International IDEA

STIFTUNG MERCATOR

NAVIGATING THE EUROPEAN UNION'S DIGITAL REGULATORY FRAMEWORK: PART 1

A Compact Overview of Its Impact on Electoral Processes

NAVIGATING THE EUROPEAN UNION'S DIGITAL REGULATORY FRAMEWORK: PART 1

A Compact Overview of Its Impact on Electoral Processes

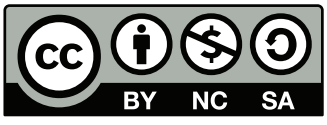
Sebastian Becker Castellaro, Gladiola Lleshi and Juliane Müller

International IDEA
INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

STIFTUNG MERCATOR

The project 'Closing the Digital Gap on Elections in EU Accession' is funded by Stiftung Mercator.



International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
Tel: +46 8 698 37 00
Email: info@idea.int
Website: <https://www.idea.int>

Cover illustration: VectorMine
Design and layout: International IDEA
Copyeditor: Curtis Budden

DOI: <https://doi.org/10.31752/idea.2025.64>

ISBN: 978-91-8137-005-8 (PDF)

Project context

Digitalization is reshaping electoral processes across the European Union and its neighbouring countries that aspire to join. While it offers powerful tools to enhance democratic participation, it also introduces new vulnerabilities—ranging from non-transparent political finance in online campaigning and disinformation to foreign interference and cybersecurity threats. These challenges demand robust digital governance and vigilant oversight to ensure that elections remain free, fair and transparent both within and beyond EU borders.

To this end, the EU's comprehensive digital acquis serves as a cornerstone of democratic resilience. This body of legislation significantly influences the organization and conduct of elections, including in countries seeking EU membership. These countries, often facing resource constraints, must navigate the process of approximating the acquis while also addressing pressing challenges such as foreign interference and the effective oversight of online campaigning. In turn, the frontline experiences of enlargement countries can offer valuable lessons for the EU itself.

This research, titled Navigating the European Union's Digital Regulatory Framework, is developed under the project Closing the Digital Gap on Elections in EU Accession, funded by Stiftung Mercator. It comprises two complementary parts that together aim to address a critical gap in the interaction between the EU and candidate and potential candidate countries.

Part 1, *A Compact Overview of Its Impact on Electoral Processes*, explores the EU's digital rulebook—anchored in landmark regulations such as the Artificial Intelligence Act, the Digital Services Act, the European Media Freedom Act, the General Data Protection Regulation and the Regulation on the Transparency and Targeting of Political Advertising. It offers a concise analysis of one of the world's most comprehensive efforts to align technological innovation with democratic values. Through practical examples, it illustrates how these regulations help safeguard against cyberthreats, privacy breaches, unethical use of artificial intelligence (AI) in electoral processes, and opaque political advertising.

Part 2, *Perspectives on Electoral Processes in EU Candidate Countries*, examines the progress of candidate countries in aligning with the EU acquis. It assesses their legislation, institutional frameworks, enforcement capacities and experiences in addressing digital threats to elections. This section focuses on four candidate countries—Albania, Moldova, North Macedonia and Ukraine. Insights drawn from in-house and field research provide valuable input for both national and EU-level discussions.

The findings and recommendations presented here offer concise yet comprehensive guidance for electoral management bodies, policymakers and civil society organizations in accession countries, as well as for EU institutions. They also lay the groundwork for the next phase of the project, which aims to foster closer ties and exchange of knowledge among these actors.

This work is especially timely. The four accession countries have set ambitious goals to complete EU membership reforms by 2030, while the EU is intensifying efforts to fully enforce digital regulations to protect democratic institutions and elections—notably through the European Democracy Shield Initiative. This study supports those developments and contributes to strengthening the relationship between the EU and its aspirant members.

Acknowledgements

This report was developed by the International Institute for Democracy and Electoral Assistance (International IDEA) in the framework of the project 'Closing the Digital Gap on Elections in EU Accession', funded by Stiftung Mercator. The report was written by Sebastian Becker Castellaro, Gladiola Lleshi and Juliane Müller. The research benefited from the contributions and feedback of Alberto Fernandez Gibaja, Thijs Heinmaa, Blerta Hoxha, Phillip Rothe, Sophie Rau, Sam van der Staak and Peter Wolf.

Abbreviations

AI	Artificial intelligence
CJEU	Court of Justice of the European Union
DSA	Digital Services Act
ECHR	European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms)
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDS	European Democracy Shield
EMB	Electoral management body
EMFA	European Media Freedom Act
ENISA	European Union Agency for Cybersecurity
FIMI	Foreign information manipulation and interference
FRIA	Fundamental rights impact assessment
GDPR	General Data Protection Regulation
HRW	Human Rights Watch
ICT	Information and communication technology
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TTPA	Regulation on the Transparency and Targeting of Political Advertising
VLOP	Very large online platform
VLOSE	Very large online search engine

Contents

EXECUTIVE SUMMARY

This mapping study provides a comprehensive overview of the European Union's digital regulatory framework and its growing influence on democratic processes and electoral integrity. Rooted in the EU's foundational values (i.e. democracy, the rule of law and fundamental rights), the study examines how key legislative instruments have been designed to address the complex challenges posed by digital technologies and their interactions with electoral processes. The analysis demonstrates how these regulations—including the Artificial Intelligence Act (2024), the Digital Services Act (2022), the European Media Freedom Act (2024), the General Data Protection Regulation (2016) and the Regulation on the Transparency and Targeting of Political Advertising (2024)—are collectively shaping a legal environment that upholds transparency, accountability and fairness in an increasingly digitalized electoral landscape.

Furthermore, the study underscores the importance of safeguarding fundamental rights in the context of data use, online content and artificial intelligence. It illustrates how the misuse of personal and sensitive data, opaque algorithmic systems and manipulative online practices threaten the integrity of electoral processes. Through legal analysis and jurisprudence from EU courts, the study highlights how democratic principles are protected through data minimization, proportionality, consent and transparency standards. These principles are critical in managing the risks posed by artificial intelligence–driven microtargeting, political advertising and content amplification, particularly on very large online platforms.

Case studies of the 2022 Hungarian parliamentary election and the 2024 Romanian presidential campaign vividly demonstrate the consequences of regulatory and enforcement gaps. These real-world examples reveal how online manipulation, disinformation and the

failure to protect sensitive data can distort electoral outcomes and erode public trust. The study calls attention to the urgent need for more robust institutional cooperation, clearer regulatory mandates and consistent enforcement at the levels of both the EU and its member states.

From the perspective of electoral management bodies (EMBs) across EU member states, this evolving regulatory landscape presents both opportunities and significant operational challenges. EMBs are increasingly being assigned additional responsibilities, though their legal mandates and institutional capacities often vary widely. It is noteworthy that the implementation of the EU's digital regulatory framework remains novel and poses challenges even for the most advanced member states, many of which continue to navigate complex legal, technical and institutional ecosystems in adapting to the evolving digital landscape.

Despite such complexities, the EU's digital rulebook represents one of the most ambitious efforts globally to align technology governance with democratic values. Going forward, effective implementation will depend on the ability of EU institutions and the authorities in member states, including EMBs, to coordinate more closely, share good practices, and reinforce digital literacy and resilience throughout the electoral cycle.

In conclusion, the study positions the EU's digital acquis as not only a framework for market regulation but also a vital instrument for democratic resilience. It calls for coordinated governance and vigilant oversight to ensure that technological innovation serves, rather than undermines, the values of open, fair and transparent democratic systems. Initiatives such as the European Democracy Shield exemplify this forward-looking approach, aiming to strengthen societal and institutional defences against evolving digital threats to democracy.

Chapter 1

FUNDAMENTAL PRINCIPLES UNDERPINNING EU DIGITAL REGULATION AND ITS IMPACT ON ELECTORAL PROCESSES

1.1. DEMOCRACY, FUNDAMENTAL RIGHTS AND RULE OF LAW AS CORE EUROPEAN VALUES OF THE EU DIGITAL ACQUIS

Democracy, the rule of law and respect for fundamental rights are core principles embedded in the founding treaties of the European Union. The principles mentioned in article 2 of the Treaty on European Union (TEU) serve as the cornerstone of EU policy and regulation, including the EU digital acquis.

The importance of article 2 of the TEU lies in its declaration:

> The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.

At the same time, article 6(1) of the TEU makes explicit reference to the Charter of Fundamental Rights of the European Union (the Charter), recognizing its legal value to be the same as that of the Treaties. The Court of Justice of the European Union (CJEU) has affirmed the binding nature of the Charter insofar as EU law is applicable and has played a crucial role in interpreting its provisions (CJEU 2021).

In addition to the Charter, article 6(3) of the TEU further reinforces the protection of fundamental rights by establishing that the rights

guaranteed by the European Convention on Human Rights (ECHR) form general principles of EU law. With regard to the ECHR as a living instrument, the European Court of Human Rights (ECtHR) has played a significant role in shaping the understanding of these rights, influencing both national and EU legal frameworks.

The CJEU also takes ECtHR jurisprudence into account when interpreting fundamental rights under EU law, ensuring coherence between EU law and the broader European human rights framework and legitimizing CJEU statements (Tinière 2023: 328).

EU values, as well as the rights and freedoms enshrined in the EU's legal framework, must be respected online as they are in the real world.

The EU's commitment to an inclusive, fair, safe and sustainable digital transformation is enshrined in the European Declaration on Digital Rights and Principles. A first of its kind, the Declaration builds upon the Charter, citing article 2 of the TEU in stipulating that EU values, as well as the rights and freedoms enshrined in the EU's legal framework, must be respected online as they are in the real world.

The above overview provides a clear picture of how fundamental rights, democracy and the rule of law are not only foundational principles of the EU but also legally binding obligations for both EU institutions and member states. By embedding these principles into the EU's legal framework, including the digital acquis, the EU is ensuring that digital policies—such as those governing data protection (the General Data Protection Regulation, GDPR), platform regulation (the Digital Services Act, DSA), AI governance (Artificial Intelligence Act, AI Act), media freedom (European Media Freedom Act, EMFA), and political advertising transparency (Regulation on the Transparency and Targeting of Political Advertising, TTPA), among others—are aligned with fundamental rights.

Furthermore, the explicit reference in article 51(1) of the Charter reinforces member states' obligation to respect these rights when implementing EU law, ensuring consistency in upholding democratic values and the rule of law across the Union.

This legal framework provides the foundation for safeguarding electoral integrity, protecting privacy and ensuring transparency in the digital space.

1.2. PROTECTING ELECTORAL INTEGRITY IN EU JURISPRUDENCE: THE ROLE OF THE ECTHR AND THE CJEU IN SHAPING ELECTIONS

The EU's digital policy is profoundly shaped by the foundational principles laid out in the TEU and the broader EU legal framework. This framework includes core documents such as the EU Charter of Fundamental Rights and the ECHR, as well as pivotal jurisprudence from the CJEU and the ECtHR. These principles underscore the EU's commitment to upholding democratic values, including the integrity of elections, which is a cornerstone of any functioning democracy.

The right to free elections is enshrined in article 3 of Protocol No. 1 to the ECHR. This principle, as interpreted by the ECtHR, emphasizes transparency, accessibility and the protection of voters' rights against external manipulation.

The ECtHR has progressively interpreted this article to address challenges posed by modern technological advancements, particularly in the realm of digital platforms. This evolution in jurisprudence underscores the importance of transparency, accessibility and the protection of voters' rights against external manipulation in the digital age.

In *Davydov and Others v Russia*,[1] the ECtHR emphasized the state's positive obligation to ensure the integrity of the electoral process, including the careful regulation of the process in which the results of voting are ascertained, processed and recorded.

Additionally, the ECtHR offers a comprehensive guide highlighting the evolving nature of electoral rights, noting the necessity for member states to adapt their legal frameworks to address new challenges, including those arising from digital technologies. The guide underscores that the right to free elections encompasses not only the act of voting but also the broader context in which elections occur, including the information environment shaped by digital platforms (European Court of Human Rights 2024).

The ECtHR offers a comprehensive guide highlighting the evolving nature of electoral rights, noting the necessity for member states to adapt their legal frameworks to address new challenges, including those arising from digital technologies.

The CJEU has played a fundamental role in shaping EU policies around electoral integrity, especially regarding data protection and privacy. In *Schwarz v Stadt Bochum*,[2] the Court emphasized the necessity of stringent data protection measures in electoral contexts, ensuring that voter data is handled responsibly. Further jurisprudence,

1 App no 75947/11 (ECtHR, 30 May 2017).
2 Case C-291/12 (2013).

such as in *Digital Rights Ireland Ltd v Ireland*,[3] addressed the delicate balance between security concerns (data retention) and fundamental rights, influencing policies such as the GDPR.

These rulings illustrate the broader need for transparency in data collection practices and the protection of voters' privacy in digital contexts.

The Planet49 GmbH case[4] and *Google v CNIL*[5] underscore the importance of explicit consent for data processing under the GDPR. While the Planet49 case emphasizes the need for active, informed consent (such as avoiding pre-checked boxes), the Google case highlights the territorial scope of privacy protections, specifically the right to be forgotten. These rulings, although not directly related to political microtargeting, illustrate the broader need for transparency in data collection practices and the protection of voters' privacy in digital contexts, which is crucial for political campaigns that engage in microtargeting.

Lastly, the EU digital acquis is firmly rooted in the Union's core values of democracy, the rule of law and fundamental rights, ensuring that digital transformation supports and does not undermine electoral integrity. Grounded in the TEU, the Treaty on the Functioning of the European Union (TFEU) and the Charter, and shaped by CJEU and ECtHR jurisprudence, EU digital regulations such as the AI Act, the DSA, the GDPR, the EMFA and the TTPA collectively safeguard transparency, data protection, media freedom and fair political participation. This integrated legal framework ensures that the same rights and protections apply online as offline, preserving democratic processes in the digital age.

3 Case C-293/12 (2014).
4 *Verbraucherzentrale Bundesverband eV v Planet49 GmbH* (Case C-673/17 2019).
5 Case C-507/17 (2019).

Chapter 2

STRENGTHENING DEMOCRACY ONLINE: EUROPEAN DIGITAL RULEBOOK AND ELECTIONS

2.1. THE RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION IN ELECTORAL PROCESSES

Reliance on personal data has created ongoing tension between data protection principles and electoral requirements.

Election authorities are increasingly gathering, analysing and using personal data to improve the efficiency of the electoral cycle. Electoral actors can use such data to identify voters, for voter registration and to deploy electoral campaigns, among other things. However, this reliance on personal data has created ongoing tension between data protection principles and electoral requirements. For example, while voter lists need to be transparent and accessible for scrutiny by electoral stakeholders, this need for openness can conflict with the obligation to safeguard individuals' personal information.

Electoral authorities should acknowledge this tension and develop mechanisms that comply with both data protection principles and electoral requirements. In this vein, International IDEA has developed guidelines on the use of biometric technologies during elections (Wolf et al. 2017) and a database of the use of information and communication technologies (ICTs) in elections (International IDEA n.d.). These products should be used with the utmost caution and with an understanding of the serious challenges that reliance on digital technologies to improve the efficiency of electoral processes pose to the right to privacy and protection of personal data.

Accordingly, to protect the right to privacy and personal data, the EU enacted the GDPR (European Union 2016). This piece of legislation seeks to protect fundamental rights recognized by the Charter, such as respect for private and family life (article 7) and the protection of personal data (article 8). The same protections can be found in article 16(1) of the TFEU. The main goal of the GDPR is to establish

data protection principles and rules that must be followed by state authorities and private actors. Consequently, EU member states should update their existing national data protection laws based on the GDPR in order to harmonize their legal frameworks and ensure the free flow of personal data among different countries (FRA and CoE 2018: 29).

The implementation of free and fair elections might limit the exercise of the right to the protection of personal data through a proportionality test.

To implement democratic elections, electoral authorities must comply with the right to privacy and data protection in electoral contexts (Gross 2010: 5–6). These rights are part of a broader system of European values. Accordingly, these rights may be limited if it is necessary to achieve an objective of general interest. Limitations on data protection and the right to privacy should be evaluated case by case under specific circumstances. Based on article 52(1) of the Charter and article 23(1) of the GDPR, for instance, the implementation of free and fair elections might limit the exercise of the right to the protection of personal data through a proportionality test, which should:

- be carried out in accordance with the law;
- respect the essence of the fundamental right to data protection;
- be subject to the principles of proportionality, necessity and legitimate aim; and
- pursue an objective of general interest recognized by the EU (FRA and CoE 2018: 36).

2.1.1. **The application of GDPR principles in relation to elections**

The use of technologies in the context of democratic elections relies on collecting, storing and analysing personal data. Voter registration, biometric identification technologies and electronic voting are examples of how the use of technologies is closely linked to the processing of personal data during elections. According to article 5 of the GDPR, electoral actors' use of these technologies must comply with the following principles: (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimization; (d) data accuracy storage limitation; and (e) integrity and confidentiality.

These principles govern the processing of personal data. Any restrictions on or exemptions to these principles should be provided by law, pursue a legitimate aim and be necessary and proportionate

Box 2.1. **Overview of the GDPR: Key elements for elections**

The GDPR upholds democracy and the rule of law by preventing the misuse of personal data, promoting transparency and ensuring accountability in electoral processes (European Commission n.d.b). These elements are particularly relevant in the context of digital political campaigns, where personal data is increasingly used for microtargeting voters, often leading to concerns over manipulation and privacy violations.

The GDPR establishes clear legal safeguards against the unlawful collection and processing of voter data, reinforcing citizens' rights and electoral integrity. In an era where data-driven political campaigns and microtargeting have become prevalent, the GDPR serves as a crucial mechanism for ensuring that digital election strategies respect democratic principles and fundamental rights (Monteleone 2019).

By embedding strong data protection principles into the EU's legal framework, the GDPR ensures that political actors, online platforms and electoral authorities operate in a transparent, fair and accountable manner. This legal safeguard protects electoral integrity, prevents undue influence in democratic decision making and reinforces the rule of law across the EU.

in a democratic society (article 23[1] GDPR), and they should be evaluated on a case-by-case basis.

Hence, in the context of free and fair elections, the lawfulness of the processing of personal data by electoral actors should be based on one of three grounds: (a) a legal obligation; (b) the consent of the data subject; or (c) the necessity of performing a task in the public interest or in pursuit of a legitimate interest.

For instance, to make a reliable voter list in a specific electoral district, an electoral management body (EMB) must process voters' personal data in order to implement the voter registration and authentication system. This processing of personal data could be permitted based either on freely, informed and unambiguous consent (article 4[11] and article 7 GDPR) or on the national electoral law (Council of Europe 2024). If either of these standards is met, it is considered lawful for electoral authorities to process personal data in the course of implementing ICTs or other digital technologies in elections. In other words, electoral authorities should always have a clearly established legal basis for processing personal data under the GDPR.

Consent is being used to circumvent the GDPR and obtain huge amounts of personal data in the context of online political advertisements without meaningful knowledge on the part of the user.

2.1.2. **The problem of consent**

There are limitations to the processing of personal data under the GDPR. In the context of online political advertising, several actors have denounced the illusion of freely, informed and unambiguous consent needed under the GDPR. For instance, the new European regulation, the TTPA, cautions against 'dark patterns' that 'materially distort or impair, either on purpose or in effect, the autonomous and informed decision-making of ... individuals' (recital No. 75 TTPA). The European Data Protection Supervisor (EDPS) underscores the risks of leading users 'into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data' (European Data Protection Supervisor 2022: 2). In short, consent is being used to circumvent the GDPR and obtain huge amounts of personal data in the context of online political advertisements without meaningful knowledge on the part of the user.

When it comes to special categories of personal data such as political beliefs, ethnicity or sexual orientation, the processing of personal data is prohibited in principle (article 9 GDPR) unless explicit consent is given for data processing—or other legal grounds mentioned in article 9(2) of the GDPR apply. The TTPA applies the same criteria: the use of special categories of personal data is prohibited in the context of online political advertising, including in the context of using targeting and ad-delivery techniques employed by online publishers, unless the data subject's consent is collected explicitly and separately for the purposes of political advertising (article 18 TTPA).

Reliance on consent to prevent the processing of sensitive data and the lack of mechanisms to prevent exploitation by private actors have had an enormous impact on online political advertising. The use of personal data in the context of online political advertising has transformed how voters are targeted and engaged. Thanks to behavioural targeting techniques, online political campaigns are using artificial intelligence (AI) systems to microtarget citizens on social media platforms with tailored political messages (Juneja 2024). Microtargeting entails the following:

- collecting data and dividing voters into segments based on characteristics such as personality traits, interests, background or previous voting behaviour;

- designing personalized political content for each segment; and

- using communications channels to reach the targeted voter segment with these tailor-made messages (International IDEA 2018).

These techniques can benefit both political parties and EMBs by expanding access to information for people who are not normally engaged in electoral processes. However, the same tools may also be used to manipulate citizens and undermine the public sphere by hindering public deliberation, accelerating political polarization and facilitating the spread of disinformation (Gorton 2016). The use of targeting techniques based on personal and sensitive data often takes place without users' consent or clear understanding (Bashyakarla et al. 2019).

As mentioned earlier, given how platforms and the online advertising industry are using deception (such as so-called dark patterns) to obtain 'consent', these risks of manipulation, polarization and the spread of disinformation may affect the integrity of elections. At the same time, deceptive consent practices create vulnerabilities that malicious actors can exploit to disseminate disinformation and manipulative content.

Deceptive consent practices create vulnerabilities that malicious actors can exploit to disseminate disinformation and manipulative content.

2.1.3. **Microtargeting and delivery techniques to reach voters: AI and automated decision making under the GDPR**

The GDPR recognizes that automated decision-making processes—such as AI systems for profiling or online advertising delivery techniques—may have serious consequences. Thus, article 22 of the GDPR states that individuals have the right to not be subject to a decision based solely on automated processing (without human involvement in the decision process). However, the GDPR (article 22[1]) establishes that AI models can be trained on personal data if there is a specific lawful ground, such as consent, a contract or a legitimate interest. Furthermore, the GDPR also stipulates that citizens should be informed of the intention to train an AI model and be given the right to object or withdraw consent. Finally, individuals can appeal to the data controller for meaningful information about the logic behind the processing or to have an automated decision reviewed by a human.

Despite these rules, civil society organizations and scholars have highlighted the limitations of applying the GDPR to AI systems and the implications doing so has for individual rights. For instance, even though online platforms ensure that a certain category of personal data will not be collected, other data is collected and combined, revealing sensitive information about individuals, such as their

political opinions, that social media companies, data brokers or third parties can infer. Additionally, given the very nature of deep machine-learning AI tools, data subjects (citizens) cannot possibly receive a meaningful explanation of how their personal data is processed, since these AI systems are inherently opaque and lack interpretability (Juneja 2024: 12; European Partnership for Democracy 2022: 5). Moreover, the fragmented and delayed application of the GDPR (Massé 2023: 3–4) makes it even more difficult to comply with GDPR principles such as data minimization and purpose limitation in the field of online campaigns.

2.1.4. **Microtargeting and amplification techniques under the GDPR**

As mentioned earlier, microtargeting techniques in online political campaigns target users based on an analysis of their personal and sensitive data to create highly tailored profiles based on their online behaviour (International IDEA 2018). Although microtargeting techniques may provide benefits for citizens by amplifying information around electoral processes, these techniques also pose several risks to rights and freedoms, such as manipulation or foreign interference (European Parliamentary Research Service 2019: 22). Microtargeting and amplification techniques not only reinforce polarization through the business models of big tech companies; they are also built upon an opaque structure that prevents authorities from monitoring compliance with data protection rules and from determining how money flows between publishers, social media companies, political parties and other actors (Heinmaa 2023: 15).

One of the greatest challenges for electoral authorities is determining how to oversee online electoral campaigns when they are highly personalized and take place within an opaque system.

These business models rely heavily on engagement-driven algorithms, which tend to prioritize emotionally charged or divisive content—often referred to as 'rage bait'—to maximize user attention and advertising revenue. This dynamic incentivizes the spread of polarizing narratives, deepening social divisions. The lack of transparency surrounding how content is promoted, who funds it and which users are targeted makes it nearly impossible to understand what information has been seen, by whom, under what conditions and as a result of what algorithmic decisions—undermining accountability and democratic oversight. One of the greatest challenges for electoral authorities is determining how to oversee online electoral campaigns when they are highly personalized and take place within an opaque system.

2.1.5. **Limiting the use of special categories of personal data in electoral contexts**

We have seen that there are both limitations and challenges in the application of the GDPR in the context of electoral processes.

In response to the significant challenges posed by the use of personal data in online political advertising—such as the lack of transparency, profiling based on sensitive information and potential manipulation of voter behaviour—the European Data Protection Supervisor has called for a prohibition on the collection and processing of special categories of personal data, including information about individuals' health, sexual orientation and political affiliation (European Data Protection Supervisor 2022). This guidance reflects concerns that the GDPR alone may not adequately prevent the exploitation of sensitive data in political campaigning. Notably, this position aligns with the proposed provisions in article 18 of the TTPA, which seeks to impose stricter limits on the use of such data for targeting purposes in political contexts.

There is no justification in a democratic society for collecting and processing sensitive data for online political campaigns. The potential risks of microtargeting techniques, the underenforcement of the GDPR by electoral and data protection authorities, and the challenges surrounding consent under the GDPR are all arguments against allowing any exceptions for the use of special categories of personal data for the purposes of online political advertising.

There is no justification in a democratic society for collecting and processing sensitive data for online political campaigns.

In sum, the use of microtargeting techniques during elections has also revealed the limitations of enforcing GDPR rules in relation to online political advertising. Limiting the flow of personal data between private and public actors helps prevent infringements of fundamental rights that could undermine electoral processes. Ensuring the effective implementation of the GDPR in electoral contexts is one of the most important challenges for electoral authorities and policymakers.

2.1.6. **Electoral authorities as controllers: Data protection impact assessments**

In the context of elections, political parties, electoral authorities, individual candidates, civil society organizations (observers) and publishers, among others, may fall under the scope of the GDPR, meaning that public authorities have a legal obligation to process personal data and that other actors—such as political parties—must obtain consent or be able to demonstrate a legitimate interest (European Commission 2018: 5).

Box 2.2. **Hungary's 2022 parliamentary election**

A remarkable example of how the GDPR has functioned in the context of elections is the well-documented case of the 2022 parliamentary election in Hungary. A weak data protection framework, combined with a lack of enforcement by data protection authorities, contributed to abuses by authorities, political parties and private actors, enabling the deployment of illegal and deceptive online political campaigns. The OSCE ODIHR report (2022) highlighted practices of unlawful collection and misuse of personal data online. Such failures undermine the EU's values and principles concerning elections, the rule of law and democracy.

Human Rights Watch (HRW) documented the use of sensitive personal data by the political party Fidesz and the Hungarian Government to conduct targeted political campaigns during the election. According to HRW (2022), 'Evidence indicates that the government of Hungary has collaborated with the ruling party in the way it has used personal data in political campaigns.'

The lack of institutional independence in Hungary—particularly within the electoral authorities and data protection bodies—entailed privacy concerns (HRW 2022). The Civil Liberties Union for Europe (2022) expressed a similar concern: 'where independent institutions are captured by the governing party, an EU-level enforcement mechanism is of key importance. It is unlikely that national watchdogs would enforce the regulation in a neutral, unbiased manner.'

Furthermore, the role of social media in the 2022 election revealed the limitations of GDPR enforcement and the challenges electoral authorities face when monitoring online political campaigns. The Civil Liberties Union for Europe (2022: 17–18) reported that social media platforms played a crucial role in developing personalized online campaigns that violated GDPR principles and rules. Publishers were able to target individuals based on sensitive characteristics—such as gender, sexual orientation or political affiliation—using tools like customer lists, custom audiences and lookalike audiences. However, there was no clear evidence that these campaigns obtained meaningful, free and informed consent from the individuals whose data was used. HRW (2022) made similar remarks, stating that the opaque nature of online platforms allowed political parties to target political advertising with little transparency.

HRW (2024) also reported that the government's control over the media had severely affected journalistic independence and freedom of speech, directly impacting the electoral process. This systematic undermining of media freedom is a direct threat to fundamental rights, particularly those relating to freedom of expression and access to diverse viewpoints in electoral contexts.

The EU's response to Hungary's restrictions on media freedom included invoking mechanisms such as article 7 of the TEU to address systemic breaches of EU values, such as the rule of law, judicial independence and media pluralism.

Hungary's case underscores the intersection of digital policy and electoral integrity, where control over the media—both traditional and online—poses significant risks to fair elections.

Box 2.2. **Hungary's 2022 parliamentary election (cont.)**

The lessons from Hungary's 2022 election reinforce the critical need for a strong and independent regulatory framework to enforce data protection rules in electoral contexts. Such a framework should include the following measures:

- strict enforcement of GDPR principles and rules regarding the processing and transfer of personal data among public authorities;
- enhanced enforcement of GDPR provisions related to the use of sensitive personal data in online political campaigns; and
- stronger interagency collaboration between data protection authorities and electoral authorities to demand greater transparency and accountability from online platforms, which play a significant role in modern electoral campaigns.

Whether based on a legal obligation, consent or public interest, electoral authorities and other actors must ensure that the use, collection and processing of personal data comply with the GDPR. As the CJEU has stated, actors involved in the collection and processing of personal data qualify as 'controllers' and therefore have obligations under data protection law.[6] If a legal entity processes personal data only on behalf of and as instructed by the controller, it also falls under the GDPR. For instance, if an EMB asks a private company to prepare a biometric voter registration list, the processing of this biometric data by the electoral authority and the company must comply with the GDPR.

Compliance with GDPR standards touches upon the principles mentioned above—data minimization and purpose limitation, accountability, transparency, security and confidentiality, among others. These requirements mean that electoral authorities must put in place appropriate measures to mitigate data protection risks and implement privacy-by-design tools in the context of elections.

For instance, the GDPR states that, where processing is likely to result in a high risk to the rights and freedoms of individuals, controllers must carry out a prior assessment of the impact of the envisaged processing operation on the protection of personal data. Article 35 of the GDPR refers to this as a 'data protection impact assessment'. These assessments should examine the specific impact of the intended processing on a data subject's rights and determine whether

6 Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388, paragraph 26.

the processing operation fulfils the proportionality test and complies with the above-mentioned principles.

Taking the same example of implementing a biometric voter registration list, a data protection impact assessment should comply with the above-mentioned principles and ask questions such as the following: Is this necessary for the performance of an election-related task (principle of necessity)? Is biometric data being processed fairly (principle of fairness)? Are data subjects informed about how their data is being used (principle of transparency)? Is the purpose of processing biometric data sufficiently specific and clear (principle of purpose limitation)? Is the processing of biometric data necessary, and could it not be reasonably fulfilled by other means (principle of storage and data minimization)? (For further details, see 3.3: Data processing by electoral management bodies.)

In a democratic society, cybersecurity involves protecting the integrity of elections and 'ensuring the transparent operation of a governance or election system'.

2.2. **CYBERSECURITY IN ELECTIONS**

Electoral authorities, in cooperation with other relevant institutions, are responsible for managing and mitigating risks—including cyberthreats—involved in organizing elections. In a democratic society, cybersecurity involves protecting the integrity of elections and 'ensuring the transparent operation of a governance or election system' (European Union Agency for Cybersecurity 2019: 4). Cyberthreats, such as attacks against the confidentiality, integrity and availability of election-related data or technologies during elections, could undermine electoral integrity (van der Staak and Wolf 2019).

Similarly, while often associated with disinformation, foreign information manipulation and interference (FIMI) also encompasses cybersecurity threats and cyberattacks targeting critical electoral infrastructure. Tactics, techniques and procedures used to exploit vulnerabilities highlight the need for a comprehensive approach to safeguarding election integrity. Hybrid threats such as FIMI, disinformation on social media, AI and deepfakes might also affect the integrity of electoral processes.

In the EU context, cybersecurity relates to protecting the integrity, availability and confidentiality of electoral processes based on an all-hazards, comprehensive and integrated approach. Although the organization of elections falls strictly within the competence of member states, the EU has developed several initiatives to address cyberthreats. Given the widespread use of digital technologies to

support electoral processes, the promotion of cybersecurity across the EU plays an important role in safeguarding elections.

The NIS Cooperation Group, a collective effort of EU member states, the European Commission and the European Union Agency for Cybersecurity (ENISA), highlights the need for vigilance around elections because election technologies could be affected by 'cyberattacks, system failures, human errors, natural disasters and similar contingencies such as power cuts and network outages' (NIS Cooperation Group 2024: 4–5). This all-hazards approach has been outlined in a compendium on election cybersecurity written by the NIS Cooperation Group, which maps the main cyberthreats across the entire electoral cycle, including those targeting external actors such as political parties and politicians.

Given that human factors may impact cybersecurity during elections, EU initiatives have called for cooperation and knowledge sharing on online disinformation and hybrid threats such as FIMI. For instance, the European Cooperation Network on Elections has called for an exchange of information and good practices among member state networks to assess risks and identify cyberthreats and other incidents that could affect the integrity of elections (European Cooperation Network on Elections n.d.: 2). Similarly, the European Commission (2023: paragraph 20) has called for ensuring closer 'cooperation between public and private entities involved in the cybersecurity of elections' and for raising awareness of cyber hygiene among political parties, candidates, election officials and other entities related to elections.

EU initiatives have called for cooperation and knowledge sharing on online disinformation and hybrid threats such as FIMI.

Platforms for cooperation are particularly important due to the limited competences that the EU has on electoral issues, as these remain primarily with the member states. This division of responsibilities is grounded in articles 4 and 5 of the TEU, which provide that competences not conferred on the Union remain with the member states. As a result, electoral matters fall largely within the national domain, limiting the EU's ability to legislate directly. Within the scope permitted by the Treaties, however, the EU plays a complementary role—facilitating coordination, supporting voluntary cooperation and encouraging the exchange of good practices through platforms that promote mutual learning and policy dialogue.

Examples of interagency cooperation include collaboration between the European Cooperation Network on Elections and the NIS Cooperation Group. Other initiatives to strengthen the resilience of electoral processes against cyberthreats include EU-CyCLONe

(European Cyber Crisis Liaison Organisation Network), a cooperation network for the national authorities of member states responsible for cyber crisis management. Additional expertise across the EU could also help to tackle cyberthreats during elections through bodies such as the European Data Protection Board (EDPB), the European Union Agency for Cybersecurity, the Emergency Response Coordination Centre, Europol and networks of audiovisual regulators, among others (European Cooperation Network on Elections n.d.).

2.3. **PLATFORM REGULATION IN EUROPE: AN OVERVIEW**

Box 2.3. **What is the DSA, and what are its main goals?**

The DSA is an EU regulation adopted in 2022 that sets the legal standards for online content within the EU. The DSA plays a critical role in protecting democracy and electoral integrity by regulating the liability and responsibilities of online platforms and digital services. Through a set of fundamental principles and rules, it regulates the publication and distribution of online content by intermediary services such as online platforms (e.g. Facebook, Instagram or YouTube). It seeks to ensure that digital platforms operate transparently and responsibly while aligning with the fundamental rights outlined in the EU Treaties and the Charter.

The European Parliament highlighted the importance of upholding the values enshrined in article 2 of the TEU and emphasizes that fundamental rights—such as the protection of privacy and personal data, the principle of non-discrimination, and freedom of expression and information—must be ingrained at the core of a successful and durable EU policy on digital services (European Parliament 2020).

The DSA is primarily based on article 114 of the TFEU, which empowers the EU to adopt measures for the approximation of national laws that directly affect the establishment and functioning of the internal market. This legal basis enables the DSA to harmonize divergent national rules governing intermediary services—particularly in areas such as content moderation, online disinformation and illegal content—thereby ensuring the free movement of digital services across member states and preserving the integrity of the internal market.

Information integrity during elections is crucial for electoral processes, particularly in how (electoral) information flows in online contexts. In the EU, various legislative measures address this issue, notably the DSA (European Union 2022).

The DSA is a comprehensive legal framework designed to enhance transparency and digital safety by addressing the liability and accountability of various digital service providers, especially for digital platforms with more than 45 million users, including both search engines and social media platforms such as Facebook, Instagram and YouTube. On the one hand, the DSA aims to ensure fairness, trust and safety in the digital environment through a horizontal regulation that coexists with other specific legislation. On the other hand, the DSA stipulates obligations for digital service providers in order to prevent the dissemination of illegal or harmful content in online spaces, thus protecting the fundamental rights of citizens, the rule of law and democratic values.

Regulating content through the moderation decisions of private platforms falls within the field of fundamental rights and democratic issues. The power of digital service providers (private actors) to decide what content should remain online touches on constitutional matters concerning the regulation of freedom of expression and political speech. Under the DSA, 'responsible and diligent behaviour by providers of intermediary services [is] essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights, in particular the freedom of expression and of information' (recital 3 of the DSA). Thus, the EU faces a complex challenge when it comes to regulating online platforms in order to protect, promote and reinforce the fundamental rights enshrined in the Charter as well as European values.

Although the DSA is the most important European legislation for addressing online harms, other EU laws also regulate information flow during elections. Rather than examining each piece of legislation individually, this section focuses on the principles and general rules governing content moderation in online spaces in order to safeguard fundamental rights and protect electoral integrity.

2.3.1. **Challenges with online content moderation: The DSA and EU principles**

The DSA follows three overarching principles developed during the 2000s by the Electronic Commerce Directive and the jurisprudence of the CJEU (Madiega 2022: 2):

1. *Country-of-origin principle (recital 38 of the DSA)*. Online service providers must comply with the law of the member states in which they are legally established.

2. *Limited liability regime (article 9 of the DSA)*. Online intermediaries are exempt from liability for the content they convey and host (users' content) unless they have 'actual knowledge' (article 6 of the DSA) of illegal content or activity occurring on their platforms.

3. *Prohibition of general monitoring (article 8 of the DSA)*. Member states should refrain from imposing on online intermediaries a general obligation to monitor the information available through those online intermediaries.

These principles ensure that platforms are generally not liable for illegal activity or illegal content posted by users (limited liability principle). Additionally, they uphold users' freedom of expression in online contexts, preventing private online platforms from monitoring and controlling content creation.

To give effect to these principles, the DSA takes a procedural approach. Rather than aiming to censor or determine which specific illegal content should remain online, it establishes specific procedures for identifying illegal or harmful content. This approach has been described as the 'proceduralisation of intermediary responsibility' (Busch and Mak 2021). Consequently, in line with the country-of-origin principle, member states have the freedom to define and regulate illegal content without hindering the implementation of the DSA's core principles and rules. For example, electoral laws regulating online political campaigns can be aligned with the DSA framework and its approach to content moderation in the digital sphere.

The DSA adopts a layered approach, where obligations vary based on the type, impact and size of online intermediary services, which are categorized into three groups:

1. *Mere conduits*. These are services that transmit information in a communication network (e.g. Internet access providers, DNS authorities, messaging apps).

2. *Catching services*. These are services that provide automatic, intermediate and temporary storage of third-party information, such as content delivery networks.

3. *Hosting services*. These are services that store information at the request of third parties—for example, search engines, social networks, content-sharing services, trading platforms, discussion

forums, cloud services and app stores. This category includes both online platforms and very large online platforms.

In order to understand the interplay between the safety of online speech and electoral integrity, this report focuses mostly on very large online platforms (VLOPs) and very large online search engines (VLOSEs)—online intermediaries hosting services with more than 45 million monthly active recipients (users). These online services pose special risks when it comes to the dissemination of disinformation and illegal content. Examples of such services include online intermediaries such as Google (VLOSE), LinkedIn (VLOP), Facebook (VLOP), Instagram (VLOP), etc.

One of the DSA's main goals is to address the dissemination of illegal content online and the societal risks posed by disinformation. To this end, intermediary services must include in their terms and conditions information about any restrictions they might impose in relation to the use of their services (article 14.1 DSA), such as content moderation policies, procedures, measures and automated tools (algorithms) used to implement and monitor their terms and conditions. For instance, Facebook's terms and conditions prohibit the posting of nudity, and any nude content is filtered or removed by its algorithmic tools, as permitted by the DSA.

One of the DSA's main goals is to address the dissemination of illegal content online and the societal risks posed by disinformation.

Any restrictions should pay due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the users, such as the freedom of expression, media freedom and pluralism, and other fundamental rights enshrined in the Charter.

Furthermore, the DSA mandates that all providers of hosting services and online platforms, regardless of their size, must implement notice-and-action mechanisms (article 16 DSA) that allow users to report specific pieces of information that may be considered illegal content. In other words, users must have the right to notify an online platform (e.g. Facebook) in a simple and user-friendly manner about illegal content (e.g. non-consensual sharing of intimate or manipulated material). These mechanisms must comply with the requirement to provide a statement of reasoning (article 17 DSA) and with other specific rules to protect the rights and legitimate interests of all affected parties, particularly their fundamental rights guaranteed in the Charter.

Users must have the right to notify an online platform (e.g. Facebook) in a simple and user-friendly manner about illegal content.

2.3.2. **Content moderation addressing online gender-based violence**

The same DSA principles and rules apply to the EU Directive on Combating Violence against Women and Domestic Violence (European Union 2024c), particularly regarding orders and other measures requiring the removal of or disabling of access to material that may depict online gender-based violence. The removal or restriction of access to such material, when it constitutes a criminal offence, should be carried out in a transparent manner and with adequate safeguards. The relevant criminal offences include the following:

- non-consensual sharing of intimate or manipulated material (article 5), which includes deepfakes that alter audiovisual material to make it appear as if a person is engaged in sexually explicit activities without that person's consent;

- cyber harassment (article 7), which involves engaging in publicly accessible threatening or insulting conduct that causes serious psychological harm to a person, or making a person's personal data publicly accessible without that person's consent; and

- cyber incitement to violence or hatred (article 8), such as inciting violence or hatred against a group of persons or a member of such a group, defined by reference to gender, by publicly disseminating such content by means of ICTs.

In the context of electoral processes, these offences are regarded as aggravating circumstances wherever an offence is committed by abusing a recognized position of trust, authority or influence (article 11[m] of the Directive) or if an offence is committed against a person because that person is a public representative (for instance, women politicians).

In the context of this Directive, the 'competent authorities' who are empowered to order the removal or disabling of harmful material are those designated under national law as competent to carry out the duties provided for in this Directive (recital 14). Accordingly, only national electoral law can confer on electoral authorities the power to order the removal or disabling of access to the above-mentioned harmful material in the context of electoral processes.

2.3.3. **The role of media in electoral democratic processes: Moderating online media content**

An exception to the general rules on content moderation in the EU concerns how online media content is moderated by VLOPs under the EMFA (European Union 2024b). The EMFA is a vertical regulation that should be applied directly to member states alongside the DSA. According to article 18(4), a VLOP may not suspend or restrict the visibility of content from a self-declared media service provider (such as *The Guardian*, *The New York Times* or France 24) except by following a special procedure outlined in the regulation. This rule acknowledges the importance of press freedom, media plurality and journalism as essential democratic institutions that guarantee citizens access to reliable news.

These fundamental rights apply even more in electoral contexts. For this reason, the EU legislator believes that self-declared media service providers should not be unilaterally silenced by VLOPs based exclusively on their terms and conditions or other specific legal grounds (Nenadić and Brodgi 2023).

Before a VLOP restricts or suspends content that might contain disinformation under its terms and conditions, it must provide a statement explaining the decision and give the media service provider 24 hours to respond. During this period, the VLOP may neither remove nor restrict the content.

It is important to highlight that this provision does not apply to illegal content pursuant to EU law such as hate speech or non-consensual intimate or manipulated material. Thus, specific illegal content posted by media service providers is subject to DSA rules and the terms and conditions of online platforms. VLOPs should follow article 9 of the DSA and remove illegal content based on orders issued by the relevant judicial or administrative authorities, put in place notice-and-action mechanisms, inform competent national enforcement or judicial authorities if they become aware of a criminal offence on their platforms, and suspend users who misuse their services by providing manifestly illegal content (article 23 and recital 62 of the DSA). Finally, VLOPs should also follow the risk assessment and mitigation risk obligations to protect against illegal content (Nenadić and Brodgi 2023).

Specific illegal content posted by media service providers is subject to DSA rules and the terms and conditions of online platforms.

Box 2.4. **The EMFA in brief: Ensuring a free and fair media landscape in the EU**

The EMFA reinforces the protection of media pluralism, editorial independence and the safety of journalists. Anchored in the principles of democracy, the rule of law and fundamental rights, the EMFA builds upon article 11 of the Charter, which guarantees freedom of expression and information, as well as article 2 of the TEU, which enshrines democracy as a core EU value.

The EMFA complements existing EU legislation, such as the DSA and GDPR, by addressing challenges posed by increasing digitalization, political interference and economic pressures on media independence. By setting clear safeguards against the misuse of surveillance tools, undue state influence and opaque ownership structures, the EMFA ensures that journalism remains free from interference and that citizens have access to reliable, diverse and independent information.

By preventing political and economic pressures on media outlets, strengthening safeguards against spyware abuses, and enhancing transparency in media ownership and funding, the EMFA upholds press freedom as an essential pillar of democracy. In conjunction with the DSA and the GDPR, the EMFA contributes to a resilient and fair digital information ecosystem, ensuring that fundamental rights remain protected in an increasingly digitalized media landscape.

2.3.4. **Due diligence obligations under the DSA: Risk assessment and mitigation measures**

As mentioned earlier, the DSA establishes a layered set of obligations based on the type, impact and size of online intermediaries. VLOPs and VLOSEs represent the largest category of online intermediaries and are therefore subject to special obligations. These corporations and their obligations fall under the competence of the European Commission.

One of the most important obligations for VLOPs and VLOSEs is to diligently identify, analyse and assess any systemic risks arising from the design or functioning of their services, including algorithmic systems, as specified in article 34 of the DSA. In other words, platforms must conduct their own assessments of systemic risks, which include the following:

- the dissemination of illegal content through their services;
- any actual or foreseeable negative effects for the exercise of fundamental rights, including freedom of expression, media pluralism, and the right to vote and to stand as a candidate at elections;

- any actual or foreseeable negative effect on civic discourse and electoral processes; and

- any actual or foreseeable negative effects in relation to gender-based violence.

The identification of these systemic risks will entail putting in place reasonable, proportionate and effective mitigation measures, set out in reports that identify and assess the most prominent and recurring risks. In addition, these reports should include best practices for VLOPs and VLOSEs to mitigate these systemic risks. The reports must be broken down by member state and, upon request, submitted to the relevant digital services coordinator as well as the European Commission (article 34[3] DSA).

Some of the actual and foreseeable risks include a lack of diversity and meaningful sources in online contexts, manipulation through micro- and nanotargeting techniques, misidentification of political advertising, radicalization and polarization of online spaces, disinformation, the spread of hate speech, and censorship by politicians or political candidates, among other things (Reich and Calabrese 2025).

The identification of these systemic risks will entail putting in place reasonable, proportionate and effective mitigation measures.

Box 2.5. **The DSA as a safeguard for electoral integrity: The case of Romania**

On 24 November 2024 the far-right extremist candidate Călin Georgescu received the most votes in the first round of the Romanian presidential election. Despite running with no campaign budget, he secured almost 23 per cent of the vote (around 2 million votes) by campaigning almost exclusively online, mainly on TikTok.

Other presidential candidates subsequently filed judicial complaints. In addition, several reports from Romania's intelligence agencies documented the use of voter manipulation techniques via social media platforms, cyberattacks, Russian electoral interference and illegal online practices. On 6 December 2024, taking these elements into consideration, the Constitutional Court of Romania decided to annul the elections ex officio.

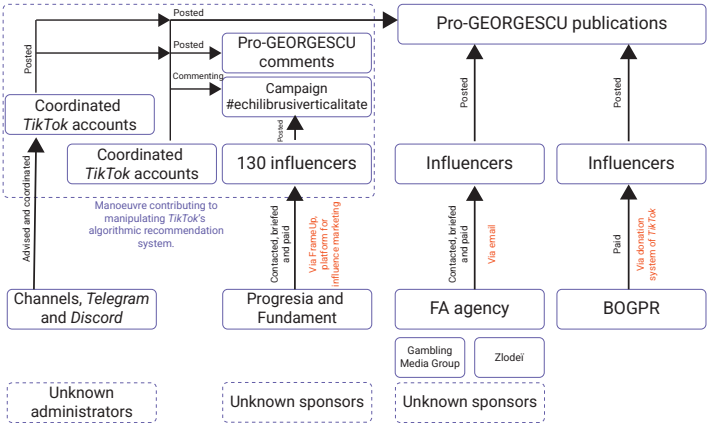
Multiple irregularities exposed by several authorities revealed manipulation of the vote and violations of the principles of transparency and of the free and fair conduct of elections, including the non-transparent use of digital technologies and AI in the campaign, as well as the financing of the campaign from undeclared sources, both in violation of electoral legislation and undermining the principle of equal opportunity among electoral competitors (Venice Commission 2025). Ultimately, these breaches 'distorted the free and fair nature of the vote, compromised electoral transparency, and disregarded legal provisions on campaign financing' (Barata and Lazăr 2025).

Regarding the alleged manipulation of voting through social media, the European Digital Media Observatory reported that the number of followers on Georgescu's account tripled between 10 and 24 November 2024 (Botan 2024). An astroturfing campaign, coordinated through thousands of TikTok accounts and a network of paid influencers, exploited TikTok's recommender systems to artificially boost the visibility of Georgescu's messages. Nevertheless, the presidential candidate declared no expenses at all (Cornea 2025). As a result of this online strategy, hashtags related to Georgescu's campaign reached ninth place in TikTok's global ranking (VIGINUM 2025: 7).

All these mechanisms to artificially increase the visibility of TikTok accounts are prohibited under the platform's terms and conditions. However, the campaign's use of bots and influencers to exploit the algorithms is not illegal under either the DSA or the TTPA (for an overview of the manoeuvres taken by the candidate, see Figure 2.1).

Box 2.5. **The DSA as a safeguard for electoral integrity: The case of Romania (cont.)**

Figure 2.1. **Pro-Georgescu online campaign scheme made by VIGINUM**



Source: VIGINUM, 'Manipulation d'algorithmes et instrumentalisation d'influenceurs : Enseignements de l'élection présidentielle en Roumanie & risques pour la France' [Manipulation of Algorithms and Instrumentalization of Influencers: Lessons from the Presidential Election in Romania and Risks for France], February 2025, <https://www.sgdsn.gouv.fr/files/files/Publications/20250204_NP_SGDSN_VIGINUM_Rapport_public_Elections_roumanie_risques_france_VFF.pdf>, accessed 16 August 2025.

The European Commission opened a formal proceeding against TikTok under the DSA, requesting information regarding the actions the platform had taken to reduce potential algorithmic bias during the electoral process. In other words, TikTok was asked to provide details on the measures it took regarding the 'management of risks to elections or civic discourse' linked to its recommender systems, notably the risks 'linked to the coordinated inauthentic manipulation or automated exploitation of the service', as well as its policies on political advertisements and paid political content (European Commission 2024e).

This case shows that it is difficult to foresee the type and impact of measures that the European Commission may take against platforms, particularly since it is the companies themselves that decide how to address systemic risks on their platforms in electoral processes. Even though the Commission has issued guidelines on safeguarding online electoral integrity, these measures are not legally binding. Consequently, their implementation differs from one company to another. Moreover, civil society organizations have pointed out that 'the guidelines do not contain benchmarks by which the success or failure of the suggested measures can be evaluated' (Alvarado Rincón 2025). Other experts have highlighted that the case has shown that 'certain forms of (allegedly paid) political messaging became almost impossible to tackle when included as short mentions in long influencer videos mainly focusing on make-up trends' (Barata and Lazăr 2025).

Box 2.5. **The DSA as a safeguard for electoral integrity: The case of Romania (cont.)**

This case illustrates how easily deceptive actors can exploit VLOPs' algorithmic recommender systems to manipulate electoral processes. It also underscores the responsibility of online social media platforms to ensure a safe online environment in the context of elections. Furthermore, it highlights the need for the European Commission to work hand in hand with EMBs and other national actors to monitor such developments in order to prevent breaches of European values, including the conduct of free, fair and transparent elections.

2.4. ONLINE POLITICAL ADVERTISING: TOWARDS HARMONIZED EUROPEAN REGULATION

The DSA treats online political advertising as a form of online advertising and content. This means that online political advertising must comply with both the general rules governing online advertising and the DSA's content moderation rules (e.g. terms and conditions, notice-and-action mechanisms, trusted flaggers, systemic risk assessments, etc.).

Article 3(r) of the DSA defines advertising as:

> information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes and presented by an online platform on its online interface against remuneration specifically for promoting that information.

The two key elements of this definition are as follows:

1. It explicitly includes 'non-commercial purposes' (e.g. political content).
2. It requires that content be promoted 'against remuneration'.

Organic political content could fall under the new European Regulation on the Transparency and Targeting of Political Advertising.

Hence, organic political content (unpaid content and information flows driven by algorithmic recommender systems) does not fall within the scope of online advertising under the DSA.

Conversely, organic political content could fall under the new European regulation, the TTPA (European Union 2024a). The TTPA's definition of political advertising includes content that is 'normally provided for remuneration' (article 3[2]). In other words, unpaid political speech could still fall under this regulation, raising concerns

about potential restrictions on freedom of expression and political speech in online spaces (ARTICLE 19 2023; Heinmaa 2023).

This regulatory overlap may affect the enforcement of the DSA, given the contradictions between the two legal frameworks. It could also create coordination problems among electoral authorities, digital services coordinators and other regulatory bodies (such as media authorities), all of which may have an interest in enforcing the EU's online political advertising regulations (Heinmaa 2023).

As mentioned earlier (see 2.1.5. section), the DSA requires that online advertising provided by VLOPs and VLOSEs must not be displayed based on profiling that uses special categories of personal data (such as political opinion, sexual orientation or ethnic origin). This rule impacts the targeting and ad-delivery techniques that publishers use to identify the most precise audiences for online political advertising. However, the rule has not had the intended impact. Due to the mechanisms used by big tech companies to monitor, extract and collect behavioural data, targeted advertising that does not rely on profiling or does not use special categories of data in the context of profiling may still be allowed (Duivenvoorde and Goanta 2023: 9–10).

Targeting and ad-delivery techniques involve the collection of personal data, including observed and inferred data (but not sensitive data), which may nonetheless reveal sensitive aspects concerning citizens (Becker Castellaro and Penfrat 2022). Moreover, under both the DSA and the TTPA, as well as the Code of Conduct on Disinformation, the explicit consent of a data subject to process their personal data specifically for the purpose of political advertising creates an exception to this prohibition (European Commission 2025c).

Several civil society organizations, along with the European Data Protection Board, the Committee on the Internal Market and Consumer Protection of the European Parliament (2023) and Juneja (2024), have recommended a total ban on microtargeting techniques that use special categories of sensitive data for political purposes. This recommendation aims to mitigate the risks of polarization, the creation of echo chambers and the spread of disinformation associated with targeting and ad-delivery techniques (Becker Castellaro and Penfrat 2022).

However, this prohibition has not been incorporated into either the DSA or the TTPA.

Box 2.6. **Regulation on the transparency and targeting of political advertising: Ensuring fair and transparent digital political campaigning in the EU**

Grounded in article 7 (respect for private and family life), article 8 (protection of personal data) and article 11 (freedom of expression and information) of the Charter, as well as article 2 of the TEU, which enshrines democracy as a core EU value, the TTPA aims to prevent manipulation, ensure transparency and safeguard electoral integrity in the digital age (European Commission n.d.a).

In line with article 16 of the TFEU, which guarantees the protection of personal data, and article 8 of the Charter, which enshrines data protection as a fundamental right, the TTPA complements the GDPR by limiting the unlawful use of personal data in political advertising. It establishes safeguards against the exploitation of sensitive data, the misuse of AI-driven microtargeting techniques and opaque algorithmic amplification of political messages.

Furthermore, the TTPA complements the DSA by imposing stricter accountability measures on online platforms and ad providers, ensuring that political ads are clearly labelled, traceable and accessible for public scrutiny. This regulatory approach prevents undue influence in democratic processes, strengthens electoral integrity and enhances transparency in digital political campaigning.

By combating disinformation, preventing data-driven voter manipulation and ensuring fairness in digital political discourse, the TTPA helps safeguard democratic principles and fundamental rights in the digital era (Rabitsch and Calabrese 2024: 7).

Transparency and reliable data on online political advertising are crucial for evaluating the accountability of online platforms in their fight against disinformation.

2.4.1. **Transparency on political advertising**

Transparency and reliable data on online political advertising are crucial for evaluating the accountability of online platforms in their fight against disinformation. Some transparency requirements are already included in the DSA and the Code of Conduct on Disinformation, including user-facing transparency commitments, ad repositories, engagement with civil society organizations, and monitoring and research based on online platform data (European Commission 2025c).

Various regulations in the European legal framework, including the Code of Conduct on Disinformation, serve as legal sources of measures and obligations for ensuring transparency in online political advertising. The objective of all these legislative instruments is to enable citizens to easily recognize political advertising.

Among these legal sources, the TTPA is the most important regulation for understanding the transparency measures that online

platforms must implement regarding online political advertising. Under article 8 of the TTPA, the identification of a political advertisement should include the following elements: (a) the content of the message; (b) the sponsor of the message; (c) the language used to convey the message; (d) the context in which the message is conveyed, including the period of dissemination; (e) the means by which the message is prepared, placed, promoted, published, delivered or disseminated; (f) the target audience; and (g) the objective of the message.

Based on article 7 of the TTPA, sponsors (e.g. politicians or political parties) must declare whether an advertisement constitutes a political ad, and service providers (e.g. a VLOP or VLOSEs) must request the necessary information to comply with the regulation once such a declaration is made by the sponsor. In other words, the obligation to declare an advertisement as political rests with the sponsors. Civil society organizations have warned, however, that transparency obligations could be circumvented by both sponsors and online platforms if they simply fail to indicate 'that the ads that they are running are political' (Calabrese 2024a: 3).

In addition, the TTPA establishes a European repository for online political advertisements that should be put in place by the European Commission. This public repository is intended to publish all online political advertisements deployed in the European Union. The information should be available in a machine-readable format and publicly accessible via a single portal. The repository should include transparency notices for political advertising, including the following information (article 12[1)] TTPA):

> (a) the identity of the sponsor and, where applicable, of the entity ultimately controlling the sponsor, including their name, email address, and, where made public, their postal address, and, when the sponsor is not a natural person, the address where it has its place of establishment;
>
> (b) the information required under point (a) on the natural or legal person that provides remuneration in exchange for the political advertisement if this person is different from the sponsor or the entity ultimately controlling the sponsor;
>
> (c) the period during which the political advertisement is intended to be published, delivered or disseminated;
>
> (d) the aggregated amounts and the aggregated value of other benefits received by the providers of political advertising services, including those received by the publisher in part or full exchange for the political advertising

services, and, where relevant, of the political advertising campaign;

(e) information on public or private origin of the amounts and other benefits referred to in point (d) as well as whether they originate from inside or outside the Union;

(f) the methodology used for the calculation of the amounts and value referred to in point (d);

(g) where applicable, an indication of elections or referendums and legislative or regulatory processes with which the political advertisement is linked;

(h) where the political advertisement is linked to specific elections or referendums, links to official information about the modalities for participation in the election or referendum concerned;

(i) where applicable, links to the European repository for online political advertisements referred to in Article 13;

(j) information on the mechanisms referred to in Article 15(1);

(k) where applicable, whether a previous publication of the political advertisement or of an earlier version of it has been suspended or discontinued due to an infringement of this Regulation;

(l) where applicable, a statement to the effect that the political advertisement has been subject to targeting techniques or ad-delivery techniques on the basis of the use of personal data, including information specified in Article 19(1), points (c) and (e);

(m) where applicable and technically feasible, the reach of the political advertisement in terms of the number of views and of engagements with the political advertisement.

The TTPA establishes specific functions for electoral authorities to ensure compliance. According to article 16, electoral authorities ('national competent authorities') may request that providers of political advertising services (such as VLOPs and VLOSEs) transmit any required information mentioned above. The deadline for complying with these rules range from 2 to 12 days, depending on the size of the company involved. In the last month preceding an election or a referendum, providers of political advertising services must provide the requested information within 48 hours.

Each provider of political advertising services, including VLOPs and VLOSEs, must designate a contact point for communication with the competent national authorities.

In addition, each provider of political advertising services, including VLOPs and VLOSEs, must designate a contact point for communication with the competent national authorities. The above-

mentioned data could also be shared with vetted researchers, civil society organizations, political actors, national or international observers and journalists.

2.4.2. **Data access for researchers: DSA and TTPA examples**

The DSA covers third-party scrutiny and research (data access). According to the European Commission (2024c), 'Stable and reliable data access for third-party scrutiny is of utmost importance during electoral periods to ensure transparency, advance insights and contribute to the further development of risk mitigation measures around elections.' In addition to their legal obligations under article 40 of the DSA, the Commission recommends that VLOPs and VLOSEs provide free access to data to study risks related to electoral processes, including scrutinizing AI models, visual dashboards and other additional data points.

Data access is essential for establishing checks and balances on how online platforms comply with the DSA and the TTPA and, ultimately, in combating illegal content and disinformation. Such access permits vetted researchers to assess systemic risks to electoral processes and civic discourse (such as FIMI, disinformation and the spread of hate speech, among other things) and to develop evidence-based online policies to mitigate those risks (see 3.4.1: The role of EMBs in risk assessment and mitigation under the DSA: Due diligence obligations of VLOPs and VLOSEs in electoral processes).

Furthermore, member states must designate a national competent authority responsible for keeping publicly available and machine-readable online registers of all legal representatives registered on their territory under the TTPA. Each national competent authority is required to ensure that such information is easily accessible and that it is complete and regularly updated (article 22 TTPA). The TTPA establishes a closed list of powers, granting national competent authorities the power to do the following:

> (a) request access to data, documents or any necessary information, in particular from the sponsor or the providers of political advertising services concerned, which the competent authorities are to use only for the purpose of monitoring and assessing compliance with this Regulation, in accordance with relevant legislation on the protection of personal data and the protection of confidential information;
>
> (b) issue warnings addressed to the providers of political advertising services regarding their non-compliance with the obligations under this Regulation;

(c) order the cessation of infringements and require sponsors or providers of political advertising services to take the steps necessary to comply with this Regulation;

(d) impose or request the imposition by a judicial authority of fines or financial penalties or other financial measures as appropriate;

(e) where appropriate, impose a periodic penalty payment, or request a judicial authority in their Member State to do so;

(f) where appropriate, impose remedies that are proportionate to the infringement and necessary to bring it effectively to an end or request a judicial authority in their Member State to do so;

(g) publish a statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Regulation and the nature of that infringement;

(h) carry out, or request a judicial authority to order or authorise, inspections of any premises that providers of political advertising services use for purposes related to their trade, business, craft or profession, or request other public authorities to do so, in order to examine, seize, take or obtain copies or extracts of information in any form, irrespective of the storage medium.

The TTPA emphasizes the importance of holding a 'regular exchange of information' among the national contacts designated by member states.

The TTPA also emphasizes the importance of holding a 'regular exchange of information' among the national contacts designated by member states, along with sharing best practices and promoting cooperation between national authorities and the European Commission in all aspects of its implementation. This cooperation should include collaboration with the European Cooperation Network on Elections, the European Regulators Group for Audiovisual Media Services, and other relevant networks or bodies. Additionally, national authorities may also cooperate with other national stakeholders to support implementation and compliance with the TTPA.

Although electoral authorities play a role in communicating with and requesting information from online platforms regarding repositories of political advertising, the relevant digital services coordinator or the European Commission (depending on whether or not the platforms are designated as VLOPs or VLOSEs) is the competent authority responsible for supervising online intermediaries' compliance with transparency obligations. Furthermore, the digital services coordinator is tasked with ensuring coordination at the national level for implementing transparency measures.

Box 2.7. **The European Democracy Shield**

In response to mounting systemic threats to democratic processes, the European Commission unveiled the European Democracy Shield (EDS) to address 'the evolving nature of threats to [European] democracy and electoral processes' (European Parliament 2025). At the time of writing, the European Democracy Shield remains under preparation, with its final form and content expected to be unveiled by late November 2025. Launched shortly before elections to the European Parliament in 2024, the EDS builds on the European Democracy Action Plan of 2020 (European Commission 2024d) but goes one step further: it provides a comprehensive protection package aimed at strengthening the EU's democratic and societal resilience, with a particular focus on information and electoral integrity.

Taking a holistic approach, the EU has made it a priority to shield its democracy from FIMI and hybrid threats. To achieve this goal, the EDS builds on the strong implementation and enforcement of key legislative instruments introduced over recent years, such as the DSA, the EMFA, the AI Act, the proposed EU regulation on strategic lawsuits against public participation (SLAPPs) and the TTPA. Furthermore, the EDS aims to boost its efforts in digital and media literacy, integrating the expertise of civil society actors, democracy-focused civil society organizations and disinformation researchers.

As part of its efforts to shield Europe from foreign interference, the EDS additionally foresees more extensive coordination among institutions. Alongside civil society and other national and European bodies that will be involved in shaping and implementing the EDS, the European Commission created the Project Group on Democracy, chaired by Commissioner Michael McGrath (Democracy, Justice, Rule of Law and Consumer Protection) and Commissioner Henna Virkkunen (Executive Vice-President for Tech Sovereignty, Security and Democracy). The Group's purpose is to foster coordination and align efforts across various strategic areas.

The European Parliament established the Special Committee on the European Democracy Shield on 18 December 2024. The Committee's responsibilities include, among other things, assessing 'relevant existing and planned legislation and policies to further detect possible loopholes, gaps and overlaps that could be exploited for malicious interference in democratic processes' (European Parliament 2024), developing recommendations and maintaining relations with EU institutions and other relevant societal and non-state partners.

2.5. **AI AND ITS IMPACT ON ELECTORAL INTEGRITY**

The EU AI Act (European Union 2024d) is a regulation with a horizontal scope, applicable to AI systems placed on the European market. A general exemption applies to AI systems used for national security. Its objective is to ensure that such systems are implemented in a safe, transparent manner that respects fundamental rights. The regulation follows a risk-based approach, categorizing AI systems according to the level of risk they pose to both society and individuals' rights.

The AI Act seeks to uphold the EU's core values of democracy and respect for fundamental rights (Bogucki et al. 2022). It establishes a regulatory framework that addresses the potential risks posed by AI systems to electoral integrity, ensuring that technological advancements do not compromise the democratic process.

The regulation distinguishes between different categories of operators involved with AI systems—providers, deployers, importers, distributors and product manufacturers. Electoral authorities may fall into one or more of these categories.

According to article 3(3) of the AI Act, providers are natural or legal persons, public authorities, agencies or other bodies that develop AI systems, or have them developed, and place them on the Union market or put them into service under their own name or trademark. Deployers are natural or legal persons, public authorities, agencies or other bodies that use AI systems under their authority unless the use is for personal, non-professional purposes.

The AI Act has a regulatory impact on the use of AI systems in the context of elections. Its aim is to promote human-centric and trustworthy AI while protecting fundamental rights such as the right to vote, participation in elections, democracy and the rule of law. The risk-based approach varies depending on the level of risk AI systems pose to health, safety and fundamental rights. This risk-based classification includes the following four categories:

1. *Unacceptable risk*. These are AI systems that pose a clear threat to important Union public interests that are protected by Union law (e.g. social scoring or manipulative AI). Since they cannot be developed, sold or used in the EU, these AI systems are prohibited under article 5 of the AI Act.

2. High risk (article 6 AI Act). These AI systems are permitted but subject to requirements and ex ante conformity assessments, such as risk assessment and mitigation measures.

3. Limited risk (recital 53 AI Act). These AI systems are subject to specific transparency obligations.

4. Minimal risk. These AI systems are largely unregulated.

In the context of elections, some AI systems are prohibited by law, including those that employ subliminal manipulation to distort a person's behaviour and are likely to cause significant harm, as well as AI systems that exploit vulnerabilities or use biometric categorization to infer people's race, political opinions, religious or philosophical beliefs, among other things.

However, civil society organizations have raised concerns about the harm-based approach to prohibited AI systems. For instance, the European Partnership for Democracy argues that 'it is very difficult to prove the existence of significant harm in the context of elections, to measure it as "significant", and to demonstrate how likely it is that a certain AI system causes a certain harm' (Calabrese 2024b: 3). For example, AI systems that incidentally hallucinate or generate false or misleading information will not fall into this category because they are not considered 'deceptive techniques' and therefore would not be prohibited under the AI Act (European Commission 2025b: 29).

Certain AI systems used in the administration of justice and democratic processes are categorized as high risk. Annex III, point 8(b) of the AI Act specifically mentions these AI systems in the context of elections:

> AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems to the output of which natural persons are not directly exposed, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view.

This category is limited to the intended potential outcomes that these systems may entail. For instance, AI systems such as microtargeting and amplification techniques, which may be considered 'intended to be used to influence elections', should be linked directly to the outcome of the elections. By contrast, organizational AI systems,

such as voter registration and identification tools, voter list management and election cost forecasting, among others, do not fall within this category. Again, intentionality is a critical element to consider here (Calabrese 2024b).

For example, institutional chatbots designed to inform citizens about elections could potentially provide manipulative information that influences voting behaviour. However, such chatbots may be classified as organizational systems and therefore not be subject to risk assessments, mitigation measures or registration in a public EU database.

Nevertheless, when these systems are created specifically to influence elections or referendums or individuals' voting behaviour (such as through microtargeting and amplification techniques) and are deployed by bodies governed by public law or by private entities providing public services, they must undergo a fundamental rights impact assessment. In doing so, deployers should identify the potential impact on fundamental rights. However, the assessment process does not involve consultations with external stakeholders.

Deployers of systems that generate or manipulate image, audio or video content (e.g. deepfakes) must disclose that the content has been artificially generated or manipulated.

On a different note, the AI Act also regulates AI-generated synthetic audio, image, video and text content. Systems that generate such content must ensure that outputs are marked in a machine-readable format and are detectable as artificially generated or manipulated. Deployers of systems that generate or manipulate image, audio or video content (e.g. deepfakes) must disclose that the content has been artificially generated or manipulated. In other words, AI-generated content must be labelled as such.

The Act does not explicitly mention deepfakes or gender-based attacks on women politicians in the context of elections. In this context, the EU Directive on Combating Violence against Women and Domestic Violence (European Union 2024c) (see 2.3.2: Content moderation addressing online gender-based violence) provides the most appropriate legal framework for protecting against AI-generated content that contributes to gender-based violence.

Chapter 3

ENFORCEMENT AND LIMITS OF THE EXISTING EU DIGITAL REGULATORY FRAMEWORK

As highlighted in the previous chapter, the EU's digital acquis represents one of the most ambitious regulatory frameworks globally, establishing comprehensive governance systems for digital services, data protection and online content. Central to this framework is the creation of a comprehensive and coherent enforcement architecture designed to provide oversight at the EU level while also having a significant impact at the level of member states.

This chapter aims to clarify the complexities of this enforcement architecture, focusing in particular on its functioning and the interplay between national and EU-level authorities in the context of elections. The goal is to equip policymakers and electoral monitoring bodies with a clear understanding of compliance requirements and enforcement strategies related to these regulations.

Furthermore, the discussion identifies implementation and coordination challenges that are especially pertinent to the electoral context. Drawing on the experiences of European electoral commissions, this chapter provides practical insights and concrete recommendations. It also examines interagency and cross-authority coordination efforts, highlighting effective practices and common hurdles encountered in the enforcement and implementation of digital regulations during elections.

3.1. IMPLEMENTATION OF DATA PROTECTION SAFEGUARDS IN THE CONTEXT OF ELECTIONS

The GDPR established an early model of decentralized enforcement that continues to influence newer digital regulations while also revealing important challenges in cross-border implementation.

The enforcement of the GDPR primarily relies on national supervisory authorities, also referred to as data protection authorities, which monitor and supervise data controllers and processors within their jurisdictions. Furthermore, these authorities are empowered to investigate and sanction GDPR infringements, including those that arise in electoral contexts (European Commission n.d.b).

3.1.1. The European Data Protection Board and the European Data Protection Supervisor

At the EU level, several important mechanisms are in place to ensure consistent data protection standards at both European and member state levels. The European Data Protection Board (EDPB), which is composed of the heads of the national data protection authorities, and the European Data Protection Supervisor have legal personality and are responsible for ensuring that the GDPR and the Law Enforcement Directive are applied consistently across Europe (article 68 GDPR). They also ensure cooperation among European and national bodies, including on GDPR enforcement.

The EDPB provides general guidance by issuing guidelines, recommendations and best practices to harmonize EU data protection laws (European Data Protection Board n.d.b). In March 2019, for example, the EDPB released Statement 2/2019 on the use of personal data in political campaigns, warning that modern elections involve extensive use of personal data and profiling by parties and emphasizing that GDPR compliance is crucial for democratic integrity (European Data Protection Board 2019). The EDPB has also responded to specific concerns, such as the controversial plan for all-postal voting in Poland in 2020 (Wanat 2020). The EDPB issued a letter stressing that there had to be a sound legal basis for any transfer or processing of voter data and that such actions had to comply with the GDPR's requirements for security and transparency, highlighting that emergency election-related measures cannot override fundamental data protection principles (European Data Protection Board 2020a).

While national elections are outside its scope, the EDPS has overseen data protection in activities related to European Parliament elections. A prominent example was the EDPS's investigation into the European Parliament's 2019 voter outreach website, which had used a US-based campaign company, NationBuilder. The EDPS found that the Parliament had failed to ensure compliance (notably in transparency and data transfer safeguards) and issued its first-ever reprimand to an EU institution. All data collected through that campaign site was later moved to the Parliament's own servers, and the EDPS secured commitments that EU institutions would 'lead by example' in protecting personal data during elections (European Data Protection Supervisor 2020).

However, since data processing frequently crosses borders, enforcement often becomes transnational and requires coordination between multiple national authorities (Mustert 2023). Therefore, the GDPR established a cooperation mechanism through which national data protection authorities must coordinate enforcement procedures for cross-border cases (Mustert 2023). When needed, the EDPB can step in to resolve disagreements between national authorities, and its decisions are binding (article 65 of the GDPR).

Since data processing frequently crosses borders, enforcement often becomes transnational and requires coordination between multiple national authorities.

In the electoral context, modern campaigns often use online platforms (such as social media and advertising networks) that operate across borders. In such cases, the GDPR's one-stop-shop mechanism may designate a lead data protection authority (e.g. Ireland's Data Protection Commission for Facebook) to handle investigations (European Data Protection Board n.d.b). However, data protection authorities may take urgent measures if waiting for the lead authority would risk undermining an election. During Italy's 2022 general election, for example, the Italian data protection authority (Garante) invoked article 66 of the GDPR to order Meta (Facebook) to halt a new voter engagement feature until concerns about lawfulness and transparency were addressed. Garante coordinated with the Irish Data Protection Commission, but when satisfactory answers were not provided in time, it issued a formal warning and imposed a temporary ban on the feature's use in Italy (GDPR Hub 2023).

In summary, national data protection authorities are on the front line of enforcement during elections, conducting investigations and issuing sanctions within their jurisdictions. At the EU level, the European Commission, the EDPB and the EDPS provide guidance, facilitate cooperation and can intervene in specific cross-border or institutional cases.

3.2. CHALLENGES OF CROSS-BORDER COORDINATION

The complex enforcement mechanism—particularly the multi-level coordination required for cross-border cases—has been criticized for its procedural complexity, which presents significant practical challenges (Gentile and Lynskey 2022; Mustert 2023; Mildebrath 2024). The GDPR establishes a standardized set of tasks and powers for supervisory authorities under articles 57 and 58, yet it leaves numerous procedural steps undefined, allowing significant national discretion. This latitude has led to inconsistent enforcement practices across EU member states, notably regarding the initiation of formal investigations, their scope and the severity of the corrective measures imposed (Gentile and Lynskey 2022; Mustert 2023).

Procedural fragmentation complicates the establishment of clear boundaries between acceptable national variations and practices that undermine EU principles of effectiveness, proportionality and dissuasiveness. For example, national rules limiting the time frame for lodging complaints or fining strategies that significantly diverge from the GDPR's maximum penalties create practical barriers for data subjects seeking to exercise their rights effectively (Gentile and Lynskey 2022: 806–07; Mustert 2023).

Another structural flaw inherent in the GDPR's enforcement architecture is the decentralized enforcement design.

Another structural flaw inherent in the GDPR's enforcement architecture is the decentralized enforcement design, which can complicate cross-border cooperation and create friction and substantial delays (Gentile and Lynskey 2022: 800). This flaw may reduce enforcement to a common minimum standard. Furthermore, institutional imbalances, where the lead supervisory authority can exert disproportionate influence over case outcomes, can diminish the authority of other concerned authorities (Gentile and Lynskey 2022: 809, 811).

Procedural ambiguity also negatively impacts vertical cooperation with the EDPB. The EDPB, lacking independent investigative authority, relies exclusively on national supervisory authorities for comprehensive and timely case information. Delayed or incomplete reporting from national authorities frequently undermines the EDPB's dispute resolution mechanism, further exacerbating delays and inconsistencies in enforcement outcomes (Gentile and Lynskey 2022; Mustert 2023).

The European Parliamentary Research Service also identifies procedural ambiguity and insufficient clarity as critical issues hampering effective GDPR enforcement. Unclear procedural rules can exacerbate discrepancies between supervisory authorities and hinder prompt and uniform decision making in cross-border cases. Thus, it recommends reforms aimed at clarifying procedural obligations, strengthening the role of concerned authorities, and ensuring consistent and timely enforcement decisions across member states (Mildebrath 2024).

Scholars and practitioners have therefore called for further harmonization of certain procedural aspects. Recommended measures include standardizing admissibility criteria for complaints, mandating that complaint procedures conclude with legally binding decisions subject to judicial review, clarifying cooperative duties (particularly concerning the timely exchange of comprehensive information), and establishing early consensus on the scope of and regular progress reporting on investigations (see, for example, Mustert 2023).

3.3. **DATA PROCESSING BY EMBS**

As mentioned earlier, EMBs—whether independent election commissions, national ministries or local authorities—are responsible for core election data processing, chiefly voter registration and related personal data of voters. Under the GDPR, these EMBs are typically data controllers (often public authorities), meaning they bear full responsibility for compliance.

Under the GDPR, these EMBs are typically data controllers (often public authorities), meaning they bear full responsibility for compliance.

Table 3.1. **Key obligations and implications for EMBs**

GDPR principles and rules	Obligation and competences
Article 5(1)(a) and (b): Principles of legality and purpose limitation	EMBs usually process voter data under a legal obligation or in the public interest, as defined in election laws. The GDPR emphasizes that data collected for managing elections must not be repurposed for incompatible uses. A cautionary example comes from Belgium, where a mayor who accessed citizens' data (originally collected for administrative purposes) for distribution in his re-election campaign letters was found in breach of the GDPR's purpose limitation principle. Belgium's data protection authority imposed its first GDPR fine on this official, in 2019, making it clear that even public officials cannot reuse voter data for campaigning without a proper legal basis (Hunton 2019). EMBs must ensure that any use of voter information is strictly aligned with electoral purposes (e.g. generating polling station notifications or ballot mailings) and not used for partisan advantage.
Article 5(1)(a): Transparency principle Articles 13 and 14: Right of data subject to be informed	EMBs are required to inform voters about how their personal data will be used in the electoral process. Typically, election laws or privacy notices spell out what data is on the electoral roll, who can access it and how long it will be retained. Voters have the right to access their data and request corrections (crucial for addressing voter register errors). In some cases, voters may opt out of sharing certain information. In Germany, for example, residents can object to their addresses being passed to political parties for campaign purposes (section 50 Absatz 5 Satz 2 Bundesmeldegesetz i. V. m. section 36 Absatz 2 Satz 2 Bundesmeldegesetz). Data protection authorities stress that clear communication is key. In France, the National Commission for Information Technology and Civil Liberties fined a political association EUR 20,000 (approximately USD 22,000) in 2024 for failing to properly inform individuals during political canvassing (CNIL 2025). EMBs should thus maintain up-to-date privacy notices and respect any objections to the use of voter data, for example, when a voter opts out of public electoral registers or propaganda mailings.

Table 3.1. **Key obligations and implications for EMBs (cont.)**

GDPR principles and rules	Obligation and competences
Article 5(1)(f): Principle of data security Article 5(a)(d): Principle of data accuracy Article 5(1)(d): Principle of accountability Article 33: Notification of personal data to the supervisory authority Article 34: Communication of a personal data breach to the data subject	Protecting the confidentiality and integrity of voter data is paramount. EMBs must implement appropriate security measures (access controls, encryption for digital databases, secure storage for paper files) to prevent unauthorized access or leaks. Any data breach involving an electoral register (e.g. a leaked voter list or a hacked election IT system) can undermine public trust and even affect electoral integrity. In such cases, the GDPR's breach notification rules apply: the EMB must notify the data protection authority (and potentially the affected voters) without undue delay if a breach poses risks (article 33 GDPR). The CJEU[1] clarified that even if a breach is caused by a technical error or external attack, controllers can be held liable if they lacked adequate safeguards. This decision underscores the need for accountability and risk management by public bodies, including EMBs.
Article 5(2): Accountability principle Article 24: Responsibility of the controller and processor Articles 35 and 36: Data protection impact assessment and prior consultation Article 25: Data protection by design and by default	EMBs should conduct data protection impact assessments for new election technologies (e.g. e-voting systems, biometric voter ID) to identify and mitigate risks up front. These assessments should be presented in a clear and accessible manner in order to ensure that data subjects can fully exercise their rights under the GDPR. Protecting the rights of citizens requires the implementation of appropriate technical and organizational measures (see articles 26 and 28 GDPR). EMBs should also develop both in-house and technical expertise to ensure GDPR compliance and data protection by design and by default when implementing new election technologies. They also should appoint a data protection officer (required since EMBs are public bodies) to oversee compliance and serve as a liaison with the data protection authority (article 37 [1][a] GDPR).

1 Case C-340/21, *VB v Natsionalna agentsia za prihodite* ECLI:EU:C:2023:986.

Table 3.1. **Key obligations and implications for EMBs (cont.)**

GDPR principles and rules	Obligation and competences
Article 5(2): Accountability principle Article 26: Joint controller Article 24: Responsibility of the controller and processor Article 29: Processing under the authority of the controller or processor	It is common for EMBs to outsource certain tasks, such as printing ballots or voter cards, maintaining IT infrastructure or providing mailing services. Under the GDPR, any vendor processing personal data on behalf of an EMB must be bound by a data processing agreement and act only on the EMB's instructions (article 28[3] GDPR). The importance of this requirement can be seen in Poland's attempted postal voting arrangement in 2020. The government tasked the national postal service (a third party) with mailing ballots to all voters and sought to obtain voter data from local municipalities. Numerous mayors refused to hand over this data, citing the lack of legal basis and inadequate security (the request came via an unsigned email asking for unencrypted citizen data files) (Wanat 2020). Similarly, if an EMB engages an IT firm, it must vet the firm's security practices. Any mishandling of data by a contractor can expose the EMB, as controller, to liability, and any deviation can trigger an investigation by the data protection authority.

3.4. THE ROLE OF EMBS IN DSA ENFORCEMENT AND INTERAGENCY COORDINATION

The DSA employs a two-tier enforcement mechanism at both the national and EU levels. It introduces a 'layered responsibilities' enforcement model, allocating duties between national authorities and the EU level depending on the size and impact of online services. In practice, this means that day-to-day supervision of most online intermediaries is handled by regulators in each member state, the so-called digital services coordinators. Additionally, the European Commission directly oversees the largest platforms—VLOPs and VLOSEs. This two-tiered approach requires close coordination between national regulators and the Commission, especially during elections, when online disinformation or illegal content can threaten democratic processes.

To ensure coordination and consistency across this two-tier system, the DSA also establishes a new body, the European Board for Digital Services, composed of national regulators (digital services coordinators) and chaired by the Commission. The Board was designed to be an independent advisory group that brings together

all the national digital services coordinators (one per member state) with the European Commission. The Board is meant to act collectively in the EU's interest. Its establishment reflects the model used in EU data protection (the EDPB under the GDPR), aiming for coordinated enforcement across the single market.

3.4.1. The role of EMBs in risk assessment and mitigation under the DSA: Due diligence obligations of VLOPs and VLOSEs in electoral processes

One of the most important obligations for VLOPs and VLOSEs is to diligently identify, analyse and assess any systemic risks arising from the design or functioning of their services, including algorithmic systems, as specified in article 34 of the DSA.

In order to help VLOPs and VLOSEs meet this obligation, the European Commission published guidelines on 26 March 2024 aimed at mitigating systemic online risks affecting elections and safeguarding electoral integrity under the DSA (European Commission 2024b). These guidelines ensure that VLOPs and VLOSEs address risks to electoral integrity by promoting transparency, countering disinformation, tackling AI-generated content and enhancing cooperation with authorities, all while safeguarding freedom of expression and ensuring compliance with the DSA (European Commission 2024b).

The guidelines include measures throughout the entire electoral cycle—the pre-electoral, electoral and post-electoral periods—and that apply at local, regional, national and European levels. For instance, the guidelines highlight systemic risks such as FIMI, the spread of extremist content and radicalization, as well as content generated by AI tools (e.g. deepfakes). The list is non-exhaustive, and EMBs, alongside other authorities, can highlight other systemic risks to electoral integrity.

The European Commission also calls for reinforced internal processes during electoral periods, stressing the importance of identifying relevant information and making it available to the public during elections. VLOPs and VLOSEs should therefore collect and highlight relevant data for electoral processes, such as political party programmes, manifestos and events, including official election information, such as voting procedures, the legal framework and official communication channels, among other things. Moreover, VLOPs and VLOSEs are encouraged to ensure information and analysis are collected on national, regional and local context-specific risks (European Commission 2024b). Hence, VLOPs and VLOSEs

VLOPs and VLOSEs should build 'dedicated, clearly identifiable internal teams' that should engage with EMBs to reinforce the electoral processes at local, regional and national levels.

should build 'dedicated, clearly identifiable internal teams' (European Commission 2024b) that should engage with EMBs to reinforce the electoral processes at local, regional and national levels.

The Commission also calls for implementation of the Code of Practice on Disinformation (a self-regulatory tool developed by the European Commission in 2022 that became part of the DSA in 2025 as the Code of Conduct on Disinformation, European Commission 2025d) and other relevant EU industry codes, such as the Code of Conduct on Countering Illegal Hate Speech Online, best practices under the Content-Agnostic Election Integrity Framework for Online Platforms, and recommendations from civil society organizations and other stakeholders. The guidelines also call for the following measures: (a) media literacy initiatives; (b) fact-checking labels; (c) labelling of accounts and AI-generated content; (d) indications of official accounts; and (e) tools and information to help users assess the trustworthiness of information sources (European Commission 2024b):

The European Commission highlights the importance of cooperation and structured dialogue among national authorities, including electoral authorities and the digital services coordinators.

The Commission also highlights the importance of cooperation and structured dialogue among national authorities, including electoral authorities and the digital services coordinators—for example, organizing regular communication channels among stakeholders, developing incident response mechanisms and creating working groups to coordinate key electoral stakeholders.

3.4.2. **The Code of Conduct on Disinformation as a due diligence obligation to identify and mitigate systemic risks in civic discourse and electoral processes**

As already mentioned, VLOPs and VLOSEs are required to conduct risk assessments to identify and mitigate systemic risks on their platforms, including the spread of disinformation. In order to help them meet this requirement, the European Board for Digital Services incorporated the self-regulatory Code of Practice on Disinformation into the DSA's legal framework. In other words, the Code of Practice is a benchmark for determining DSA compliance in identifying and mitigating systemic disinformation risks.

The code provides a structured framework outlining more detailed and technical guidance—including specific quantitative and qualitative key performance indicators—that platforms can implement to reduce the prevalence and impact of disinformation. Signatories to the code agree to implement various mitigation measures, including demonetizing disinformation, ensuring

transparency in political advertising, maintaining service integrity and empowering users and fact-checkers.

Although the Code of Conduct addresses electoral disinformation as one of its top concerns, electoral authorities are given a minimal role in enforcing and implementing the code. Nevertheless, some provisions may overlap with the interests and competences of electoral authorities. These areas include 'civil society commitments', where signatories should increase oversight of online political advertising, use shared terminology on manipulative behaviours and practices, and provide evidence about tactics, techniques and procedures. Despite this overlap, EMBs are not assigned a formal role under the code.

Within the framework of the Permanent Task-force of the Code—the main body responsible for monitoring enforcement of the code—EMBs could advocate to influence its decisions on implementation of the code (Commitment 37). For instance, in order to reduce the spread of online disinformation, the Task-force is required to involve 'relevant experts in [its] activities …, and … [to organize] exchanges with third-party stakeholders to keep them updated and gather insights related to the disinformation phenomenon' (European Commission 2025c). The code also calls on signatories to 'cooperate and coordinate their work in special situations like elections or [crises]' (Measure 37.2). Thus, electoral authorities could advocate to be invited to take part in those discussions or to propose joint efforts with the European Cooperation Network on Elections in an effort to play an active role by contributing their expertise in electoral matters.

3.4.3. **Enforcement opportunities for EMBs under the DSA**

While the DSA primarily regulates online intermediaries, it also creates potential new roles and responsibilities for EMBs in how they oversee online political campaigns. EMBs could adapt their legal and operational practices to use the DSA's mechanisms to effectively counter disinformation and hate speech in online contexts.

Table 3.2. **Key DSA provisions and what they mean for EMBs**

DSA provision	Obligations/Role of EMBs
Article 9: Orders to remove illegal content	An EMB can issue a removal order only if national law designates it as a competent administrative authority for that purpose. For example, if election laws empower an EMB to require the removal of unlawful online election material, the EMB could act under article 9. Otherwise, an EMB cannot directly issue binding removal orders; it would need to refer the matter to the appropriate authority (such as a court or a regulator with the proper mandate).
Article 10: Orders to provide information	An EMB may issue a data disclosure order only if empowered by law as a competent authority to obtain such information (for instance, to identify the source of illegal campaign content). If the EMB lacks such a designation, it cannot compel platforms to divulge user information under the DSA. Instead, it would have to coordinate with law enforcement agencies or another authorized body to obtain the needed information.
Articles 11–13: Points of contact and legal representative	The DSA requires all online platforms to designate an EU legal representative and points of contact for authorities. This greatly aids EMBs, as they have a single official channel to reach each platform during elections. EMBs must utilize these channels to flag urgent issues or send formal orders. In practice, EMBs should maintain up-to-date contact lists for major platforms and establish liaison routines (especially during election periods) so that any notices or orders are received and acted on without delay. This is a new operational norm, moving away from ad hoc emails to leveraging the DSA-mandated contact points for more structured communication.

Table 3.2. **Key DSA provisions and what they mean for EMBs (cont.)**

DSA provision	Obligations/Role of EMBs
Article 22: Trusted flaggers	EMBs (or affiliated entities) can apply to become 'trusted flaggers' for election-related illegal content and, in specific cases, content that violates the terms and conditions of online platforms. Trusted-flagger status, granted by the national digital services coordinator, means an EMB's content reports get high-priority handling by online platforms. To qualify, EMBs must have expertise and independence and adhere to accuracy and objectivity standards. If accredited, an EMB's moderation team could rapidly flag things like voter intimidation posts or illegal paid ads, and the platform must 'process and decide on' these notices without undue delay. Being granted this status could help EMBs tackle harmful content short of formal orders. However, EMBs would also have an obligation to flag responsibly—providing sufficient evidence and legal rationale in each notice. EMBs could participate directly in the content moderation policies of online platforms (such as Facebook, X, YouTube, etc.), flagging content and submitting an internal complaint to the digital services coordinator. Finally, online platforms would have to inform the competent enforcement authorities in the event that there is suspicion of serious criminal offences involving a threat to individuals' safety (e.g. online gender-based violence).
Article 34: Systemic risk assessment (elections)	VLOPs must assess 'any actual or foreseeable negative effects on civic discourse and electoral processes' on their services. While this obligation rests with platforms, EMBs can play a role in informing and evaluating risk assessments. EMBs might want to communicate local electoral risk factors to platforms and digital services coordinators (e.g. known patterns of misinformation or past interference tactics). They could also play an active role vis-à-vis platforms' independent auditors or peer regulators to provide expert insight into how platform algorithms or behaviours are impacting their national elections. In essence, EMBs become stakeholders in the risk assessment process, helping ensure that platforms identify the correct election-related risks (such as deepfake propaganda or microtargeted voter suppression efforts).

Table 3.2. **Key DSA provisions and what they mean for EMBs (cont.)**

DSA provision	Obligations/Role of EMBs
Article 36: Crisis response mechanism	In exceptional cases (e.g. a security crisis impacting an election), the European Commission can declare a DSA crisis and require platforms to take extraordinary measures for a limited time. If an election in one member state were undermined by a sudden massive disinformation attack from a foreign actor, for example, this event could trigger article 36. In such scenarios, EMBs might want to coordinate closely with the European Commission and digital services coordinator—providing evidence of the crisis, helping shape temporary measures (such as a rapid takedown of specific content or the imposition of an algorithmic restriction) and communicating with the public about any impacts (for instance, if certain platform features are throttled during the emergency). While not routine, EMBs should be prepared for such a contingency by developing crisis communication plans in coordination with European authorities and online platforms.
Article 40: Data access for researchers	Although this article empowers vetted researchers, not EMBs, it has indirect benefits for EMBs. EMBs can partner with research institutions[1] that obtain data access to detect, identify and analyse systemic risks in the EU and to assess the adequacy, efficiency and impacts of risk mitigation measures in the context of elections. Insights from such research (e.g. detailed analysis of how disinformation spreads on a platform during an election) can inform EMBs' future regulatory actions or legal reforms. EMBs should thus be aware of this provision and support bona fide research institutes conducting research into online electoral campaigns, effectively leveraging the transparency that the DSA creates.

1 As defined in article 2(1) of Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

3.5. **INTERAGENCY COORDINATION**

In the context of the implementation of mitigation measures on the part of VLOPs and VLOSEs in electoral processes at the national level, the European Board for Digital Services and the European Commission issued the DSA Elections Toolkit for Digital Services Coordinators. Inspired by the Commission's Guidelines for Elections, the Toolkit outlines measures to safeguard the integrity of electoral processes, including addressing the spread of hate speech, disinformation and the deceptive use of AI-generated content or other forms of FIMI.

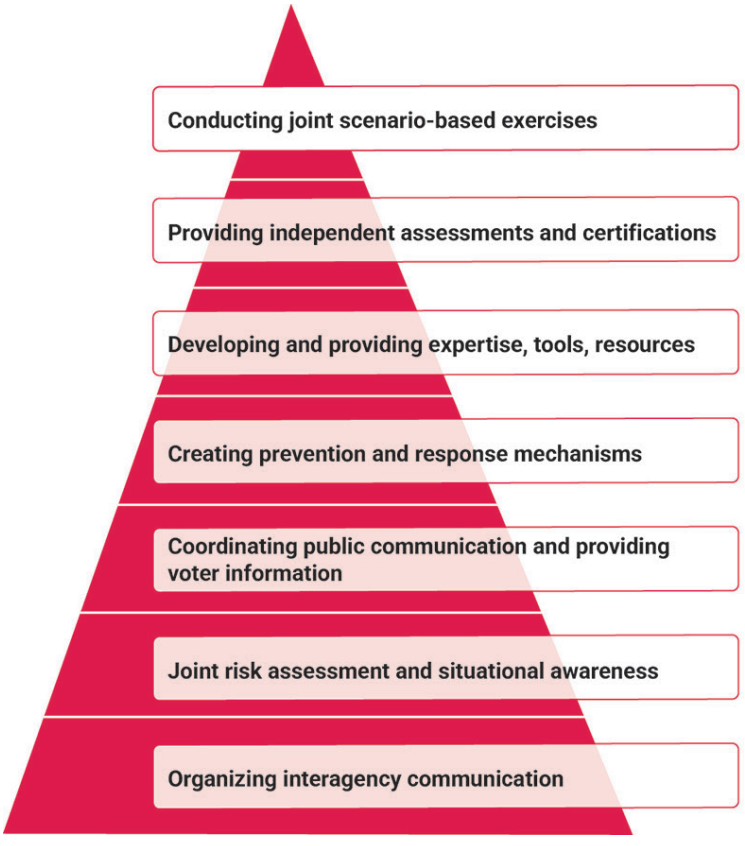
According to these guidelines, the role of digital services coordinators is structured around four key pillars: (a) stakeholder management—building relationships to share knowledge and resources; (b) communication and media literacy—informing, educating and building trust; (c) monitoring and analysis of election-related risk—facilitating public scrutiny and assessing the performance of VLOPs' and VLOSEs' mitigation measures; and (d) incident response—preparing, reacting and providing support during crises.

Within these four pillars, EMBs should be encouraged to leverage their central role in safeguarding electoral integrity and reinforce their expertise in working with key stakeholders to strengthen their capacity to safeguard and preserve the integrity of online electoral information, including countering disinformation operations, spread of hate speech, or FIMI, among others.

Interagency collaboration between digital services coordinators, EMBs and other relevant bodies provides an opportunity to address existing gaps within EMBs while fostering new in-house expertise. In this regard, International IDEA has developed a model for interagency collaboration in the field of cybersecurity (van der Staak and Wolf 2019), which could be adapted and applied to the context of mitigating risks to electoral processes.

When it comes to implementation of the DSA, the European Commission has already started to develop 'organizing interagency communications', which is in the base of our pyramid of 'level of inter-agency collaboration' (see Figure 3.1). The European Board for Digital Services has created a working group dedicated to ensuring the integrity of the information space, the scope of which encompasses electoral processes, FIMI, misinformation and disinformation, and other civil discourse (European Commission 2025a). This working group may be able to help establish a shared understanding of risk assessment and create prevention and response mechanisms in coordination with electoral authorities. The European Cooperation Network on Elections could play a key role here. A good example to be replicated is the implementation of cybersecurity exercises to evaluate and strengthen working methods for European elections, which shows how interagency collaboration can reinforce the protection of electoral integrity in Europe.

Figure 3.1. **Levels of interagency collaboration**



Source: S. van der Staak and P. Wolf, *Cybersecurity in Elections: Models of Interagency Collaboration* (Stockholm: International IDEA, 2019), <https://doi.org/10.31752/idea.2019.23>.

A collaborative effort between EMBs, digital services coordinators and online platforms could help to build resilience among electoral stakeholders to counter the main challenges to electoral integrity in the digital realm.

In sum, the protection of electoral information integrity is a complex and long-term undertaking that requires the coordination of several national and European institutions to exchange good practices, share information and resources, and maintain situational awareness. A collaborative effort between EMBs, digital services coordinators and online platforms could help to build resilience among electoral stakeholders to counter the main challenges to electoral integrity in the digital realm.

3.6. THE ROLE OF ELECTORAL AUTHORITIES UNDER THE AI ACT

In terms of institutional enforcement, the AI Act (article 70) mandates that each EU member state must designate a national supervisory authority for implementation and oversight. Although electoral commissions are not designated as enforcement bodies, they will likely be drawn into the AI governance network through interagency coordination, especially where AI is used in election logistics or campaign monitoring. For example, electoral authorities may be required to audit AI systems for conformity assessments or collaborate with data protection authorities on AI deployments involving personal data (European Data Protection Board and European Data Protection Supervisor 2021).

Moreover, enforcement of the act intersects with other relevant legislative instruments, notably the GDPR and the DSA. These laws, in conjunction with the AI Act, create a comprehensive compliance environment for electoral actors and platforms, with electoral bodies likely serving as norm enforcers and intermediaries.

A key concern addressed by the AI Act is the use of manipulative or deceptive AI in political communication. The prohibition of AI systems that manipulate behaviour or exploit vulnerabilities (article 5) directly targets applications such as emotionally persuasive deepfakes or AI-driven disinformation bots (Floridi et al. 2018). While electoral authorities are not directly tasked with enforcing these bans, they will need to monitor electoral environments for the presence of such systems and liaise with regulatory authorities to address violations, including by flagging suspicious content, promoting transparency in campaign strategies and supporting voter education on AI-generated material.

However, the implementation of these provisions in electoral contexts presents institutional and practical challenges. The most immediate challenge is fragmentation: the AI Act does not clearly set out how electoral bodies fit into the enforcement framework, which may lead to gaps in oversight or duplication of efforts (Iwańska et al. 2024: 18–19). Additionally, many electoral institutions currently lack the technical capacity to evaluate compliance with AI standards or to distinguish between lawful and unlawful AI deployments during campaigns.

The AI Act does not clearly set out how electoral bodies fit into the enforcement framework, which may lead to gaps in oversight or duplication of efforts.

Furthermore, there is also the issue of timing and responsiveness; election cycles are time-sensitive, and existing AI enforcement

mechanisms may not be agile enough to respond to fast-moving manipulative practices in real time.

Given these concerns, electoral bodies must begin preparing for the regulatory demands introduced by the AI Act. Preparation includes building internal capacity for AI risk assessment, developing mechanisms for pre-election audits, and engaging in joint task forces with data protection authorities and national AI supervisors. Preparation for these regulatory demands requires a collective effort that should be framed through interagency collaboration mechanisms (see 3.5: Interagency coordination).

Enforcement of the AI Act requires interagency communication, the development and sharing of expertise, and joint scenario-based exercises, among other things. It also requires cooperation among non-state actors such as political parties, private companies and civil society organizations. Electoral commissions should also advocate for transparency requirements for political campaigns deploying AI—such as mandatory disclosures on the use of AI-generated content or behavioural targeting tools. Public trust in elections increasingly depends not only on procedural integrity but also on the perceived fairness of the information ecosystem in which political decisions are made.

The AI Act introduces a robust regulatory framework that, while not tailored specifically for elections, has critical implications for electoral integrity.

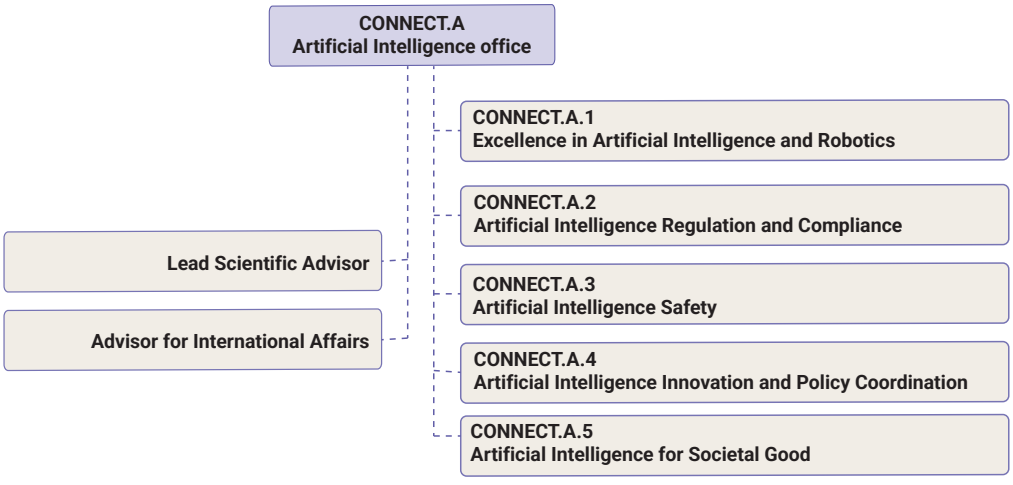
The AI Act introduces a robust regulatory framework that, while not tailored specifically for elections, has critical implications for electoral integrity. Electoral bodies must now navigate a legal environment in which AI systems, if misused, pose both technological and normative risks to democratic participation. While the act entrusts formal enforcement to national supervisory authorities, electoral commissions and regulators are de facto stakeholders in ensuring that AI technologies do not undermine free and fair elections. Their proactive engagement in enforcement, oversight and voter education will be central to the democratic legitimacy of the EU's AI governance regime.

3.6.1. **EMBs' engagement with the European AI Office**

The European Commission is the institution with primary responsibility for implementation and enforcement of the AI Act. A dedicated body, the European AI Office, operating under the responsibility of the Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT), is tasked with supporting the implementation of the act. The Office coordinates AI policies at the EU level, builds capacities and expertise, and carries out other related tasks.

In the context of elections, CONNECT A.3, the unit responsible for AI safety, is the key point of contact for electoral authorities seeking support in implementing provisions of the AI Act. This unit, within the AI Office, should engage with experts, civil society and other relevant stakeholders in cooperation with the Commission's Directorate-General for Justice and Consumers (DG JUST) and other EU bodies, such as the EU Fundamental Rights Agency and the EDPS.

Figure 3.2. **Scheme of the European AI Office within DG Connect**



Source: Iwańska et al., 'Towards an AI Act that serves people and society: Strategic Actions for Civil Society and Funders on the Enforcement of the EU AI Act', European AI & Society Fund by the European Center for Not-for-Profit Law, August 2024, p. 19, <https://ecnl.org/sites/default/files/2024-09/AIFUND_ECNL_AI_ACT_Enforcement_2024.pdf>, accessed 22 September 2025.
Note: Additionally, article 65 of the AI Act establishes the European Artificial Intelligence Board, which is tasked with ensuring consistency and coordination between national competent authorities in the member states regarding the implementation of the regulation. Although election monitoring is not explicitly mentioned, the Board should engage with relevant EU institutions and networks, including the European Cooperation Network on Elections and national electoral bodies.

Furthermore, article 77 of the AI Act provides that national public authorities responsible for supervising or enforcing compliance with EU law to protect fundamental rights have the power to request and access any documentation created or maintained under the act. Such information must be provided in an accessible language and format when necessary for authorities to effectively fulfil their mandates within the limits of their jurisdiction. The market surveillance authority must be informed of such requests.

This provision enables electoral bodies, within their competence to protect individuals' right to vote and to stand as candidates in elections, to access relevant documentation and information to uphold fundamental rights in the electoral context. The exercise of those competences should be done in cooperation and coordination with other fundamental rights bodies, such as equality bodies and data protection authorities, as well as other relevant actors, including civil society organizations.

3.6.2. **Enforcement opportunities for EMBs under the AI Act**

The AI Act represents a significant regulatory development, positioning the EU as the first jurisdiction to introduce a comprehensive legal framework for AI. While designed as a cross-sectoral regulation, the act has both direct and indirect implications for electoral processes and the public institutions that oversee them. Although electoral processes are not the act's primary concern, its focus on risk-based oversight, fundamental rights protection and governance structures intersects with the regulatory needs of democratic elections in substantial ways. For details about key provisions in the AI Act please see Table 3.3.

3.7. PERSPECTIVES OF EMBS ACROSS EU MEMBER STATES

The research for this report included interviews with electoral stakeholders from EU member states, including the EMBs of Estonia, Finland, Germany and Ireland. The following summarizes perspectives and key takeaways.

- The implementation of the European digital regulatory framework remains novel and poses challenges even for the most advanced EU member states, many of which continue to navigate complex legal, technical and institutional ecosystems as they adapt to the evolving digital landscape.

- The institutional architecture and competences conferred to EMBs differ throughout the EU. In some member states, EMBs have a broader set of competences in implementing the EU's digital regulatory framework impacting elections. In others, competences are shared among a wide network of institutions, ranging from line ministries to computer security incident response teams, personal data protection agencies and more.

Table 3.3. **Key provisions of the AI Act and opportunities for EMBs**

AI Act provision	Opportunities for EMBs
Article 5: Prohibited AI practices	The AI Act prohibits the placing on the market, putting into service or use of AI systems that manipulate human behaviour through subliminal techniques or that exploit vulnerabilities (such as age, disability or socio-economic status) in ways that may materially distort a person's behaviour, particularly in ways that impair decision making (article 5[1][a]–[b]). It also prohibits AI systems that implement social scoring by evaluating or classifying individuals based on personal traits or social behaviour over time, where this leads to unjustified or disproportionate treatment (article 5[1][c]). These prohibitions are particularly relevant to elections, where AI-generated deepfakes, persuasive chatbots and disinformation bots could manipulate voter perception or exploit voter vulnerabilities. Although EMBs are not formal enforcement authorities under article 5, they should coordinate closely with data protection authorities and national AI supervisory authorities, especially during sensitive campaign periods.
Article 6 and Annex III: High-risk AI classification	AI systems are classified as 'high-risk' if they are used in essential public services, including law enforcement, critical infrastructure and public administration functions—potentially including electoral logistics (Annex III, section 5[b]). Such systems include tools used in voter registration, automated ballot processing and identity verification. If EMBs use or procure such systems, they must comply with the obligations under articles 8–15, which include: • implementing risk management systems; • ensuring data governance and accuracy; • maintaining logging and traceability; and • guaranteeing transparency and human oversight. They must also ensure that such systems undergo conformity assessments prior to deployment—either by notified bodies or internally (if allowed under the system classification). These obligations significantly increase the regulatory burden on electoral institutions that digitize parts of the voting process. Furthermore, the use of AI systems may expand the attack surface for cyberattacks, requiring EMBs to implement routine cybersecurity training and build resilience to default vulnerabilities.

Table 3.3. **Key provisions of the AI Act and opportunities for EMBs (cont.)**

AI Act provision	Opportunities for EMBs
Article 27: Fundamental rights impact assessments	Article 27 requires deployers of high-risk AI systems in the public sector to conduct a fundamental rights impact assessment (FRIA) before putting the system into use. This requirement includes EMBs if they deploy AI for electoral services such as voter registration, digital identity verification or election-related data analysis. FRIAs must assess the system's impact on rights, including privacy, non-discrimination, freedom of expression and political participation. While the AI Act does not mandate public consultation, it does require documentation of identified risks and planned mitigation measures. There is no obligation to publish FRIAs. For EMBs, FRIAs are a critical tool for identifying and mitigating risks to voter rights, fairness and inclusion, especially in contexts involving diverse or vulnerable populations. However, due to the lack of standardized templates and procedural safeguards, EMBs should go beyond baseline requirements by: • establishing robust internal review procedures; • encouraging transparency; and • engaging oversight bodies for validation. Where appropriate, EMBs should also collect gender-disaggregated data to detect and address the disproportionate impact of AI systems on the political participation of women and other vulnerable groups. Such data can help in detecting and mitigating algorithmic bias, as well as promoting fairness and inclusivity in electoral processes.
Articles 16–29: Obligations for high-risk AI deployers (users)	If an EMB deploys a high-risk AI system, it is legally considered a 'deployer' (user) under the AI Act and must ensure compliance in terms of: • human oversight (article 14); • logging and record keeping (article 12); • post-market monitoring and incident reporting (articles 72 and 73); and • technical documentation and conformity support (article 11). These provisions introduce legal accountability for EMBs even if the AI tools they employ are developed by third-party vendors. EMBs should update their procurement policies to require providers to supply conformity documentation, including CE markings or internal audit records, and ensure that systems meet relevant obligations under the act.
Article 50: Transparency obligations for AI-generated content	The act mandates that users of AI systems generating or manipulating content (e.g. deepfakes, synthetic videos, persuasive bots) must clearly disclose that the content was AI-generated (articles 52–54). This provision affects political parties and campaigns using AI-generated media. EMBs, in line with their responsibility for monitoring campaign conduct, can enforce these transparency standards by requiring political disclosures and updating campaign rules to prohibit undisclosed AI use.

Table 3.3. **Key provisions of the AI Act and opportunities for EMBs (cont.)**

AI Act provision	Opportunities for EMBs
Article 74: Enforcement	The act requires member states to designate national supervisory authorities to enforce the AI Act (article 70). While EMBs are not explicitly designated, national governments may assign a complementary or consultative role to EMBs regarding electoral AI systems. To ensure effective coordination, EMBs should engage with: • national AI supervisory authorities; • data protection authorities; and • digital services coordinators (in the framework of the DSA). This interagency collaboration is especially critical during election periods.
Articles 72–73: Post-market monitoring and incident reporting	EMBs that deploy high-risk AI systems must conduct ongoing monitoring, maintain incident logs and report serious system failures that affect user safety or rights. These measures are particularly relevant during elections, where technical reliability is crucial and public trust is fragile. EMBs should: • maintain internal AI risk registers; • conduct post-election technical audits; and • establish incident response plans aligned with electoral crisis protocols (van der Staak and Wolf 2019).
Article 57: Regulatory sandboxes	The act encourages innovation through regulatory sandboxes (article 57), where EMBs can test AI tools (e.g. for voter education, accessibility or fraud detection) under the guidance of regulators. EMBs should apply to participate in national or EU-level sandboxes, gaining support for AI experimentation while minimizing legal risks.

- The various competences are reflected in each EMB's role and its engagement with national and European institutions in shaping EU digital regulation. EMBs with greater powers in implementing the EU digital acquis also maintain more direct ties and closer involvement with EU institutions. Those with more limited competences—due to the division of competences with other institutions, such as the data protection authority, the information security authority or the media regulator—are less directly engaged.

EMBs with greater powers in implementing the EU digital acquis also maintain more direct ties and closer involvement with EU institutions.

- The protection of personal data and GDPR compliance remain at the forefront of institutional action in EU member states. As such,

EMBs report that voter lists are not published, access to voter data is restricted and such data is handled with extreme care.

- Regarding threats to electoral processes, some EMBs report that they have not experienced cyberattacks, while noting the role of the information security authority and close cooperation with European structures, such as the European Cooperation Network on Elections and the European Agency for Cybersecurity, in this regard. Other EMBs report cybersecurity incidents, in particular targeting political party websites. It is noteworthy that such attacks have not threatened the overall integrity of elections.

- EMBs take different approaches to content moderation, with some employing monitoring tools to identify disinformation or illegal speech (in the context of elections) on social media. Some EMBs engage companies to identify disinformation and illegal speech through a media listening tool or by using in-house experts who search for disinformation and correct it. One EMB reported that parties were required to label all AI-generated content. Other EMBs consider the monitoring of social media during elections to fall outside their competences, while noting other competent authorities that conduct monitoring activities.

- On AI, EMBs remain generally reluctant to deploy tools such as chatbots for their electoral management, though preliminary conversations exploring the use of AI by EMBs have taken place. One EMB noted that it employs such tools, though it follows a defensive approach. AI is mainly used for public education and engagement campaigns aimed at empowering the public to identify misinformation and disinformation.

- On EU-level participation, EMBs report on active engagement with platforms such as the European Cooperation Network on Elections, input to the European Democracy Shield Initiative, and participation in shaping EU legislation through relevant ministries.

- EMBs in EU member states are largely aware of the risks and challenges faced by their peers in EU accession countries, as well as of the cross-border nature of digital threats in electoral processes.

EMBs in EU member states are largely aware of the risks and challenges faced by their peers in EU accession countries, as well as of the cross-border nature of digital threats in electoral processes.

Chapter 4

CONCLUSION

The digital transformation of electoral processes creates both unprecedented opportunities and profound challenges for democracy resilience. While electoral processes remain a national competence, the EU has progressively developed a robust legal and institutional framework aimed at reinforcing democratic values and protecting fundamental rights in the digital domain. By embedding principles such as transparency, accountability and data protection into its digital regulation, the EU fosters a cohesive environment where digital technologies serve democratic processes rather than undermine them.

Through instruments such as the GDPR, the DSA, the TTPA, the EMFA and the AI Act, the EU has created a sophisticated legal architecture that addresses the key threats to electoral integrity, ranging from data misuse and algorithmic manipulation to disinformation and platform opacity. These legal instruments not only set standards for digital service providers but also offer essential safeguards for citizens and democratic institutions.

Moreover, the EU's collaborative initiatives, including interagency networks and platforms for best practice exchange, enhance member states' capacity to respond to cross-border challenges, coordinate oversight and ensure the security and transparency of electoral ecosystems. These efforts are vital in an era where information flows and influence operations are increasingly transnational in nature.

The EU's collaborative initiatives enhance member states' capacity to respond to cross-border challenges, coordinate oversight and ensure the security and transparency of electoral ecosystems.

Looking ahead, the effective implementation and coordinated enforcement of these frameworks will be critical to addressing emerging risks, including the deployment of generative AI and evolving microtargeting strategies. Strengthening cooperation among national authorities, EU institutions, civil society and digital

platforms remains indispensable for building resilient democratic societies. In this shared digital and regulatory space, the EU plays a key enabling role in supporting member states' efforts to uphold free, fair and transparent elections, while ensuring that digital innovation aligns with the foundational values of democracy, the rule of law and fundamental rights.

Glossary

Ad-delivery techniques	Optimization techniques that are used to increase the circulation, reach or visibility of a political advertisement on the basis of the automated processing of personal data and that can serve to deliver the political advertisement to a specific person or group of persons only (article 3[12] TTPA).
Artificial intelligence system/generative AI	A machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. AI systems vary in their levels of autonomy and adaptiveness after deployment (OECD n.d.).
Astroturfing	A deceptive practice that involves hiding the sponsors of an orchestrated message or organization (e.g. a political, economic, advertising, religious or public relations organization) to make it appear as grassroots support for a particular cause or idea. This practice can take many forms such as fake social media accounts, paid influencers and fake reviews, among others. It is intended to give certain statements or organizations credibility by hiding the financial sources behind them.
Behavioural targeting	A technique where a system—often through 'real-time bidding'—targets individuals visiting a website by collecting personal data and behavioural information that is share with publishers and advertisers. For instance, Facebook offers a tool called Facebook Pixel, which is a piece of code that advertisers can place on websites to track users' activities and then target those visitors again later with ads on Facebook.
Dark patterns	Digital practices used on websites and in apps that persuade consumers and users to take decisions that they did not intend to take, such as purchasing a product or signing up for a service. The Organisation for Economic Co-operation and Development (OECD) mentions in its definition that users can be steered, deceived, coerced or manipulated into taking decisions that are against their best interest.
Deepfake	AI-generated or manipulated image, audio or video content that resembles existing individuals, objects, places, entities or events and that appears to be authentic or truthful (article 3[60] AI Act).
Disinformation	Fabricated information or deliberately manipulated audiovisual content—for instance, intentionally created conspiracy theories or rumours. The information may be legal but is designed to cause harm.

Foreign information manipulation and interference	A pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. The activities involved are manipulative, conducted in an intentional and coordinated manner, and carried out by state or non-state actors, including their proxies inside and outside of their own territory (European External Action Service 2023).
Inferred data	Data created by a data controller on the basis of the data provided by a data subject or as observed by the controller.
Information integrity	The United Nations defines information integrity as the accuracy, consistency and reliability of information. Information integrity is threatened by disinformation, misinformation and hate speech.
Misinformation	Disinformation without the intent to manipulate people. It does not include the active fabrication of misleading content. Some examples are unintentional mistakes such as inaccurate photo captions, dates, statistics, translations or satire that is taken seriously.
Observed data	Data provided by a data subject—such as a user on a social media platform—when using a service or device (likes, shares, content consulted, etc.) (European Data Protection Board 2020b: 12).
Recommender system	A fully or partially automated system used by an online platform to suggest specific information to recipients of the platform or to prioritize that information, including as a result of a search initiated by a user of the platform or otherwise determining the relative order or prominence of information displayed (article 3[s] DSA).
Targeting techniques	Techniques that are used to address a political advertisement to only a specific person or group of persons, or to exclude them, on the basis of the processing of personal data (article 3[11] TTPA).

References

Access Now, 'Commissioner Breton: Stop politicising the Digital Services Act', 19 August 2024, <https://www.accessnow.org/press-release/commissioner-breton-stop-politicising-the-digital-services-act>, accessed 30 March 2025

Alvarado Rincón, D., 'The DSA Alone Won't Save Democracy—But Its Interplay with the Rule of Law Might', Democracy Reporting International, April 2025, <https://democracyreporting.s3.eu-central-1.amazonaws.com/images/67ecf2669e5db.pdf>, accessed 8 March 2025

ARTICLE 19, 'The Implications of the Proposed EU Political Advertising Regulation for Freedom of Expression', August 2023, <https://www.article19.org/wp-content/uploads/2023/08/A19-The-implications-of-the-Proposed-EU-Political-Advertising-Regulation-A19_clean.pdf>, accessed 3 March 2025

Barata, J. and Lazăr, E., 'Will the DSA save democracy? The test of the recent presidential election in Romania', Tech Policy Press, 27 January 2025, <https://www.techpolicy.press/will-the-dsa-save-democracy-the-test-of-the-recent-presidential-election-in-romania>, accessed 8 March 2025

Bashyakarla, V., Hankey, S., Macintyre, A., Rennó, R. and Wright, G., *Personal Data: Political Persuasion – Inside the Influence Industry. How It Works* (Tactical Tech, 2019), <https://cdn.ttc.io/s/tacticaltech.org/influence-industry.pdf>, accessed 31 March 2025

Becker Castellaro, S. and Penfrat, J., 'The DSA fails to reign in the most harmful digital platform businesses – but it is still useful', Verfassungsblog, 8 November 2022, <https://verfassungsblog.de/dsa-fails>, accessed 1 April 2025

Bogucki, A., Engler, A., Perarnaud, C. and Renda, A., 'The AI Act and Emerging EU Digital Acquis: Overlaps, Gaps and Inconsistencies', Centre for European Policy Studies, September 2022, <https://cdn.ceps.eu/wp-content/uploads/2022/09/CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf>, accessed April 1 2025

Botan, M., 'Algorithmic influence on elections: Insights from Romania's case study', European Digital Media Observatory, 9 December 2024, <https://edmo.eu/blog/algorithmic-influence-on-elections-insights-from-romanias-case-study>, accessed 1 April 2025

Bradshaw, S. and Howard, P. N., 'Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation', Oxford Internet Institute, Working Paper 2018.1, <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/07/ct2018.pdf>, accessed 10 April 2025

Burke, H., 'European Democracy Shield Explored', Institute of International and European Affairs, March 2025, <https://www.iiea.com/images/uploads/resources/Democracy_shield_explainer_final.pdf>, accessed 9 April 2025

Busch, C. and Mak, V., 'Putting the Digital Services Act into context: Bridging the gap between EU consumer law and platform regulation', *Journal of European Consumer and Market Law*, 109, (2021), <https://doi.org/10.2139/ssrn.3933675>

Calabrese, S., 'Reaction: Political agreement on the regulation on transparency and targeting of political advertising', European Partnership for Democracy, 10 January 2024a, <https://epd.eu/content/uploads/2024/01/Political-Advertising-Reaction-Paper-1.pdf>, accessed 1 April 2025

—, 'Is election integrity integral to the Artificial Intelligence Act?', European Partnership for Democracy, 2024b, <https://epd.eu/content/uploads/2024/07/Is-election-integrity-integral-to-the-Artificial-Intelligence-Act_-1-1-7.pdf>, accessed 16 March 2025

Center for Democracy and Technology, 'Initial Analysis on the First Round of Risk Assessments Reports under the EU Digital Services Act', March 2025, <https://cdt.org/wp-content/uploads/2025/03/RA-Report-Assessment-Report.pdf>, accessed 1 April 2025

Civil Liberties Union for Europe, 'Political Advertising on Facebook during the 2022 Hungarian Parliamentary Elections: Country Report', September 2022, <https://www.liberties.eu/f/fs3mhp>, accessed 1 April 2025

Commission Nationale de l'Informatique et des Libertés (CNIL), 'The sanctions issued by the CNIL', 2 January 2025, <https://www.cnil.fr/en/investigating-and-issuing-sanctions/sanctions-issued-cnil>, accessed 30 March 2025

Cornea, R., 'Romanian militant democracy in action: Shielding democracy from subversion and annulling the elections', Verfassungsblog, 1 April 2025, <https://doi.org/10.59704/1a0400f2b9629e46>

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 'Convention 108: Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data for the Purposes of Voter Registration and Authentication', T-PD(2023)2rev6, 7 June 2024, <https://rm.coe.int/tpd-2023-2rev6-processing-pd-in-vote-and-elections-en-final/1680b1511c>, accessed 31 March 2025

Court of Justice of the European Union (CJEU), Research and Documentation Directorate, 'Field of Application of the Charter of Fundamental Rights of the European Union', March 2021, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_en.pdf>, accessed 1 April 2025

Cunningham, F., 'Which countries have already designated their Digital Services Coordinators under the DSA?', Bird&Bird, 27 October 2023, <https://www.twobirds.com/en/insights/2023/global/which-countries-have-already-designated-their-digital-services-coordinators-under-the-dsa>, accessed 30 March 2025

Duivenvoorde, B. and Goanta, C., 'The regulation of digital advertising under the DSA: A critical assessment', *Computer Law & Security Review*, 51 (2023), <https://doi.org/10.1016/j.clsr.2023.105870>

European Commission, Democracy and Electoral Rights, [n.d.a], <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights_en>, accessed 1 April 2025

—, Legal Framework of EU Data Protection, [n.d.b], <https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en>, accessed 1 April 2025

—, 'Guidance Document: Commission Guidance on the Application of Union Data Protection Law in the Electoral Context', Document COM/2018/638, *Official Journal of the European Union* (12 September 2018), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0638>, accessed 5 March 2025

—, 'Commission Recommendation EU 2023/2829 of 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', Document C/2023/8626, *Official Journal of the European Union* (20 December 2023), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302829>, accessed 5 March 2025

—, 'Questions and answers on the Digital Services Act', 22 February 2024a, <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348>, accessed 30 March 2025

—, 'Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections', 26 March 2024b, <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707>, accessed 1 April 2025

—, 'Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes Pursuant to Article 35(3) of Regulation (EU) 2022/2065', Document C/2024/3014, *Official Journal of the European Union* (26 April 2024c), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024XC03014&qid=1714466886277>, accessed 5 March 2025

—, 'Mission Letter', 17 September 2024d, <https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf>, accessed 10 April 2025

—, 'Commission opens formal proceedings against TikTok on election risks under the Digital Services Act', 17 December 2024e, <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487>, accessed 8 March 2025

—, 'Working Groups under the European Board for Digital Services', last updated 12 February 2025a, <https://digital-strategy.ec.europa.eu/en/policies/dsa-board-working-groups>, accessed 14 April 2025

—, 'Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)', Document C(2025) 884, 27 July 2025b, <https://ec.europa.eu/newsroom/dae/redirection/document/112367>, accessed 1 April 2025

—, 'Code of Conduct on Disinformation', 2025c, <https://crta.org.cy/assets/uploads/pdfs/Code_of_Conduct_on_Disinformation_FoMhXqsV0yrrqv7x7rydctBc4_112678.pdf>, accessed 16 March 2025

—, 'Commission endorses the integration of the voluntary Code of Practice on Disinformation into the Digital Services Act', 2025d, <https://digital-strategy.ec.europa.eu/en/news/commission-endorses-integration-voluntary-code-practice-disinformation-digital-services-act>, accessed 27 August 2025

European Commission for Democracy through Law (Venice Commission), 'Urgent Report: On the Cancellation of Elections Results by Constitutional Courts', CDL-AD(2025)003, Opinion No. 1218/2024, 27 January 2025, <https://www.coe.int/en/web/venice-commission/-/urgent-report-on-the-cancellation-of-election-results-by-constitutional-courts>, accessed 14 April 2025

European Cooperation Network on Elections, Terms of Reference, [n.d.], <https://commission.europa.eu/document/download/f6b67fff-e28d-4af2-aac6-deb836da7f82_en?filename=terms_of_reference.pdf>, accessed 5 March 2025

European Court of Human Rights, 'Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights: Right to Free Elections', 31 August 2024, <https://ks.echr.coe.int/documents/d/echr-ks/guide_art_3_protocol_1_eng>, accessed 10 April 2025

European Data Protection Board, Tasks and Duties, [n.d.a], <https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en>, accessed 30 March 2025

—, 'The EDPB: Guaranteeing the Same Rights for All', [n.d.b], <https://www.edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf>, accessed 30 March 2025

—, 'Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns', 13 March 2019, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf> accessed 30 March 2025

—, 'EDPB adopts letter on Polish presidential elections data disclosure & discusses recent Hungarian government decrees in relation to the coronavirus during the state of emergency', 8 May 2020a, <https://www.edpb.europa.eu/news/news/2020/edpb-adopts-letter-polish-presidential-elections-data-disclosure-discusses-recent_en>, accessed 30 March 2025

—, 'Guidelines 8/2020 on the Targeting of Social Media Users', Version 1.0., September 2020b, <https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf>, accessed 1 April 2025

European Data Protection Board and European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)', 18 June 2021, <https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en>, accessed 10 April 2025

European Data Protection Supervisor, 'Data Protection', [n.d.], <https://www.edps.europa.eu/data-protection/data-protection_en>, accessed 1 April 2025

—, 'EDPS closes investigation into European Parliament's 2019 election activities', 23 March 2020, <https://www.edps.europa.eu/press-publications/press-news/press-releases/2020/edps-closes-investigation-european-parliaments_en>, accessed 30 March 2025

—, 'Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them', Version 1.0, 14 March 2022, <https://www.edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf>, accessed 31 March 2025

European External Action Service, '1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards Framework for Networked Defence', February 2023, <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf>, accessed 27 August 2025

European Parliament, 'Resolution of 20 October 2020 on Digital Services Act and Fundamental Rights Issues Posed', Document P9_TA(2020)0274, 20 October 2020, <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_EN.pdf>, accessed 10 April 2025

—, 'MEPs toughen rules on political advertising', Press release, 24 January 2023, <https://www.europarl.europa.eu/news/en/press-room/20230123IPR68616/meps-toughen-rules-on-political-advertising>, accessed 13 May 2025

—, 'Setting Up a Special Committee on the European Democracy Shield, and Defining Its Responsibilities, Numerical Strength and Term of Office', Document 2024/2999(RSO), 18 December 2024, <https://www.europarl.europa.eu/doceo/document/TA-10-2024-0065_EN.html>, accessed 9 April 2025

—, 'European Democracy Shield', Legislative Train Schedule, 20 March 2025, <https://www.europarl.europa.eu/legislative-train/package-european-democracy-action-plan/file-european-democracy-shield>, accessed 9 April 2025

European Parliamentary Research Service, 'Polarisation and the Use of Technology in Political Campaigns and Communications', Document PE634.414, March 2019, <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf>, accessed 1 April 2025

European Partnership for Democracy, 'Targeting and Amplification in Online Political Advertising', March 2022, <https://epd.eu/content/uploads/2023/08/Targeting-and-amplification-in-online-political-advertising.pdf>, accessed 1 April 2025

European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)', *Official Journal of the European Union* (27 April 2016), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>, accessed 5 March 2025

—, 'Regulation (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC', *Official Journal of the European Union* (17 April 2019), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790>, accessed 27 August 2025

—, 'Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)', *Official Journal of the European Union* (27 October 2022), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>, accessed 5 March 2025

—, 'Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the Transparency and Targeting of Political Advertising', *Official Journal of the European Union* (20 March 2024a), <https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng>, accessed 5 March 2025

—, 'Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 Establishing a Common Framework for Media Services in the Internal Market and Amending Directive 2010/13/EU (European Media Freedom Act)', *Official Journal of the European Union* (17 April 2024b), <https://eur-lex.europa.eu/eli/reg/2024/1083/oj/eng>, accessed 5 March 2025

—, 'Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence against Women and Domestic Violence', *Official Journal of the European Union* (24 May 2024c), <https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng>, accessed 5 March 2025

—, 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)', *Official Journal of the European Union* (12 July 2024d), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>, accessed 5 March 2025

European Union Agency for Cybersecurity, 'Election Cybersecurity: Challenges and Opportunities', February 2019, <https://www.enisa.europa.eu/sites/default/files/all_files/2019-02-28%20ENISA%20Opinion%20Paper-%20Election%20Cybersecurity.pdf>, accessed 5 March 2025

European Union Agency for Fundamental Rights (FRA) and Council of Europe (CoE), *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018), <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>, accessed 30 March 2025

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P. and Vayena, E., 'AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations', *Minds and Machines*, 28/4 (2018), pp. 689–707, <https://doi.org/10.1007/s11023-018-9482-5>

GDPR Hub, 'Garante per la protezione dei dati personali (Italy)' [Data Protection Authority (Italy)], 23 February 2023, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9853406>, accessed 30 March 2025

Gentile, G. and Lynskey, O., 'Deficient by design? The transnational enforcement of the GDPR', *International and Comparative Law Quarterly*, 71 (2022), pp. 799–830, <https://doi.org/10.1017/S0020589322000355>

Gorton, W. A., 'Manipulating citizens: How political campaigns' use of behavioral social science harms democracy', *New Political Science*, 38/1 (2016), pp. 61–80, <https://doi.org/10.1080/07393148.2015.1125119>

Gross, A., 'Draft Report on Timeline and Inventory of Political Criteria for Assessing an Election', European Commission for Democracy through Law (Venice Commission), Document CDL-EL(2010)021, 27 May 2010, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-EL(2010)021-e>, accessed 10 April 2025

Haeck, P., 'Romania gives Europe's digital police their first big test', *POLITICO*, 12 December 2024, <https://www.politico.eu/article/romania-election-eu-digital-services-act-social-media-tiktok-calin-georgescu>, accessed 30 March 2025

Heinmaa, T., *Winning Elections the Right Way: Online Political Advertising Rules in Europe and Selected Countries Globally* (Stockholm: International IDEA, 2023), <https://doi.org/10.31752/idea.2023.77>

Human Rights Watch (HRW), 'Trapped in a Web: The Exploitation of Personal Data in Hungary's 2022 Elections', 1 December 2022, <https://www.hrw.org/report/2022/12/01/trapped-web/exploitation-personal-data-hungarys-2022-elections>, accessed 1 April 2025

—, '"I Can't Do My Job as a Journalist": The Systematic Undermining of Media Freedom in Hungary', 13 February 2024, <https://www.hrw.org/report/2024/02/13/i-cant-do-my-job-journalist/systematic-undermining-media-freedom-hungary>, accessed 14 April 2025

Hunton, 'First fine imposed by the Belgian DPA since GDPR', 4 June 2019, <https://www.hunton.com/privacy-and-information-security-law/first-fine-imposed-by-the-belgian-dpa-since-gdpr>, accessed 30 March 2025

Information Commissioner's Office, 'Guidance for the use of personal data in political campaigning', [n.d.], <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1>, accessed 30 March 2025

International IDEA, ICTs in Elections Database, [n.d.], <https://www.idea.int/data-tools/data/icts-elections-database>, accessed 16 August 2025

—, *Digital Microtargeting*, Political Party Innovation Primer 1 (Stockholm: International IDEA, 2018), <https://doi.org/10.31752/idea.2018.32>

Iwańska, K., Skoric, V., Fanucci, F., Keskindemir, B. and Kokkula, S., 'Towards an AI Act That Serves People and Society: Strategic Actions for Civil Society and Funders on the Enforcement of the EU AI Act', European Center for Not-for-Profit Law, August 2024, <https://ecnl.org/sites/default/files/2024-09/AIFUND_ECNL_AI_ACT_Enforcement_2024.pdf>, accessed 10 April 2025

Juneja, P., *Artificial Intelligence for Electoral Management* (Stockholm: International IDEA, 2024), <https://doi.org/10.31752/idea.2024.31>

Madiega, T., 'Digital Services Act', European Parliamentary Research Service, Document PE 689.357, November 2022, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf>, accessed 1 April 2025

Massé, E., 'Five Years under the EU GDPR: Becoming an Enforcement Success', Access Now, May 2023, <https://www.accessnow.org/GDPR-5-years>, accessed 31 March 2025

Mildebrath, H., 'An Analysis of the Newly Proposed Rules to Strengthen GDPR Enforcement in Cross-Border Cases', European Parliament, Document PE 757.613, April 2024, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757613/EPRS_BRI%282024%29757613_EN.pdf>, accessed 1 April 2025

Monteleone, S., 'Artificial Intelligence, Data Protection and Elections', European Parliamentary Research Service, Document PE 637.952, May 2019, <https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637952/EPRS_ATA%282019%29637952_EN.pdf>, accessed 1 April 2025

Mustert, L., 'Effectiveness and procedural protection in cross-border GDPR enforcement', EU Law Enforcement, 31 December 2023, <https://eulawenforcement.com/?p=8739>, accessed 27 March 2025

Nelson, G., 'Assessing the EU's Digital Services Coordinators on resourcing and readiness', Tech Policy Press, 28 May 2024, <https://www.techpolicy.press/assessing-the-eus-digital-services-coordinators-on-resourcing-and-readiness>, accessed 30 March 2025

Nenadić, I. and Brogi, E., 'Why news media need article 17 of the European Media Freedom Act', Centre for Media Pluralism and Media Freedom, 16 November 2023, <https://cmpf.eui.eu/why-news-media-need-article-17-of-the-european-media-freedom-act>, accessed 1 April 2025

—, 'The Game of Boards: The role of authorities in concerting the Digital Services Act and the Media Freedom Act for protecting media freedom', *Media Laws: Law and Policy of the Media in a Comparative Perspective*, 28 August 2024, <https://www.medialaws.eu/the-game-of-boards-the-role-of-authorities-in-concerting-the-digital-services-act-and-the-media-freedom-act-for-protecting-media-freedom>, accessed 1 April 2025

NIS Cooperation Group, 'Compendium on Election Cybersecurity and Resilience', last updated 2024, <https://ec.europa.eu/newsroom/dae/redirection/document/103148>, accessed 1 April 2025

Organisation for Economic Co-operation and Development (OECD), 'OECD AI Principles overview', [n.d.], <https://oecd.ai/en/ai-principles>, accessed 1 April 2025

Organization for Security and Co-operation in Europe (OSCE) Office for Democratic Institutions and Human Rights (ODIHR), 'Hungary, Parliamentary Elections and Referendum, 3 April 2022: Election Observation Mission Final Report', 29 July 2022, <https://www.osce.org/odihr/elections/523568>, accessed 8 October 2025

Rabitsch, A. and Calabrese, S., 'The EU's Artificial Intelligence Act and Its Impact on Electoral Processes: A Human Rights-Based Approach', European Partnership for Democracy and Election-Watch, September 2024, <https://epd.eu/content/uploads/2024/09/AI-and-elections.pdf>, accessed 1 April 2025

Reich, O. and Calabrese S., 'Civic Discourse and Electoral Processes in the Risk Assessment and Mitigation Measures Reports under the Digital Services Act', European Partnership for Democracy and Civil Liberties Union for Europe, March 2025, <https://www.liberties.eu/f/ielo4z>, accessed 1 April 2025

Tinière, R., 'The use of ECtHR case law by the CJEU: Instrumentalisation or quest for autonomy and legitimacy?' *European Papers*, 8/1 (2023), pp. 323–30, <https://doi.org/10.15166/2499-8249/654>

van der Staak, S. and Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration* (Stockholm: International IDEA, 2019), <https://doi.org/10.31752/idea.2019.23>

Veale, M. and Borgesius, F. Z., 'Demystifying the draft EU Artificial Intelligence Act— Analysing the good, the bad, and the unclear elements of the proposed approach', *Computer Law Review International*, 22/4 (2021), pp. 97–112, <https://doi.org/10.9785/cri-2021-220402>

VIGINUM, 'Manipulation d'algorithmes et instrumentalisation d'influenceurs : Enseignements de l'élection présidentielle en Roumanie & risques pour la France' [Manipulation of Algorithms and Instrumentalization of Influencers: Lessons from the Presidential Election in Romania and Risks for France], February 2025, <https://www.sgdsn.gouv.fr/files/files/Publications/20250204_NP_SGDSN_VIGINUM_Rapport_public_Elections_roumanie_risques_france_VFF.pdf>, accessed 16 August 2025

Wanat, Z., 'Polish postal vote raises data privacy concerns', *POLITICO*, 24 April 2020, <https://www.politico.eu/article/polish-postal-vote-raises-data-privacy-concerns>, accessed 30 March 2025

Wolf, P., Alim, A., Kasaro, B., Saneem, M., Namugera, P. and Zorigt, T., *Introducing Biometric Technology in Elections* (Stockholm: International IDEA, 2017), <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>, accessed by 1 April 2025

About the authors

Sebastian Becker Castellaro is an Associate Programme Officer of the Digitalization and Democracy Programme at International IDEA. His work focuses on the impact of technology in democracies worldwide, providing research, policy analysis and project support. He holds an LLM in International Law from the Université Libre de Bruxelles and an LLM in Public Law from the University of Chile.

Gladiola Lleshi is an Associate Project Officer at International IDEA within the Regional Europe Programme. Her work focuses on the EU digital acquis and enlargement, particularly addressing the impact of emerging technologies on electoral processes. Previously, Gladiola worked at the European Insurance and Occupational Pensions Authority. In this role, she engaged with key EU regulatory frameworks such as the AI Act and the larger digital landscape.

Juliane Müller is an Associate Programme Officer in International IDEA's Digitalization and Democracy Programme. She specializes in the democratic implications of emerging technologies—particularly AI—with a focus on human rights and electoral integrity. Her work focuses on the programme's global AI capacity-building initiative for electoral management bodies and includes research and policy analysis. She holds an LLM in International Law from the University of Edinburgh and an LLB from the University of Mannheim.

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with 35 Member States founded in 1995, with a mandate to support sustainable democracy worldwide.

WHAT WE DO

We develop policy-friendly research related to elections, parliaments, constitutions, digitalization, climate change, inclusion and political representation, all under the umbrella of the UN Sustainable Development Goals. We assess the performance of democracies around the world through our unique Global State of Democracy Indices and Democracy Tracker.

We provide capacity development and expert advice to democratic actors including governments, parliaments, election officials and civil society. We develop tools and publish databases, books and primers in several languages on topics ranging from voter turnout to gender quotas.

We bring states and non-state actors together for dialogues and lesson sharing. We stand up and speak out to promote and protect democracy worldwide.

WHERE WE WORK

Our headquarters is in Stockholm, and we have regional and country offices in Africa and West Asia, Asia and the Pacific, Europe, and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

OUR PUBLICATIONS AND DATABASES

We have a catalogue with more than 1,000 publications and over 25 databases on our website. Most of our publications can be downloaded free of charge.

<https://www.idea.int>

STIFTUNG MERCATOR

International IDEA
Strömsborg
SE-103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

International IDEA
INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

This report analyses the European digital regulation and its impact on electoral integrity. Through a comprehensive approach, it examines how the EU digital playbook will play a role in regulating the main challenges of our (digital) democracies: data protection threats, cybersecurity attacks, content moderation, online gender-based violence, the use of AI in electoral management, online electoral campaigns, and the use of AI-generated content during elections.

While the organization of elections falls into European member state sovereignty, electoral authorities should develop collaborative mechanisms among European authorities to respond to digital threats. This report calls for electoral stakeholders to embrace the EU digital playbook through interagency collaboration to exchange experiences and capacities, among the EU electoral authorities and EU digital regulatory bodies, as well as to respond to the cross-border challenges that digital threats pose in democracies.

ISBN: 978-91-8137-005-8 (PDF)