the ECtHR. For example, the Court has developed detailed standards for the protection of personal data. Further standards are found in the Modernised Convention 108 which establishes principles and regulations for personal data processing, sets standards for the establishment of data protection supervision, and provides that data must be processed fairly and transparently, collected for explicit, specified, and legitimate purposes, and not processed in a manner incompatible with those purposes. All this is of immediate relevance for the protection of privacy rights in electoral processes.

Concerning cyberattacks during election campaigns, the Budapest Convention deals with disinformation operations that violate rules regarding the protection of personal data, political finances, media coverage, or the broadcasting of elections. While this type of conduct does not constitute cybercrime *per se*, the evidence that such rules are broken often takes the form of electronic evidence. It is therefore essential, according to the Convention, that states provide their criminal justice authorities with the necessary powers to secure such evidence. However, despite the significance of AI tools introduced during election campaigns, there is currently no instrument regulating the use of AI in elections. While the ECtHR has never specifically addressed AI in elections, certain insights may be derived from the Court's jurisprudence relating to algorithms and violations of Article 8 ECHR (right to private life, e.g. *Centrum för Rättvisa v. Sweden*) or Article 10 ECHR (freedom of expression, e.g. *Big Brother Watch v. The United Kingdom*), and indirectly Article 14 ECHR (non-discrimination). Although certain judgments of the ECtHR address some of the critical issues related to the use of ICT in elections, its practical impact remains rudimentary as regards standard setting in the area of elections. Likewise, the above-mentioned Conventions adopted in the field do not cover all relevant aspects.

Finally, within the **EU legislative framework**, the DSA regulates the online information environment, which involves limiting the dissemination of illegal and harmful content, such as disinformation and hate speech. This is achieved by imposing a set of obligations on private entities, including online platforms, social networks, and application stores. Additionally, the DSA ensures the protection for users, for instance by requiring online platforms to enhance transparency on algorithmic usage and on recommended content. The legislation is applicable to all online platforms which are obliged to implement measures to prevent and remove posts containing illegal content, while simultaneously providing the means to report this type of content. Moreover, DSA guidelines prepared by the Commission aim to present relevant online platforms with best practices and possible measures to 'mitigate systemic risks that may threaten the integrity of

democratic electoral processes'. The enforcement of and compliance with the DSA is conducted by the Commission together with relevant national authorities, and violations of the rules by online platforms may be progressively fined or result in temporary suspension of services within the EU. This presents quite a significant potential of deterrence. While the DSA has not been tested during elections so far, overall, it has been positively accepted and should improve the upcoming EP elections.

Looking ahead

European standards for ICT uses during election campaigns are rudimentary. However, best practices and electoral principles applicable to e-voting and the use of ICT in elections in compliance with human rights usefully complement applicable standards. Best practices establish that during election campaigns, the freedom of expression and information must be fully translated into the digital environment, in line with provisions of ECHR and ECtHR case law.
Yet, freedom of expression is not unlimited and state authorities should effectively intervene if necessary, for instance by requiring private companies to remove clearly defined third-party content in case it breaches election legislation. Relatedly, open internet and net neutrality should be protected, in order to ensure a level playing field for users and content providers. Additionally, internet service providers must be prevented from unilaterally deciding on the availability of online contents during election campaigns. Best practices likewise provide that online advertisements should be regulated to preserve the integrity of elections. This entails revising the regulations on political advertising in terms of media access and in relation to spending, including transparency of paid advertisements. Furthermore, respect for the rules can only be achieved when criminal justice authorities have the power to investigate online violations of rules on political finances and other illegal actions. Finally, the adoption of self-regulatory frameworks by relevant internet intermediaries should be promoted. These can take the form of ethics and corporate social responsibility codes requiring that political advertisements be clearly labelled, increasing their transparency in the process of buying, and allowing for the deletion of fake accounts. International and public-private partnerships would be beneficial for exchanging information as well as for increasing the efficiency of possible investigations, prosecutions and sanctions for illegal conduct. All this contributes to concretising the right to freedom of expression (Article 10 ECHR) in relation to ICT uses in electoral processes. So, overall, we are faced with an emerging regulatory framework for ICT uses during election campaigns. It remains to be seen whether it will suffice for the upcoming EP elections.