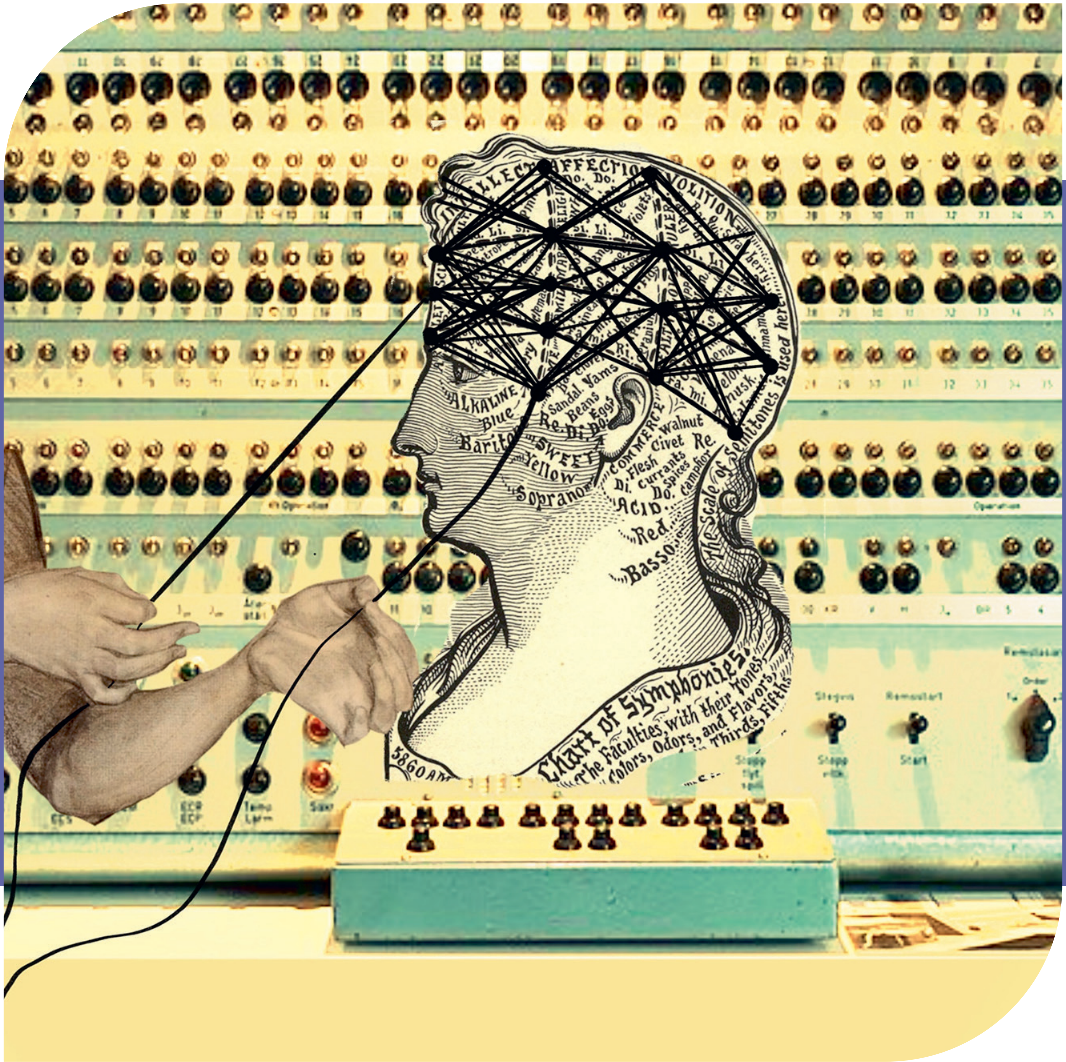
International IDEA

European Partnership for Democracy

THE ELECTION YEAR 2024 AND TECH POLICY AROUND THE WORLD

What lessons for the European Union?



THE ELECTION YEAR 2024 AND TECH POLICY AROUND THE WORLD

What lessons for the European Union?

Sofia Calabrese 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

European
Partnership for
Democracy

European Partnership for Democracy
Rue Froissart 123-133
B-1040 Brussels
BELGIUM
+46 8 698 37 00
info@epd.eu
www.epd.eu

International IDEA publications are independent of specific national or political interests. Views expressed in this publication do not necessarily represent the views of International IDEA, its Board or its Council members.

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: Turning Threads of Cognition by Hanna Barakat & Cambridge Diversity Fund. Published on Better Images of AI under a CCL BY 4.0
Design and layout: International IDEA
Copyeditor: Accuracy Matters Ltd.

DOI: <https://doi.org/10.31752/idea.2025.68>

ISBN: 978-91-8137-021-8 (PDF)

Abbreviations

AI	Artificial intelligence
CCIA	Computer and Communications Industry Association
DSA	Digital Services Act
DSCs	Digital services coordinators
EDMO	European Digital Media Observatory
EDRi	European Digital Rights
EPD	European Partnership for Democracy
FEC	Federal Election Commission
FIMI	Foreign information manipulation and interference
GPAI	General purpose artificial intelligence
ISD	Institute for Strategic Dialogue
RFI	Request for information
UNESCO	United Nations Educational, Scientific and Cultural Organization
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine

Acknowledgements

Gratitude is extended to Enzo Martino for his valuable input and editing contribution. Valuable feedback on the draft was also provided by International IDEA colleagues: Katarzyna Gardapkhadze, Peter Wolf, Therese Pearce Laanela, Alberto Fernández Gibaja, Sebastian Becker and Blerta Hoxha.

Thanks are also due to Jenefrida Isberg for administrative support, and to Lisa Hagman and Tahseen Zayouna in International IDEA's Publications team for their support in the production of this report.

Contents

EXECUTIVE SUMMARY

As digital technologies have increasingly shaped electoral processes throughout the 2024 election year, new challenges have emerged when it comes to artificial intelligence (AI), online political advertising campaigns, direct messaging, disinformation and hate speech.

This report seeks to identify a series of key issues and policy gaps in the European Union at the intersection of digital policy and elections, drawing on insights from the 2024 elections in other regions. It is written for EU institutional actors responsible for EU digital legislation in the context of elections—particularly officials in the European Commission (e.g. DG CONNECT, DG JUST) and members of the European Parliament engaged in electoral integrity and platform governance, alongside national digital services coordinators, electoral regulators and civil society watchdogs who shape, negotiate or enforce the rules that govern the online information space during elections. The report applies comparative lessons of the 2024 'super election cycle' to the EU's regulatory framework, focusing particularly on the online information environment, political advertising, platform accountability and emerging AI-enabled threats; it does not examine in detail specific election technologies, such as voting technologies or offline campaign finance rules, and traditional media regulation, except where these overlap with online dynamics. Building on global examples, the paper assesses which regulatory measures are most likely to succeed—or struggle—in the EU context and offers tailored, prioritized recommendations. It also flags emerging risks that will escalate if left unaddressed. Case studies were selected through purposive sampling: elections or incidents from 2024 were selected as case studies when they shed light on at least one of the four areas and offered clear lessons for EU policymakers. The sample spans a range of political systems and regions (e.g. Indonesia, Japan, Mexico, Pakistan, Romania, South Africa and the United Kingdom), yet the discussion draws most frequently on data-rich, high-profile contests in the United States, Brazil and India; this selective emphasis is acknowledged as illustrative rather than exhaustive. Findings rely on these illustrative cases and publicly available sources rather than a comprehensive dataset, and because regulatory landscapes, platform policies and AI capabilities evolve rapidly, some examples may date quickly; nevertheless, the paper pairs each identified risk with targeted recommendations before concluding with a forward-looking agenda for EU enforcement and coordination.

For each identified risk, the paper puts forward targeted recommendations and concludes with proposals for the road ahead. Main risks for the EU include legal fragmentation, the use of AI in election campaigns, the shortcomings of soft law, new trends such as the role of influencers and direct messaging, and the lack of structural solutions. A summary of the main gaps and recommendations can be found in Box 0.1.

Box 0.1. Summary of main gaps and recommendations

1. **Legal fragmentation can undermine the effectiveness of any regulatory regime**

   Ensure consistent implementation, enforcement and effective coordination across different legal frameworks.

2. **There are still weaknesses even in the most advanced digital policy frameworks on AI**

   Expand the interpretation of the Artificial Intelligence Act to explicitly include AI systems designed to influence elections within the scope of Annex III, thereby closing regulatory gaps and ensuring these technologies are appropriately governed.

3. **Non-binding instruments and soft law can complement and enhance regulatory frameworks and their enforcement**

   While soft law can be a valuable tool, it should not stand alone. If relied upon, it must be paired with concrete enforcement mechanisms and clear standards for compliance.

4. **New issues and trends seem to be emerging**

   To keep policy measures relevant and comprehensive, extend monitoring beyond platforms to new evolving trends such as encrypted direct messaging campaigns and influencer-driven political content or formats yet to emerge. Each institution should track developments within its mandate, actively listen to insights from external stakeholders, and feed insights into a regular exchange with peer bodies, researchers and civil society partners to enable early detection and coordinated response.

   Existing coordination mechanisms, such as the European Digital Media Observatory or the EU Rapid Alert System, could be leveraged or adapted to support this monitoring function, providing a practical foundation for identifying and addressing emerging threats in a timely and collaborative manner.

5. **Addressing disinformation, hate speech and election manipulation exclusively with rules for online platforms is not enough**

   Identify and tackle the (offline) root causes of online issues by strengthening public trust, promoting civic education and reducing societal polarization.

Chapter 1
BACKGROUND

Before and during the 2024 'super election cycle'—a year during which more than 60 nations, both established and emerging democracies across Africa, America, Asia and Europe, held critical votes—observers had grown increasingly alarmed by the expanding influence of digital technologies on electoral outcomes. Particular challenges included transparency, privacy, data protection and civic participation. Not only did this sweeping electoral exercise coincide with this rapid evolution of tools, but it was accompanied by rising global tensions and political polarization.

Of particular concern was the way anti-democratic forces frequently take advantage of online platforms to manipulate or undermine public opinion.

Of particular concern was the way anti-democratic forces frequently take advantage of online platforms to manipulate or undermine public opinion, which intensified fears that disinformation driven by artificial intelligence (AI) and other digital tools would be weaponized for political gain. In fact, the increasingly passive stance of some platforms—most notably X—in safeguarding electoral integrity further contributed to anxiety about technology-related risks in 2024 (Barrett, Hendrix and Richard-Carvajal 2024).

These concerns also find recognition in Pew Research's global elections report (Wike, Fagan and Clancy 2024) which labelled 2024 as a year of 'political disruption', and social media platforms and the Internet have been serving as a central stage for this upheaval. For instance, throughout **Venezuela's** 2024 elections, disinformation campaigns, some launched by the incumbent's party, made extensive use of digital methods—such as paid social media troll accounts and fabricated fringe websites—to discredit and harass members of the opposition, journalists, human rights defenders and politicians (Singer 2023; Puyosa, Azpúrua and Suárez Pérez 2024). The impact of these campaigns is difficult to evaluate due to the election's fraudulent nature, as recognized by a multitude of parties. Examples of anomalies ranged from voting irregularities to regulations preventing voting from abroad and the rejection of an EU observer (Asplund et al. 2025). The opposition showed that their candidate had the votes to win the election by a large margin (Wells 2024), suggesting that public opinion may not have been swayed by disinformation. The results of the election itself have been rejected by the United States, the European Union and 10 Latin American countries (Phillips 2024).

At the same time, digital tools also served legitimate campaign purposes, such as increasing outreach and engagement with voters. In **India**—home to the world's second-largest Internet user base—platforms like YouTube, Facebook, X, Instagram and WhatsApp helped candidates—mainly the incumbent—connect with diverse constituencies ahead of the general elections (Christopher and Bansal 2024; Singh 2024). In places like the **USA, Japan** and **Pakistan**, AI tools were employed to translate political speeches or mobilize voter turnout.

At the same time, digital tools also served legitimate campaign purposes, such as increasing outreach and engagement with voters.

To address the complex challenges posed by digital technologies—ranging from transparency and privacy to data protection and civic participation—governments worldwide have pursued a variety of strategies. Some rely on soft law or non-binding guidelines, while others opt for more narrowly targeted or comprehensive legislation, both sectoral and general.

African nations, for example, have taken notable steps in shaping the responsible use of digital media during elections. The Association of African Election Authorities, with support from the Electoral Commission of South Africa, launched the influential 'Principles and Guidelines for the Use of Digital and Social Media in Elections in Africa' (Electoral Commission of South Africa n.d.), which marks an important milestone in establishing frameworks to safeguard electoral processes.

Turning to Europe, in the **EU**, around 13 member states went to vote in 2024, and the European Parliament elections also took place between 6 and 9 June. The EU stands out with its emerging digital regulatory ecosystem that seeks to ensure accountability and transparency among major online platforms. In particular, the EU has one of the most advanced frameworks of rules for online platforms, the Digital Services Act (DSA), which was fully applicable as of February 2024. This regulation includes mechanisms to address disinformation and hate speech and obliges Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) to assess risks to civic discourse and electoral processes.

While some incidents have taken place throughout the different elections in the **EU**, it is generally agreed that the situation has remained largely stable and manageable when it comes to the influence of social media, advertising campaigns and deepfakes on the outcome of the elections, in particular the European Parliament elections.

The new EU rules are still very young and their effectiveness is still being tested against real cases.

The EU has been resilient to disinformation strategies, partially due to several initiatives such as fact-checking programmes, codes of conduct among political parties and a strong regulatory framework (EDMO 2024). In late 2024, however, the cancellation of elections in **Romania** came as a shock, showing the importance of fully enforcing transparency rules for the funding of digital campaigning and highlighting the existence of weaknesses and gaps in the current frameworks. For example, it showed the lack of effort by VLOPs involved in conducting risk assessment and adopting mitigation measures mandated by the DSA at a national level and it also highlighted the vulnerabilities of recommender systems within Big Tech companies such as TikTok. It also showed that the new EU rules are still very young and that their effectiveness is still being tested against real cases (Barata and Lazăr 2025; EDRi 2025). Finally, the DSA's political future is now uncertain. Following the European Parliament elections in 2024, some newly elected parties have openly challenged key provisions of the DSA—particularly those related to content moderation and platform accountability. Although the regulation remains in force, its implementation and enforcement may become more contested, especially in view of a broad 'simplification' effort that would address all sorts of legislation, including those that concern digital technology.

For this reason, there are two complementary paths forward: on the one hand, the EU needs to continue to have a strong stance on implementation and enforcement—as evidenced by the May 2025 legal referrals of **Czechia, Spain, Cyprus, Poland** and **Portugal** to the Court of Justice of the European Union for failing to properly designate, empower or penalize digital services coordinators (DSCs) under the DSA—and, on the other hand, it has to keep monitoring the implementation to identify the main gaps and weaknesses that might emerge in cases like the Romanian one.

The EU is not alone in this challenge. Examples from around the globe signal that the EU cannot afford to ignore the influence of new technologies on elections. While some countries, such as **Brazil**—where pioneering regulations address misinformation, political use of generative AI and electoral advertising—have taken a leading stance in digital policy, other regions reveal ongoing gaps and struggle with challenges. Chief among these is the need for robust and consistent regulatory frameworks governing online accountability mechanisms, AI-driven manipulation and oversight of political advertising.

The EU can draw valuable lessons from varied approaches around the world, which both highlight where progress has been made and underscore the need for ongoing vigilance and adaptation. Such approaches also demonstrate how insufficient legal provisions, inconsistent enforcement and policy coordination gaps can undermine electoral outcomes, reinforcing the importance of the EU's continued leadership in setting and enforcing digital rules.

Chapter 2
MAIN GAPS AND RECOMMENDATIONS

The following section outlines a series of identified issues and gaps in digital policy and elections that could benefit from further action at the EU level and reinforce the existing EU legal frameworks as well as inspire and support efforts outside the EU to improve legislation.

Examples from across the globe highlight the widespread nature of these challenges and illustrate why they warrant increased attention. This context provides the foundation for the main recommendations aimed at strengthening electoral integrity and democratic resilience in a rapidly evolving digital landscape.

The 2024 election cycle in the USA was marked by the absence of a unified national regulatory framework and platform-by-platform policies, which essentially resulted in a patchwork approach to disinformation controls.

2.1. ENSURE CONSISTENT IMPLEMENTATION, ENFORCEMENT AND EFFECTIVE COORDINATION ACROSS DIFFERENT LEGAL FRAMEWORKS

The 2024 election cycle in the **USA** was marked by the absence of a unified national regulatory framework and platform-by-platform policies, which essentially resulted in a patchwork approach to disinformation controls. Tech platforms such as Meta (Facebook, Instagram) and YouTube implemented their own election integrity policies—ranging from fact-checking partnerships to temporary political ad restrictions (ISD 2024).

Meanwhile, individual states have introduced various measures to regulate online content moderation since 2018 (CCIA n.d.). However, many of these measures did not pass or were deemed

Box 2.1. **Key takeaways**

Legal fragmentation can undermine the effectiveness of any regulatory regime. Fragmented or piecemeal approaches to accountability mechanisms and information manipulation can seriously undermine the effectiveness of any regulatory regime. Such patchworks not only cause confusion for users and regulators but also allow loopholes that malicious actors can exploit.

Looking back at the global super election cycle, the different examples of online platform regulation outlined below show that putting robust mechanisms in place to address disinformation—and ensuring platforms have content moderation policies with strong implementation and enforcement—is crucial.

Signals from countries around the world also contain a clear indication that stronger action is needed at the EU level, when it comes to ensuring consistent implementation and enforcement.

unconstitutional[1]—including ‘anti-censorship’ policies, stricter content removal transparency and disclosure requirements, and child safety provisions (CCIA n.d.).

On a federal level, however, the US Supreme Court has clarified that content moderation by social media companies is protected as an expressive activity. This means it is classified as non-commercial free speech under the First Amendment, and that the government may therefore face substantial constitutional hurdles when attempting to regulate or mandate specific moderation practices. In recent cases, the Court emphasized that social media companies engage in protected expressive conduct when moderating content and rejected arguments that merely improving the ‘marketplace of ideas’ justifies restricting platforms’ editorial discretion.[2] In other words, enabling the truth to emerge in a competitive ‘market’ of ideas is not enough to prevent platforms from fact checking.

Furthermore, section 230 of the Communications Decency Act of 1996 provides immunity to online platforms from civil liability for third-party content and content removal under certain circumstances—which adds another layer of complexity for those seeking to introduce and enforce content moderation regulations. The limitations of this clause in the face of modern Internet

[1] For example in California see *X Corp. v Bonta*, No. 24-271 (9th Cir. Sept. 4, 2024), <https://cases.justia.com/federal/appellate-courts/ca9/24-271/24-271-2024-09-04.pdf?ts=1725467437>, accessed 20 August 2025.

[2] NetChoice LLC, <https://www.supremecourt.gov/opinions/23pdf/22-277_d18f.pdf>, accessed 20 August 2025; *Murthy v Missouri*, <https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf>, accessed 20 August 2025.

realities have also been recognized by the Department of Justice (US Department of Justice 2020), and around the time of the 2024 elections, multiple bills were introduced with the aim to repeal or reform section 230, most notably a proposal to sunset the provision altogether.

Fragmented regulatory approaches to online content moderation pose significant risks to electoral integrity.

Fragmented regulatory approaches to online content moderation pose significant risks to electoral integrity, as exemplified by experiences in the **USA**. The US landscape, characterized by varying state-level regulations, inconsistent platform policies and federal legal constraints, illustrates how such a fragmented framework can undermine the effectiveness of electoral safeguards. Malicious actors exploit these inconsistencies by strategically choosing the least regulated channels to disseminate misleading content and disinformation. Additionally, contradictory legal measures complicate efforts to establish robust and consistent moderation practices, impeding timely responses to emerging threats and fostering public uncertainty regarding electoral security. Ultimately, without unified and coherent regulatory standards at the national level involving multiple stakeholders, influence campaigns—whether foreign or domestic—can more easily gain traction. Reports from oversight bodies, including the US Department of Homeland Security (Office of Inspector General 2022), have underscored the urgent need for cohesive, nationwide policies to protect election integrity. This case provides vital takeaways for the EU's own policies in this domain, calling for cohesion in regulations to reinforce electoral safeguards.

Looking towards the **EU**, 2024 was marked by the entry into application of the DSA, which included common rules for all sorts of online platforms. These include mechanisms to address disinformation and hate speech, the obligation for platforms to adopt transparent content moderation policies, and for so-called VLOPs and VLOSEs to assess the risks regarding civic discourse and electoral processes and mitigate them. The DSA is also complemented by the Guidelines on Election Integrity and the DSA Elections toolkit for DSCs (European Commission 2024a).

After the application of the DSA, there were minor incidents in some 2024 elections, such as disinformation campaigns—for example, in Italy during the EU elections (Hartmann 2024a)—but the common take is that the situation has been mostly under control. While the DSA is still a very young set of rules and was hardly implemented and enforced at that stage, it did force platforms to take some extra measures tailored to elections to protect information integrity, which have contributed to keeping the situation under control (Meta 2024).

However, even with newly introduced or proposed unified legal frameworks, weaknesses remain in coordinating the various pieces of legislation designed to regulate online platforms. While the enforcement and implementation of the DSA is centralized for VLOPs and VLOSEs and is in the hands of the European Commission, the member states' national authorities, known as DSCs, are in charge of all other smaller platforms. Many of these authorities, including the European Commission, are understaffed (EDRi 2024) and rely significantly on external advice from civil society—which is underfunded. While many investigations have been opened over the first year of DSA implementation, it is unclear how far this will be pushed in the current political climate, with VLOPs breaching their commitment to fight against hate speech and disinformation (Alvarado Rincón and Meyer-Resende 2025), and calls from political groups to withdraw the rules and from tech companies pressuring the US administration to weaken DSA enforcement (Hendrix 2025).

The **Romanian** elections showed some of the weaknesses in the current legislative framework in terms of regulating online platforms, in particular in the links between different pieces of legislation.

Ultra-nationalist pro-Russian candidate Călin Georgescu won the first round of the presidential elections. His success was linked to an ad campaign on TikTok with opaque funding sources (Paun 2024). The ads were not identified as political and hence not labelled as such, as required under Romanian law—and they were not removed either, as TikTok's ad policy would require, since it prohibits political ads. TikTok's algorithm is opaque, so understanding how videos are recommended to users remains a complex issue. Yet research has shown that, in the Romanian election, there was an overwhelming bias towards Georgescu in the videos that were being recommended to users. This bias was further supported by a survey asking Romanian users to report their experience with the platform leading up to the election. A total of 73 per cent of respondents recalled seeing a large amount of content about Georgescu, with a majority having noted suspicious behaviour and fake accounts spreading misinformation. TikTok denied these allegations, stating that the research did not reflect the reality for users. The platform is alleged to have blocked over 400,000 spam accounts and blocked fake likes to preserve its integrity (Global Witness 2024). Due to the lack of transparency behind TikTok's actions, it is hard to ascertain whether the platform truly abides by the regulations expected of it. Research seems to indicate otherwise, suggesting that under current legislation, platforms can avoid compliance with ease. While the new EU rules on transparency of political ads were not yet in force at the

TikTok's algorithm is opaque, so understanding how videos are recommended to users remains a complex issue.

time of the Romanian election, little would have changed, as TikTok would have similarly had to identify and remove the ads—or comply with the rules by labelling them as political.

What was actually in force at the time was the DSA, which mandates platforms to assess systemic risks to electoral processes and identify related mitigation measures. This should ideally include mechanisms to identify political ads. For this reason, the European Commission has opened an investigation regarding potential DSA infringement (Hartmann 2024b). This case is regarded by many as a stress test for the DSA, and a potential systemic indicator. The slow methodical analysis of risks under the DSA is now confronted with high-pace and high-profile crisis cases. TikTok and Romania themselves can be viewed as placeholders, as a multitude of platforms are now key political arenas in elections around the globe. TikTok was seen as a primary suspect in this election due to its popularity in Romania, but it was far from the only platform accused of failing to apply its own policies. Further investigations showed that similar political ad campaigns were run on other platforms such as Meta, Google Ads and even Telegram (Albert 2024).

The slow methodical analysis of risks under the DSA is now confronted with high-pace and high-profile crisis cases.

At present, these relatively new regulations appear to lack a sufficient deterrent effect, as many companies see limited incentives to invest in full compliance. This challenge is particularly acute with US-based platforms, which are increasingly pushing back against EU regulatory efforts and may become more assertive in resisting enforcement (Calabrese and Virah-Sawmy 2025).

Furthermore, while on paper the **EU** has in place harmonized rules for online platforms, requiring transparent content moderation policies and the assessment of relevant systemic risks for civic discourse and electoral processes, the effectiveness of these rules will depend on coordinated and consistent implementation, and on strong enforcement by the European Commission and national authorities.

Both the DSA and the Political Ads Regulation are very complex frameworks of rules that require a strong coordinated effort from platforms, EU enforcement authorities such as the European Commission and national enforcement to be effective. For example, when it comes to rules for funding political ad campaigns online, both the DSA and the Political Ads Regulation place oversight responsibility at the national level, requiring the establishment of new entities with responsibility for monitoring its implementation (Wolfs 2024). The DSA splits the oversight between the national DSCs and the European Commission—using the latter for the largest platforms.

For the Political Ads Regulation, the enforcement seems particularly complex, as it is distributed among five different roles and potentially five distinct authorities, namely: data protection authorities, DSCs, media regulators, electoral commissions and any additional authorities designated by member states (see EDRi, Civil Liberties Union for Europe and cdt Europe 2024). All these entities must be able to exchange information and collaborate when coordination challenges might arise, as enforcement competence is dispersed among many actors across multiple countries and governmental levels.

RECOMMENDATIONS FOR EU POLICYMAKERS

The EU should ensure strong, coordinated and consistent implementation and enforcement across different legal frameworks:

- The European Commission should stand firm on implementing existing rules such as the DSA and the Political Ads Regulation, including by clarifying the link between the different tools and by giving relevant feedback on the risk assessments performed by the platforms so that they are actually useful tools to prevent the spread of disinformation and hate speech with the same standards on the different platforms.

- The European Commission should also carry out investigations for breach of DSA rules, using all the tools at its disposal, including the Guidelines on Election Integrity, and dedicate enough resources to it.

- All authorities involved must be able to collaborate and exchange information when coordination challenges might arise, as enforcement competence is dispersed among many actors across multiple countries and governmental levels.

2.2. **ADDRESS RELEVANT GAPS IN AI REGULATION**

Box 2.2. **Key takeaways**

There are still gaps even in the most advanced digital policy frameworks on AI. In recent times, several frameworks have been adopted to regulate AI. As this is a very new topic to regulate, however, some of the new rules still contain gaps, in particular when it comes to protections for electoral processes.

Brazil's regulation, for example, is among the most comprehensive worldwide for controlling AI-generated political content, but critics point to the absence of clear definitions for key terms—such as 'disinformative content' or 'decontextualized fact'—which may undermine its effectiveness.

Such shortcomings also offer a cautionary signal to the EU: rather than overlooking similar gaps, it should reinforce its own safeguards. The EU's Artificial Intelligence Act (AI Act), however, devotes only scant attention to election-specific AI uses and still leaves significant blind spots.

In particular, the AI Act does contain wording under the prohibited AI systems that might be linked to AI applications used in the context of elections—such as AI systems for voter data analysis and predictive analytics to perform microtargeting (in particular under article 5.1a on subliminal techniques; and article 5.1b on exploiting vulnerabilities to distort the behaviour of a person)—but the requirements to prove that are extremely strict and apply to a very limited number of systems.

Similarly, the AI Act contains provisions considering AI systems 'intended' to be used to influence elections to be high risk. Intentionality, however, is also very difficult to prove, as most AI systems are not inherently designed to influence elections.

Finally, provisions for general purpose AI (GPAI) systems do not explicitly consider AI applications used in the context of elections.

Overall, the EU AI framework could benefit from an implementation oriented towards filling gaps, in particular related to its prohibited, high-risk and general purpose AI applications.

Regarding AI, a noteworthy regulatory development came in **Brazil**, where the Superior Electoral Tribunal (TSE) issued new rules in February 2024 for the upcoming municipal elections.[3] These regulations explicitly require that any campaign content generated or edited by AI must include a disclaimer acknowledging the use of AI, and they grant the TSE extensive authority to punish deceptive

[3] Tribunal Superior Eleitoral. (2024, February 27). *Resolução nº 23.732, de 27 de fevereiro de 2024.* <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>, accessed 20 August 2025.

uses of synthetic media. According to the resolution, 'the use, to harm or favor candidacy, of synthetic content in audio, video format or a combination of both, which has been digitally generated or manipulated, is prohibited, even with authorization, to create, replace or alter the image or voice of a living, deceased or fictitious person (deep fake)'.[4] Candidates whose campaigns violate these rules risk severe penalties, including removal from ballots or disqualification from the election.[5]

Notably, the regulation bans AI-generated content not only for defamation but also for boosting a candidate's image—an aspect often overlooked in other legal frameworks. For instance, in **Indonesia**'s 2024 elections, candidates have used AI to portray themselves with heightened skills and qualities (Duffy 2024). However, local regulations, such as the Information and Electronic Transactions Law, the Penal Code and the 2017 election law, largely focus on libel, slander and disinformation, focusing on preventing attacks on opponents rather than on self-promotion. Scenarios where AI is deployed to unduly enhance a candidate's image are usually not encompassed by such provisions. Nevertheless, it was Indonesia's judicial branch rather than its legislature that addressed this issue when the Constitutional Court explicitly prohibited the use of AI in political campaigns to enhance a candidate's self-image (Satrio 2025).[6]

While **Brazil's** regulation is among the most comprehensive worldwide for controlling AI-generated political content, critics warn of potential gaps that could undermine its effectiveness (Farrugia 2025). Key terms such as 'freedom of expression', 'disinformative content' and 'decontextualized fact' remain undefined, which may lead to inconsistencies in enforcement. Likewise, article 9 calls for 'preventive corrective actions', including improving content recommendation systems, yet offers no clear benchmarks for compliance, leaving platforms to interpret these obligations as they see fit. Although the regulation calls for shared responsibility among law enforcement, civil society, political parties, candidates and tech companies, it lacks specific procedures or tools to ensure ongoing monitoring and enforcement (Farrugia 2025).

Although the regulation calls for shared responsibility among law enforcement, civil society, political parties, candidates and tech companies, it lacks specific procedures or tools to ensure ongoing monitoring and enforcement.

[4] Tribunal Superior Eleitoral. (2024, February 27). *Resolução nº 23.732, de 27 de fevereiro de 2024*. <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>, accessed 20 August 2025.

[5] Tribunal Superior Eleitoral. (2024, February 27). *Resolução nº 23.732, de 27 de fevereiro de 2024*. <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>, accessed 20 August 2025.

[6] See also <https://www.mkri.id/public/content/persidangan/putusan/putusan_mkri_11343_1735801113.pdf>, accessed 20 August 2025.

In the **USA**, despite fears of widespread deepfake disruptions during the 2024 election cycle, the real impact of AI-driven misinformation proved less extensive than many anticipated. While manipulated audio and video did circulate—such as AI-generated robocalls impersonating President Joe Biden to suppress voter turnout or a fabricated video depicting Vice President Kamala Harris in a hit-and-run—there is little evidence that these incidents significantly influenced voter behaviour (Stockwell et al. 2024). Contrary to the common perception that AI is primarily used for outright disinformation, many political campaigns around the world—including in the USA—employed AI more for creative or practical purposes than for spreading false information. For example, candidates Asa Hutchinson, Dean Phillips and Francis Suarez experimented with AI-powered chatbots to engage potential supporters (CBS News 2023; Chatelain 2024; Hutchinson 2023).

Misinformation was also more limited in the **UK**. While there had been widespread concern among policymakers and election observers about the potential flood of AI-generated misinformation, this scenario did not materialize. Originally, AI experts had warned that a deluge of AI-generated content would disrupt the election; however, many regarded this election as too obvious to manipulate. With the Labour Party's landslide victory being easily predicted, it was believed to be unnecessary to manipulate the results (Johnston 2024). However, even though the flood of false content was avoided, some cases of AI content were present in this election. A doctored video of Wes Streeting, a member of the Labour Party, showed him calling Diane Abbott, a fellow politician, a 'silly woman'. The video was spread on the platform X where it garnered tens of thousands of views, with the original poster admitting that the video had been edited. They had done so as a corrective measure, as politicians 'misrepresent who they truly are' (Spring 2024). This is simply one of many cases that took place during this election, a demonstration of the constant presence of misinformation, even in contexts where their creation has no impact on electoral outcomes, requiring constant vigilance.

Similarly, in **Pakistan**, former Prime Minister Imran Khan employed a voice clone to deliver speeches from prison, while in **Japan**, independent Tokyo gubernatorial candidate Takahiro Anno relied on an AI avatar to respond to more than 8,600 voter questions, ultimately placing fifth out of 56 contenders. Although these legitimate applications can broaden voter engagement, streamline campaign outreach and overcome logistical challenges, they also raise concerns about accuracy, transparency and data privacy.

Several states in the **USA** have already enacted laws regulating AI in political advertising, while others are in the process of doing so (AXInsights 2024). Yet, policy discussions often predominantly focus on mis- and disinformation without necessarily acknowledging how AI can blur the line between legitimate campaign marketing and deceptive image-polishing. To ensure ethical and transparent use of AI, it is essential to monitor these types of uses in political campaigns, track and label AI-generated content, address emerging risks and, if needed, fill any regulatory gaps.

Policy discussions often predominantly focus on mis- and disinformation without necessarily acknowledging how AI can blur the line between legitimate campaign marketing and deceptive image-polishing.

Even in cases with robust frameworks in place, as in the case of **Brazil**, critical risks pertaining to AI-generated content in political advertising remain overlooked, an issue that remains within the EU's current approach.

During the 2024 election cycle in the **EU**, the only rules that were present with a focus on AI were, on the one hand, the Guidelines on Election Integrity stemming from the DSA (European Commission 2024a), which contained indications to limit the spread of AI-generated content on social media platforms, and on the other hand, the Code of Conduct for political parties signed ahead of the EU elections and developed by International IDEA. Both tools, however, heavily rely on voluntary commitments (European Commission 2024b).

The new binding **EU** rules on AI, the AI Act, were not yet in force and not applicable. Even if they were, however, the AI Act does not seem protective enough when it comes to electoral integrity, as it is very difficult to include any sort of AI application related to elections in either the prohibited or the high-risk category (EPD n.d.) due to the very narrow definitions which would de facto exclude most AI systems used in the context of elections from the scope.

Some AI applications used in the context of elections, such as systems for voter data analysis and predictive analytics to perform microtargeting, could feed into the scope of prohibited AI applications, in particular under article 5.1a on subliminal techniques and article 5.1b on exploiting vulnerabilities to distort the behaviour of a person. The requirements to meet for that are, however, very strict, for example when it comes to the proof of 'significant harm' and the causal link between the system and the harm. Recently published Guidelines on Prohibited AI Practices also do little to address and clarify these issues (European Commission 2025a).

Furthermore, in Annex III 8b, AI systems linked to elections[7] are explicitly mentioned as high risk, but only if they are ‘intended’ to be used to influence elections and are not only organizational tools. This would leave out even some AI systems that would naturally be included (e.g. AI systems used for microtargeting political ads or AI systems used to generate deepfakes), as it is very hard to prove the intentionality of a system that might have uses other than influencing elections.

Finally, rules for GPAI applications also don’t explicitly consider AI used to influence elections, and the current work on the Code of Practice on General Purpose AI, which will complement the rules contained in the AI Act, is also not focusing on expanding risk assessment obligations to GPAI systems used in the context of elections.

As in other frameworks, implementation and enforcement will also be crucial to guarantee an expansive interpretation of the text, which includes AI systems used in the context of elections and putting the rules into practice effectively.

RECOMMENDATIONS FOR THE EU

The European Commission and AI Office should expand on the interpretation of the AI Act to include AI systems used to influence elections:

- AI systems used to influence elections should be either taken into account as high risk in the AI Act or as prohibited systems, as previously pointed out (EPD n.d.).

- Stronger protections should also be required for GPAI systems used in the context of elections as part of the GPAI Code of Conduct.

[7] ‘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 whose output natural persons are not directly exposed to, such as tools used to organize, optimize and structure political campaigns from an administrative and logistic point of view.’

2.3. DO NOT RELY SOLELY ON SOFT LAW APPROACHES

Box 2.3. Key takeaways

Non-binding instruments and soft law can complement and enhance regulatory frameworks and their enforcement, particularly in early or experimental stages when consensus on effective solutions has not yet emerged. These approaches are valuable for testing new regulatory ideas, shaping best practices and guiding initial responses. However, due to their lack of enforceability, they become insufficient once risks are well understood, especially in high-stakes areas such as elections and civic discourse.

Globally, some jurisdictions—such as Brazil or the EU—are moving towards binding legislative frameworks—for example, to govern AI and its applications for elections and election campaigns or for online platforms more broadly. Conversely, many countries still predominantly rely on soft law instruments such as public-awareness measures and guidelines.

The continued reliance on soft law in several jurisdictions and its lack of enforceability, and with that the critical outcomes of elections, shows that in places like the EU with strong democratic institutions, the way forward would be to prioritize binding rules in critical areas such as electoral integrity, civic discourse and online advertising. While soft laws retain value in informing and supplementing binding measures, the EU should clearly transition towards enforceable regulations to effectively address known risks. Thus, recommendations for the EU should emphasize binding legal frameworks as central, complemented—but not replaced—by targeted soft law measures where appropriate.

Many countries around the world have chosen a soft law approach to many issues linked to digital policy. For example, during **India**’s April–June 2024 general election, the Election Commission issued a non-binding advisory instructing all recognized political parties to remove AI-generated deepfakes within three hours and to warn the individuals responsible. The advisory expanded the previously established voluntary Model Code of Conduct—which established practical guidelines of dos and don’ts for leaders and parties ahead of elections—to emerging technologies, steering campaign behaviour without creating new legal obligations (Election Commission of India 2024; Indian Express 2024). **Mexico**’s Secretary of State provides a case in point: in May 2024, facing the threat of AI-driven misinformation, authorities launched a statewide campaign titled ‘Seeing is no longer believing’. Running across social media, television, radio and billboards, it aimed to educate voters on deepfake risks and offered practical resources like an AI quiz and one-page guides on identifying manipulated content.

Box 2.4. **Terminology**

Soft law involves norm-setting documents—such as guidelines, codes of conduct or recommendations—issued by public bodies or institutions to influence behaviour without imposing legal obligations. In contrast, public education campaigns represent policy tools or implementation strategies aimed at informing, influencing or empowering the public, rather than setting formal standards or norms.

While the **EU** has adopted several binding rules for digital platforms, some of the new EU digital rules linked to elections—including disinformation, spread of AI-generated content and deepfakes—also rely on the risk mitigation measures that VLOPs should adopt according to article 35 of the DSA after assessing systemic risks for civic discourse and electoral processes under article 34 of the DSA. To encourage companies to adopt relevant measures for preventing incidents during elections, the European Commission has also published guidelines on this very topic, giving an indication of which mitigation measures should be adopted (European Commission 2024a).

Since they are a soft law instrument, it is unclear how the guidelines could actually be enforced, and they leave the adoption of suitable mitigation measures to the discretion of the VLOPs (EPD 2024). At the same time, while the obligation to perform risk assessments would not classify as soft law, it also relies heavily on VLOPs proactively assessing risks and putting forward mitigation measures—with little scrutiny from the Commission's side, apart from monitoring the risk assessment exercise, providing feedback and opening investigations if needed. If an investigation proves that the risks were not properly assessed or that the mitigation measures were not suitable to address them, the Commission can impose fines. This is, however, a very long procedure, and some of the allegations would be difficult to prove given the lack of data available on the functioning of some of these platforms. The risk assessment reports have already proved to be lacking fundamental details, and the Commission would have to repeatedly use the requests for information (RFIs) from the DSA to obtain the relevant data for the investigations, slowing down the process even more significantly (Calabrese 2025). Overall, it seems that it would be better for these structures to serve as an ex-post remedy, rather than a deterrent—which is particularly problematic in areas such as elections and civic discourse, where prevention is crucial.

A Code of Conduct for political parties was also signed by European political parties ahead of the EU elections, with voluntary commitments by the parties to upholding ethical and fair campaign practices, including for the use of AI-generated content and online political campaigns (European Commission 2024b). This code, however, once again lacks enforcement mechanisms and depends on self-regulation.

Other crucial areas, such as online advertising regulation, are also currently left to soft law. The way the online advertising business model works is at the core of many issues that are faced online, such as the spread of disinformation, hate speech and extremist content. Most online platforms rely primarily on selling placement for online advertising as their source of revenue. As a consequence, their recommender algorithms tend to amplify content that creates more engagement, hence driving more traffic to the online ads that are placed on their platforms. As content that creates more engagement is often the most polemic and controversial, this tends to enhance the spread of disinformation, hate speech and extremist content.

Soft law, such as codes of practice, often give too much discretion to powerful actors, such as online platforms, who have no incentives to change the status quo. This is particularly unsuitable when those rules are about addressing the root causes of the spread of disinformation and reforming the very core business model of online platforms, which relies on online advertising.

Soft law, such as codes of practice, often give too much discretion to powerful actors, such as online platforms, who have no incentives to change the status quo.

In this context, while there are transparency rules on online advertising in the DSA, other initiatives pertaining to demonetizing disinformation through online advertising and putting forward possible alternatives to the current business model are delegated to voluntary codes of practice. Companies can freely decide to sign these or not, and even when they do, such codes of practice have weak to no enforcement mechanisms.

RECOMMENDATIONS FOR THE EU

The European Commission should complement legislation with soft law approaches such as literacy—as in Mexico's example—codes of conduct or strategic communications campaigns:

- The European Commission's DSA enforcement team should require that tools such as the risk assessment reports are actually being used to their full potential by platforms. If that's not the case, investigations should be open and fines should be given for non-compliance.

- The Guidelines on Election Integrity should be closely linked to DSA enforcement and the risk assessments exercise to make their content fully actionable and effective (see European Partnership for Democracy 2024).

- Online advertising regulation should complement code of conducts by issuing binding rules, as the way the online advertising business model works is at the core of many problems that are faced online, such as the spread of disinformation, hate speech and extremist content.

2.4. EXPLORE ADDITIONAL ISSUES AND TRENDS

Box 2.5. Key takeaways

New issues and trends related to the technology world are rapidly emerging, often raising new regulatory challenges.

Observing the global trends that have emerged in the 2024 elections reveals gaps even in the existing EU framework, particularly around topics such as the role of private messaging in influencing elections, the growing use of influencers for political ad campaigns and the increasing complexity surrounding money flows in digital campaigns. Some of these topics have become increasingly central in the EU in recent months, while others may require further impact assessment to understand whether new legislation is warranted.

In the lead-up to **India**'s 2024 elections, like in the previous elections, private messaging apps again emerged as a powerful yet often overlooked channel for political communication. Platforms like

WhatsApp—ranked second only to YouTube for news consumption in India, according to the Reuters Institute Digital News Report 2023—are used to circulate hate speech and disinformation (Newman et al. 2023). Telegram, along with Facebook Messenger and Signal, are popular news sources, and reach millions of users and play a growing role in shaping political narratives. On the one hand, some platforms like Telegram have significant gaps in content moderation and lack adequate safety guardrails. On the other hand, they often also operate as 'closed' systems through end-to-end encryption and are, hence, especially difficult to monitor, analyse and regulate.

It is important to note the dual practicality of these messaging apps. The privacy they offer has enabled hateful speech and illegal content to prosper, as these apps' encryptions allow users to avoid consequences for the content of their messages. However, many have found these apps to be building blocks for important political movements, sharing data between journalists, aiding in democratic movements and even protecting whistleblowers (Monaghan 2022).

India's experience with private messaging during the 2024 elections highlights both the growing influence of these 'closed' digital ecosystems and the regulatory challenges they pose. Encryption plays a critical role in safeguarding fundamental rights, particularly the right to privacy and freedom of expression, which are indispensable for journalism, the protection of journalistic sources and building resilience against disinformation. Yet, there remains limited consensus—academically or politically—on whether legal restrictions, technological interventions or a balanced combination of both can effectively reduce the spread of hate speech and misinformation without weakening encryption. Rather than viewing encryption as an insurmountable obstacle, policymakers can explore alternative recommendations such as introducing friction points to limit virality and enhance accountability without compromising encrypted communication. As private messaging increasingly supersedes open social media as a central arena for political communication, addressing these policy implications thoughtfully and carefully becomes more vital than ever (Forum on Information & Democracy 2020).

In **South Africa**'s 2024 general elections in May, the already complex landscape of online influence was further disrupted by the rise of so-called 'cyber troops' (Sekati 2023). These government or political party actors exploited social media to manipulate public opinion and, in particular, undermine electoral institutions and processes. In addition, paid digital influencers—including some approached by external actors—leveraged their own brands and the trust they had built with their audiences to sway behaviour (Allen and le Roux 2024).

Notably, very similar tactics have been observed in other countries, including **Indonesia** (Lamb, Potkin and Teresia 2024) and **India** (Mollan 2024), highlighting what may be an emerging global trend, and one that current EU legislation is not fully equipped to address. Many of these manipulative strategies hinge on political finance issues—such as undisclosed campaign expenditures and hidden funding sources—raising questions about whether existing regulatory frameworks can effectively safeguard electoral integrity across different jurisdictions (International IDEA 2024).

In the USA, discussions have been heating up around enforcing the disclosure of campaign influencer payments on social media. Influencer posts often evade formal labelling requirements, making it hard to track who is behind them.

Similarly, in the **USA**, for example, discussions have been heating up around enforcing the disclosure of campaign influencer payments on social media—an increasingly popular campaign tactic. Influencer posts often evade formal labelling requirements, making it hard to track who is behind them. Furthermore, there is no comprehensive regulation forcing purchasers of online ads to disclose their funding sources. Although super political action committees must disclose donors, many groups effectively function as 'dark money' organizations when the origins of their funding remain hidden. Combined with limited Federal Election Commission (FEC) enforcement power, these shortcomings can obscure who is financing political messages, leaving voters without the information they need to make informed choices (International IDEA 2024).

While in the **EU** issues linked to direct messaging have not been covered under the DSA, the issue of influencers promoting the political content of political candidates has become more prominent since the incident during the **Romanian** elections, where ads by influencers for candidate Călin Georgescu were not self-declared as political and not identified as such by TikTok, as required by Romanian law. While the Political Ads Regulation and the DSA should ideally cover this kind of political advertising as well (e.g. article 3(r) of the DSA states that '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'), questions remain as regards its scope and whether platforms will be able to identify influencers' content as political ads. On the one hand, the mitigation measures to address risks for civic discourse and electoral processes (including the risks related to targeted advertising and political advertising campaigns online) under the DSA have already proved limited or insufficient, in particular when it comes to the disclosure of influencers' activities being paid political ads and transparency around the funding sources (Pina 2025). On the other hand, the Political Ads Regulation, which will enter into application in October 2025, mandates strict transparency requirements for political ads online. However, without efforts from the platforms to identify influencers' content as political ads and provide the possibility of declaring it as such, influencers' paid political activities could be considered outside of the scope, and simply the personal opinions of individuals.

Without efforts from the platforms to identify influencers' content as political ads and provide the possibility of declaring it as such, influencers' paid political activities could be considered outside of the scope, and simply the personal opinions of individuals.

More broadly, enforcement of such rules remains a major concern (Calabrese and Virah-Sawmy 2025). While the new EU digital legislation (DSA, AI Act, Political Ads Regulation) tries to make Big Tech companies accountable, they have already put in place a series of strategies to avoid compliance with the new rules (Calabrese and Virah-Sawmy 2025), such as putting pressure on the US administration to weaken DSA enforcement in the EU, reinforcing the narrative that the DSA is a censorship law and withdrawing essential services from the EU, like Google's and Meta's decision to stop providing political advertising services (Kroeber-Riel 2024; Meta 2025). Furthermore, they have already clearly stated that they do not agree with the philosophy behind these rules and try to portray them as an undue restriction on free speech. For example, X has refused to provide access to relevant data under the DSA right to access research data (Democracy Reporting International 2025) and Meta changed its content moderation policies while knowing that they are potentially infringing the new EU rules (Kaplan 2025). With the backing of the current US administration, the situation is also unlikely to improve in the coming years and might require more stringent safeguards as well as enhanced oversight mechanisms in order to maintain respect for democratic values in the online sphere. These worries about this administration were present during Trump's campaign due to his stance on censoring speech, which went against the values of his own party. These fears were further exacerbated by many of the actions taken by the Trump administration, such as when Trump appointed Andrew Ferguson to the Federal Trade Commission. This poses a large threat to free speech, as Ferguson has been vocal about his belief that tech companies have been censoring conservative speech, which he plans to combat. This would range from using antitrust laws to go after these tech companies, and to target online speech specifically related to gender-affirming care, LGBTQIA+ issues and abortions (Benson 2025).

RECOMMENDATIONS FOR THE EU

The European Commission should explore new issues such as the role of direct messaging and influencers.

Direct messaging services:

- Evaluate the role of closed messaging services (e.g. WhatsApp, Telegram, Signal) in hate speech, spreading disinformation and election manipulation.
- Assess whether and how these services could be included in future EU regulatory frameworks without undermining encryption and privacy protections.
- Use findings to develop proportionate measures balancing fundamental rights protections and democratic credentials such as electoral integrity.

Influencer participation in campaigns:

- Clarify the legal status of influencer-driven political content and assess whether such activities can be covered by the Political Ads Regulation and the DSA.
- Take appropriate measures to mitigate harms arising from paid or in-kind political endorsements by influencers, such as standardized disclosure labels and enhanced transparency requirements across all major platforms.

Digital political finance gaps:

- Close loopholes in political finance rules for online campaigning.
- Adapt existing political finance regulations to cover payments to influencers, the use of proxy networks (e.g. cyber troops that illicitly amplify political messaging) and opaque funding streams in digital campaigning, to ensure transparency and accountability in digital political campaigns.
- Clarify enforcement responsibilities across member states.

Combating monetization of disinformation:

- Governments, digital platforms and political parties must curb the monetization of disinformation, stripping away the profits that fuel it. In the same vein, weak oversight of online political spending lets parties and candidates sidestep traditional campaign finance rules.

Therefore, the Commission should introduce binding measures to curb the ability of political actors and platforms to profit from false or harmful content—whether via ad revenue, engagement algorithms or paid promotion.
- Supplement voluntary codes with enforceable standards to prevent abuse.

Oversight and enforcement:

- Explore setting up oversight and coordination mechanisms—drawing on existing EU and national bodies—to share intelligence and align responses during election periods.
- Encourage timely information-sharing among relevant authorities, platforms and civil society actors to support consistent application of EU rules.

2.5. **ACKNOWLEDGE AND TACKLE THE (OFFLINE) ROOT CAUSES OF ONLINE ISSUES**

It is important to recognize that the same root causes of threats in the offline world, such as political influence and power, financial interests and economic dominance, inevitably manifest online (see, e.g., Bradshaw and Howard 2019). Therefore, regulatory frameworks that effectively address challenges in traditional electoral processes—ranging from political advertising standards to information dissemination—must also be applied, or newly created, with equal rigour for the digital context. When these offline standards are not upheld online, critical vulnerabilities can emerge that could ultimately undermine electoral integrity.

A key example of this phenomenon is digital political advertising. In the 2024 US federal elections, online ads played a growing role in every cycle, revealing gaps in current rules designed for offline campaign messaging (Wright 2024; AXInsights 2024). In 2023, shortly before the US elections, the Honest Ads Act (HR 2499) was reintroduced in the House of Representatives to address precisely these issues.[8] The legislation aims to block foreign entities from meddling in US elections and promote greater transparency in digital political advertising. If enacted, it would have extended existing disclaimer requirements—already in place for television, radio and print ads—to online ads, establishing parity between

[8] <https://www.congress.gov/bill/118th-congress/senate-bill/486>.

Box 2.6. **Key takeaways**

Addressing disinformation, hate speech and election manipulation exclusively with rules for online platforms is not enough. It is important to acknowledge and tackle the offline root causes of (electoral) disinformation, polarization and other online issues, such as business models that incentivize disinformation, monopoly power held by Big Tech companies, distrust in politics, crisis of traditional media and unclear party funding.

As currently recommended by UNESCO, important policies which prohibit the dissemination of false information with the intention of influencing the conduct and outcome of an election by regulating digital platforms include data protection, content moderation, labelling of political ads and eliminating AI-generated content (UNESCO 2023). However, what is targeted is often the symptom rather than the root cause, as the aforementioned policies tackle the harmful uses of digital platforms post use. These legal tools remain greatly necessary but must be implemented at earlier stages of this process to bring deeper structural impacts such as reducing polarization and distrust.

The EU has made significant progress in regulating the online sphere over the past five years, but these efforts must be complemented by stronger action to address the offline root causes of disinformation and democratic backsliding.

Furthermore, the monopoly power held by Big Tech companies needs urgent attention, especially given its significant impact on information integrity. Their surveillance-based business models (Amnesty International 2022) and dominance in AI infrastructure allow these corporations to evade meaningful accountability and transparency. The narrative of being ‘too big to regulate’ is partly addressed through initiatives such as the EU’s Digital Markets Act (DMA) and its interoperability measures. Pro-competitive solutions, as proposed by organizations like Article 19, have the potential to reduce the dominance of gatekeepers, facilitating market entry by new actors, fostering innovation and decentralizing informational control. Tackling this concentration of power within Big Tech is essential for building a healthier and more resilient digital ecosystem (Article 19 2023).

offline and online campaign regulations. Additionally, it would have empowered the FEC with broader authority to oversee digital content. Platforms with at least 50 million monthly users would have been obliged to keep a publicly accessible record of all election-related ads purchased by any individual or group spending more than $500, thereby strengthening transparency. Despite these ambitious goals, the Act was still only a proposal during the 2024 presidential elections and has only since moved to the Senate’s Committee on Rules and Administration for further review. Although the bill remained in committee during the 2024 presidential campaign, it showcases an effort and the importance of adapting long-standing offline safeguards to the digital sphere to ensure that election regulations keep pace with the technologies now shaping political communication.

In the meantime, updated FEC rules for Internet-based political communication—effective 1 March 2023—tried to narrow some of these loopholes. They broadened definitions and mandated that disclaimers be ‘clear and conspicuous’, making them visible to users without further action. Nonetheless, online ads still lack the ‘stand-by-your-ad’ feature required for radio and television, meaning candidates are not obligated to personally endorse their online advertisements. Moreover, the FEC continues to allow certain exceptions, which creates potential grey areas that could be exploited.

This example illustrates how threats originating in offline arenas can migrate online, underscoring the need for aligned legal standards across both spheres. Until there is comprehensive regulation that fully extends offline safeguards to digital platforms, and until legislation like the Honest Ads Act is adopted and implemented, online environments will remain more susceptible to the very dangers that regulators have long tried to contain in traditional media.

Until there is comprehensive regulation that fully extends offline safeguards to digital platforms, online environments will remain more susceptible to the very dangers that regulators have long tried to contain in traditional media.

Recent developments—including those in **Romania**—demonstrate how opaque or unchecked funding streams can enable both domestic and foreign actors to fuel political discourse with disinformation. The monetization of harmful content, monopoly power of Big Tech companies and lack of transparency around content monetization policies can undermine election integrity and democratic processes (Whattofix 2025). Therefore, it is crucial to establish more robust mechanisms to detect and address foreign funding intended to influence elections and ensure that regulators have the necessary tools and cross-border cooperation protocols to prevent the monetization of disinformation.

Overall, disinformation is not a digital phenomenon, as research indicates that the rise of disinformation and misinformation is closely tied to political factors, particularly the rise of radical-right populism (Törnberg and Chueri 2025). This political movement often seeks to undermine democratic institutions and legitimacy in order to gain electoral advantages from a misinformed electorate. Moreover, the groups most likely to consume and share disinformation frequently exhibit low trust in institutions or hold strong partisan identities (Törnberg and Chueri 2025).

Foreign interference has also emerged as a hot topic within the EU—especially regarding discussions on the European Democracy Shield and the recently published toolbox on Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI) (European Union External Action Service 2025). Proposed strategies to combat foreign election manipulation range from enhancing media literacy and fact-checking capabilities to strengthening regulations and improving institutional coordination.

EU policy responses and cross-national studies propose approaches that address offline root causes by reinforcing democratic institutions and societal resilience such as digital, media and information literacy (OECD 2024: 74–83; NATO Strategic Communications, Centre of Excellence 2024; Bateman and Jackson 2024). The OECD's Facts not Fakes framework lists 'fostering societal resilience' alongside transparency and governance reform, emphasizing that resilience entails 'addressing the root causes of crises while strengthening the system's capacity to cope with shocks' (OECD 2024: 3, 74–76). Likewise, Bateman and Jackson (2024) conclude that many drivers of disinformation stem from wider patterns of alienation, fear and economic insecurity, cautioning that platform rules alone risk treating only the symptom.

Many drivers of disinformation stem from wider patterns of alienation, fear and economic insecurity, cautioning that platform rules alone risk treating only the symptom.

Building on global experiences, it is clear also for the EU that combating dis- and misinformation requires a multidimensional approach that goes beyond technological solutions and addresses root causes of disinformation and hate speech such as monopoly power held by Big Tech companies, distrust in politics, the crisis of traditional media and unclear party funding (Calabrese and Reich 2024).

RECOMMENDATIONS FOR THE EU

Adopt a multidimensional approach that goes beyond technological solutions:

- Strengthening public trust, promoting civic education and reducing societal polarization are all crucial elements. While measures like content moderation and fact-checking partnerships have played a role in the recent 2024 election cycle (European Commission 2025b), they must be complemented by political and social interventions—such as media literacy programmes, initiatives to strengthen trust in institutions and additional funds to independent media. As civil society organizations are heavily underfunded but are expected to do a lot of heavy lifting, including literacy campaigns, fundamental rights assessments and so on, the EU should support such efforts through partnerships with civil society with targeted funding mechanisms as part of the new Multiannual Financial Framework, and integration of such objectives in the Democracy Shield.

- Address foreign interference as part of the Democracy Shield: The EU should develop a more comprehensive and resilient strategy to protect its democracy from foreign interference, for example as part of the Democracy Shield. In this context, measures such as strengthening institutional coordination, expanding independent media support or integrating foreign interference tracking into existing election monitoring frameworks should be taken into consideration.

Chapter 3

CONCLUSIONS

In the EU, many rules have been adopted in the area of digital policy over the past few years. However, as highlighted throughout this report, critical gaps remain in EU digital policy when it comes to addressing election integrity effectively.

The key risks identified in this report underline several priorities for EU policymakers:

1. The rules—the DSA, the DMA and the AI Act—are very young and still need to be properly implemented, enforced and interpreted at EU and national levels. However, enforcement agencies often lack the resources and technical expertise to keep pace with fast-changing technologies and particularly the global reach of dominant platforms, and their increasing influence not only on the market of ideas but also on global politics is making effective implementation and enforcement ever more crucial.

2. Weaknesses persist in the EU’s AI regulatory framework. Although the AI Act represents a significant step forward, its current provisions related to election integrity are insufficiently precise. Specifically, proving that AI has been used intentionally to influence elections under the Act’s current framework remains highly challenging. In particular, the AI Act does contain wording under the prohibited AI systems that might be linked to AI applications used in the context of elections, but the requirements for proving that are extremely strict. Similarly, the AI Act contains provisions considering AI systems ‘intended’ to be used to influence elections as high risk. Intentionality, however, is also very difficult to prove as most AI systems are not inherently designed to influence elections. Finally, provisions for GPAI systems do not explicitly consider AI applications used in the

context of elections. These rules would, therefore, benefit from additional clarifications and rules complementing the existing obligations.

3. Reliance on soft law limits effectiveness. While soft law and voluntary commitments have complemented the EU's regulatory approach, these alone lack sufficient enforceability to effectively hold platforms accountable.

   The monopoly power of major tech companies—including newer or rebranded platforms like X (formerly Twitter)—raises serious questions about content moderation, algorithmic transparency, and data access for regulators and researchers. Despite the DSA's provisions on transparency and accountability, platforms still enjoy considerable discretion in how they enforce their own rules. In many cases, the EU's legal framework relies on voluntary commitments (e.g. codes of practice) that are not as binding as lawmakers initially intended, which leaves critical decisions about content moderation and user data access largely in private hands. Any reliance on soft law instruments must be accompanied by clearly defined, enforceable standards, complemented by concrete enforcement mechanisms, ensuring platforms are held to account.

4. Rapidly evolving issues and emerging trends outpace regulators. Equally important is the fact that the tech environment continues to evolve rapidly**,** with shifts in ownership, policy or platform design happening more quickly than regulators can respond. Generative AI tools and evolving social media business models have already introduced new challenges to the detection of disinformation, raising concerns about whether existing measures can adequately address issues like deepfakes, synthetic media or hyper-targeted political messaging. Examples from around the world—including the growing influence of private messaging apps and the rise of 'cyber troops'—indicate that even more sophisticated tactics may emerge in the coming years.

5. Finally, it is essential to view many of these issues through a broader lens than just digital policy. Root causes of disinformation, hate speech and electoral manipulation are often found offline or embedded in structural societal and economic factors, such as polarization or lack of trust in institutions. Addressing digital-era challenges effectively requires a holistic approach that combines clear, enforceable regulations with

initiatives to foster media literacy, strengthen independent journalism and promote civic education.

Drawing on comparative insights from the 2024 super election cycle—particularly cases from Brazil, India and the USA—has highlighted both the global scale of these challenges and the diverse regulatory responses available. These examples demonstrate that, while the EU's digital policy framework is among the most advanced globally, it must remain agile and adaptive, continuously evaluating its approaches and learning from other emerging international experiences and challenges.

In conclusion, safeguarding electoral integrity in the digital age requires a holistic and coordinated effort. The EU's regulatory framework, while robust, needs targeted refinements and specification in the context of elections, clear enforcement and implementation standards, and systematic cooperation with stakeholders. Only by addressing these gaps through proactive, coordinated and comprehensive measures can the EU—and democratic societies more broadly—ensure resilient electoral processes capable of withstanding evolving digital threats and preserving democratic integrity.

References

Albert, J., ‘TikTok and the Romanian elections: A stress test for DSA enforcement, DSA Observatory, 20 December 2024 <https://dsa-observatory.eu/2024/12/20/tiktok-and-the-romanian-elections>, accessed 16 July 2025

Allen, K. and le Roux, J., ‘Under the influence? Online mis/disinformation in South Africa’s May 2024 election’, Institute for Security Studies, December 2024, <https://issafrica.s3.amazonaws.com/uploads/pages/1734073957062-sar-61.pdf>, accessed 4 June 2025

Alvarado Rincón, D. and Meyer-Resende, M., ‘Big tech is backing out of commitments countering disinformation: What’s next for the EU’s Code of Practice?’, Democracy Reporting International, 7 February 2025, <https://democracy-reporting.org/en/office/EU/publications/big-tech-is-backing-out-of-commitments-countering-disinformation-whats-next-for-the-eus-code-of-practice#WhatLiesAheadfortheCodeofPractice>, accessed 4 June 2025

Amnesty International, ‘What is Big Tech’s surveillance-based business model?’, 16 February 2022, <https://www.amnesty.org/en/latest/campaigns/2022/02/what-is-big-techs-surveillance-based-business-model>, accessed 4 June 2025

Article 19, *Taming Big Tech: A pro-competitive solution to protect free expression* (London: Article 19, 2023), <https://www.article19.org/wp-content/uploads/2023/02/Taming-big-tech-UPDATE-Jan2023-P05.pdf>, accessed 18 September 2025

Asplund, E., Bicu, I., Campion, S., Garnett, H. A., Harty, M., James, T. S., Olafsdottir, G., Pearce Laanela, T., Thalin J. and Vashchanka, V., *Review of the 2024 Super-Cycle Year of Elections Trends, Challenges and Opportunities* (Stockholm: International IDEA, 2025), <https://doi.org/10.31752/idea.2025.22>

AXInsights, ‘2024 Political campaign ads and their impact on the media landscape’, 6 September 2024, <https://insights.audiencex.com/political-campaign-ad-media>, accessed 4 June 2025

Barata, J. and Lazăr, E., ‘Will the DSA save democracy? The test of the recent presidential election in Romania’, TechPolicy.Press, 27 January 2025, <https://www.techpolicy.press/will-the-dsa-save-democracy-the-test-of-the-recent-presidential-election-in-romania>, accessed 4 June 2025

Barrett, P. M., Hendrix, J. and Richard-Carvajal, C., ‘Digital Risks to the 2024 Elections: Safeguarding Democracy in an Era of Disinformation’, Center for Business and Human Rights, February 2024, <https://drive.google.com/file/d/15OcDNADAMeJplFWIljDIvryd6ZNSN3J2/view>, accessed 4 June 2025

Bateman, J. and Jackson, D., *Countering Disinformation Effectively: An Evidence-Based Policy Guide* (Washington DC: Carnegie Endowment for International Peace, 2024), <https://policycommons.net/artifacts/11321569/countering-disinformation-effectively/12207375>, accessed 18 September 2025

Benson, T., 'How the Trump administration threatens internet freedoms', Al Jazeera, 14 January 2025, <https://www.aljazeera.com/economy/2025/1/14/how-the-trump-administration-threatens-internet-freedoms>, accessed 21 July 2025

Bradshaw, S. and Howard, P. N., 'The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation', 2019, <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf>, accessed 4 August 2025

Calabrese, S., 'Civic discourse and electoral processes in the risk assessment and mitigation measures reports under the Digital Services Act: An analysis', March 2025, <https://epd.eu/news-publications/civic-discourse-and-electoral-processes-in-the-risk-assessment-and-mitigation-measures-reports-under-the-digital-services-act-an-analysis>, accessed 17 September 2025

Calabrese, S. and Reich, O., 'Identifying, analysing, assessing and mitigating potential negative effects on civic discourse and electoral processes', Liberties, January 2024, <https://www.liberties.eu/f/mpdgy5>, accessed 4 June 2025

Calabrese, S. and Virah-Sawmy, R., 'Big Tech is avoiding responsibility – Here is what the EU can do about it', European Democracy Hub, 26 March 2025, <https://europeandemocracyhub.epd.eu/big-tech-is-avoiding-responsibility>, accessed 4 June 2025

CBS News, 'Miami Mayor Francis Suarez launches AI chatbot for presidential campaign', 6 July 2023, <https://www.cbsnews.com/miami/news/mayor-suarez-launches-an-artificial-intelligence-chatbot-for-his-presidential-campaign-3>, accessed 4 June 2025

Chatelain, R., 'OpenAI suspends company over Dean Phillips voice bot', Spectrum News NY, 22 January 2024, <https://ny1.com/nyc/all-boroughs/politics/2024/01/22/openai-suspends-company-over-dean-phillips-voice-bot>, accessed 4 June 2025

Christopher, N. and Bansal, V., 'How a secret BJP war room mobilized female voters to win the Indian elections', Wired, 30 July 2024, <https://www.wired.com/story/how-a-secret-bjp-war-room-mobilized-female-voters-to-win-the-indian-elections>, accessed 4 June 2025

Computer and Communications Industry Association (CCIA), 'State Content Moderation Landscape', [n.d.], <https://ccianet.org/wp-content/uploads/2022/11/CCIA_State-Content-Moderation-Landscape_2023.pdf>, accessed 4 June 2025

Democracy Reporting International, 'Court orders X to allow our research on the German elections', Democracy Reporting International, 7 February 2025, <https://democracy-reporting.org/en/office/EU/news/court-orders-x-to-allow-our-research-on-the-german-elections>, accessed 4 June 2025

Duffy, K., 'AI in context: Indonesian elections challenge GenAI policies', Council on Foreign Relations, 13 February 2024, <https://www.cfr.org/blog/ai-context-indonesian-elections-challenge-genai-policies>, accessed 4 June 2025

Election Commission of India, 'No. 491/SM_SOP/2024/Communication', 6 May 2024, <https://elections24.eci.gov.in/docs/2eJLyv9x2w.pdf>, accessed 18 July 2025

Electoral Commission of South Africa, 'African nations adopt groundbreaking digital and social media principles and guidelines for elections', [n.d.], <https://www.elections.org.za/content/About-Us/News/African-nations-adopt-groundbreaking-digital-and-social-media-principles-and-guidelines-for-elections>, accessed 4 June 2025

European Commission, ‘Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections’, 26 March 2024a, <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707>, accessed 4 June 2025

—, ‘Vice-President Jourová hosts signing ceremony of the Code of Conduct for the 2024 European Parliament Elections’, 9 April 2024b, <https://ec.europa.eu/commission/presscorner/detail/fen/ip_24_1867>, accessed 4 June 2025

—, ‘Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act’, 4 February 2025a, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>, accessed 4 June 2025

—, ‘Communication from the Commission to the Euro Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions’, 6 June 2025b, <2a7fddb2-e927-4079-92cc-4bb4279e9a46_en>, accessed 4 August 2025

European Digital Media Observatory (EDMO), ‘Final report: Outputs and outcomes of a community-wide effort’, 2024, <https://edmo.eu/wp-content/uploads/2024/07/Final-Report-%E2%80%93-EDMO-TF-EU24.pdf>, accessed 4 June 2025

European Digital Rights (EDRi), ‘From policy to practice: DSA implementation in focus across the EU’, November 2024, <https://epd.eu/news-publications/from-policy-to-practice-dsa-implementation-in-focus-across-the-eu>, accessed 4 June 2025

—, ‘EDRi files DSA legal complaint against X’, 20 March 2025, <https://edri.org/our-work/edri-files-dsa-legal-complaint-against-x>, accessed 4 June 2025

European Digital Rights (EDRi), Civil Liberties Union for Europe and cdt Europe, ‘Joint Civil Society Statement: Recommendations on the Implementation of the Regulation on Transparency and Targeting of Political Advertising’, 27 February 2024, <https://epd.eu/content/uploads/2024/02/Political-Advertising-Implementation-statement.pdf>, accessed 4 June 2025

European Partnership for Democracy (EPD), ‘Is election integrity integral to the Artificial Intelligence Act?’, [n.d.], <https://epd.eu/content/uploads/2024/07/Is-election-integrity-integral-to-the-Artificial-Intelligence-Act_-1-1-7.pdf>, accessed 4 June 2025

—, ‘How can the DSA Guidelines on Election Integrity be improved?’, European Partnership for Democracy, March 2024, <https://epd.eu/news-publications/how-can-the-dsa-guidelines-on-election-integrity-be-improved>, accessed 4 June 2025

European Union, 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) (Text with EEA relevance), *Official Journal of the European Union*, L 277/1, <http://data.europa.eu/eli/reg/2022/2065/oj>, accessed 18 September 2025

European Union External Action Service, ‘Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)’, 14 March 2025, <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en?utm_source=chatgpt.com>, accessed 6 June 2025

Farrugia, B., ‘Regulating the use of AI for Brazilian elections: What’s at stake’, DFRLab, 29 May 2024, <https://dfrlab.org/2024/05/29/regulating-the-use-of-ai-for-brazilian-elections-whats-at-stake>, accessed 4 June 2025

Forum on Information & Democracy, ‘Working Groups on Infodemics: Policy Framework’, November 2020, <https://informationdemocracy.org/wp-content/uploads/2020/11/ForumID_Report-on-infodemics_101120.pdf>, accessed 4 June 2025

Global Witness, ‘What happened on TikTok around the Romanian elections?’, 17 December 2024, <https://globalwitness.org/en/campaigns/digital-threats/what-happened-on-tiktok-around-the-annulled-romanian-presidential-election-an-investigation-and-poll>, accessed 16 July 2025

Hartmann, T., ‘Facebook and TikTok kill fake news story in Italy’, Euractiv, 7 June 2024a, <https://www.euractiv.com/section/tech/news/facebook-and-tiktok-kill-fake-news-story-in-italy>, accessed 4 June 2025

—, ‘Commission opens TikTok investigation over Romanian presidential elections disinformation’, Euractiv, 17 December 2024b, <https://www.euractiv.com/section/tech/news/commission-opens-tiktok-investigation-over-romanian-presidential-elections-disinformation>, accessed 4 June 2025

Hendrix, J., ‘Transcript: Mark Zuckerberg announces major changes to Meta’s content moderation policies and operations’, TechPolicy.Press, 7 January 2025, <https://www.techpolicy.press/transcript-mark-zuckerberg-announces-major-changes-to-metas-content-moderation-policies-and-operations>, accessed 4 June 2025

Hutchinson, A., ‘Hutchinson Campaign Press Release: Governor Hutchinson Unveils Interactive AI Interface Online by Gerhard Peters and John T. Woolley’, The American Presidency Project, 27 September 2023, <https://www.presidency.ucsb.edu/node/367507>, accessed 4 June 2025

Indian Express, ‘Model Code of Conduct comes into force for 2024 Lok Sabha elections: What does it mean?’, 18 March 2024, <https://indianexpress.com/article/explained/model-code-of-conduct-meaning-9217638>, accessed 4 June 2024

International IDEA, *Political Finance in the Digital Age: A Case Study of the United States* (Stockholm: International IDEA, November 2024), <https://doi.org/10.31752/idea.2024.90>

Institute for Strategic Dialogue (ISD), ‘Updated social media policies related to elections in the US’, June 2024, <https://statesunited.org/wp-content/uploads/2023/08/SUDC_Updated-Social-Media-Policies-June-2024-3.pdf>, accessed 4 June 2025

Johnston, J., ‘Why Britain’s “deepfake election” never happened’, Politico, 27 September 2024, <https://www.politico.eu/article/britain-deepfake-election-never-happened-artificial-intelligence-online-content-misinformation>, accessed 4 June 2025

Kaplan, J., ‘More speech and fewer mistakes’, Meta, 7 January 2025, <https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes>, accessed 4 June 2025

Kroeber-Riel, A., ‘An update on political advertising in the European Union’, Google, 14 November 2024, <https://blog.google/around-the-globe/google-europe/political-advertising-in-eu>, accessed 17 September 2025

Lamb, K., Potkin, F. and Teresia, A., ‘Generative AI may change elections this year. Indonesia shows how’, Reuters, 8 February 2024, <https://www.reuters.com/technology/generative-ai-faces-major-test-indonesia-holds-largest-election-since-boom-2024-02-08>, accessed 18 September 2025

Meta, ‘2024 European Parliament post-elections report: Digital Services Act—Elections guidelines’, 21 November 2024, <https://transparency.meta.com/sr/european-parliament-report-2024>, accessed 4 June 2025

—, ‘Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation’, 25 July 2025, <https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu>, accessed 17 September 2025

Mollan, C., ‘Lok Sabha 2024: The influencers driving India’s big election’, BBC News, 5 May 2024, <https://www.bbc.com/news/world-asia-india-68920953>, accessed 4 June 2025

Monaghan, J., ‘Hate speech and the limitations of instant messaging apps’, Media Diversity Institute, 29 August 2022, <https://www.media-diversity.org/hate-speech-and-the-limitations-of-instant-messaging-apps>, accessed 16 July 2025

NATO Strategic Communications, Centre of Excellence, *Virtual Manipulation Brief: Hijacking Reality, the Increased Role of Generative AI in Russian Propaganda* (Riga: NATO Strategic Communications, Centre of Excellence, 2024), <https://stratcomcoe.org/publications/virtual-manipulation-brief-20241-hijacking-reality-the-increased-role-of-generative-ai-in-russian-propaganda/307>, accessed 19 September 2024

Newman, N., Fletcher, R., Eddy, K., Robertson, C. T. and Kleis Nielsen, R., *Reuters Institute Digital News Report 2023* (Oxford: Reuters Institute for the Study of Journalism, 2023), <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf>, accessed 4 June 2025

Office of Inspector General, Department of Homeland Security, ‘DHS needs a unified strategy to counter disinformation campaigns’, 10 August 2022, <https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-58-Aug22.pdf>, accessed 4 June 2025

Organisation for Economic Co-operation and Development (OECD), *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity* (Paris: OECD Publishing, 2024), <https://doi.org/10.1787/d909ff7a-en>

Paun, C., ‘Romania’s presidential front-runner Georgescu benefited from Russia-style booster campaign, declassified docs say’, Politico, 5 December 2024, <https://www.politico.eu/article/romanias-presidential-frontrunner-benefited-from-russia-style-booster-campaign-declassified-docs-say>, accessed 17 September 2025

Phillips, T., ‘US and 10 Latin American states reject Nicolás Maduro’s vote certification’, *The Guardian*, 23 August 2024, <https://www.theguardian.com/world/article/2024/aug/23/latin-american-states-and-us-reject-maduro-vote-certification-election-venezuela-supreme-court>, accessed 16 July 2025

Pina, R., ‘Covert Influence in the Digital Age: How Platforms Must Step Up Under the DSA, Liberties, 14 May 2025, <https://www.liberties.eu/en/stories/undue-influencers-covert-dsa/45400>, accessed 4 August 2025

Puyosa, I., Azpúrua, A. and Suárez Pérez, D., ‘Venezuela: A playbook for digital repression’, Digital Forensic Research Lab, July 2024, <https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf>, accessed 4 June 2025

Satrio, A., ‘Banning AI for political campaigns: The cultural traces in the Indonesian Constitutional Court decisions’, Verfassungsblog, 23 January 2025, <https://doi.org/10.59704/4814e56f847f921c>

Sekati, P., ‘The commodification of online influence: Addressing disinformation from cyber-troops during elections in South Africa’, ALT Advisory Insights 2023 (5), 12 December 2023, <https://altadvisory.africa/2023/12/12/the-commodification-of-online-influence-cyber-troops-during-elections-in-south-africa>, accessed 4 June 2025

Singer, F., ‘They’re not TV anchors, they’re avatars: How Venezuela is using AI-generated propaganda’, *El Pais*, 22 February 2023, <https://english.elpais.com/international/2023-02-22/theyre-not-tv-anchors-theyre-avatars-how-venezuela-is-using-ai-generated-propaganda.html>, accessed 4 June 2025

Singh, R., ‘From memes to AI: How digital tools reshaped India’s 2024 general elections’, Business Standard, 31 December 2024, <https://www.business-standard.com/elections/lok-sabha-election/2024-indian-elections-digital-campaigns-social-media-ai-124123100308_1.html>, accessed 4 June 2025

Spring, M., ‘Labour’s Wes Streeting among victims of deepfake smear network on X’, BBC News, 7 June 2024 <https://www.bbc.com/news/articles/cg33x9jm02ko> accessed 17 July 2025

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hall, J. and Kieran, ‘AI-Enabled Influence Operations: Safeguarding Future Elections’, The Alan Turing Institute/Centre for Emerging Technology and Security, November 2024, <https://cetas.turing.ac.uk/sites/default/files/2024-11/cetas_research_report_-_ai-enabled_influence_operations_-_safeguarding_future_elections.pdf>, accessed 4 June 2025

Törnberg, P. and Chueri, J., ‘When do parties lie? Misinformation and radical-right populism across 26 countries’, *International Journal of Press/Politics*, 0/0 (2025), <https://doi.org/10.1177/19401612241311886>

United Nations Educational, Scientific and Cultural Organization (UNESCO), ‘Guidelines for regulating digital platforms’, Internet for Trust, February 2023, <https://www.unesco.org/sites/default/files/medias/fichiers/2023/04/draft2_guidelines_for_regulating_digital_platforms_en.pdf>, accessed 21 July 2025

US Department of Justice, ‘Section 230: Nurturing Innovation or Fostering Unaccountability?’, June 2020, <https://www.justice.gov/ag/media/1072971/dl?inline=>, accessed 4 June 2025

Wells, I., ‘Overwhelming evidence Venezuela opposition won election – Blinken’, BBC News, 3 August 2024, <https://www.bbc.com/news/articles/cd1d10453zno>, accessed 16 July 2025

Whattofix, ‘Social Media Monetization 2025’, 2025, <https://drive.google.com/file/d/16albh0VSb2tj2_HabwylbZ0xz-8JB4fY/view>, accessed 4 June 2025

Wike, R., Fagan, M. and Clancy, L., ‘Global Elections in 2024: What We Learned in a Year of Political Disruption’, Pew Research Center, 11 December 2024, <https://www.pewresearch.org/global/2024/12/11/global-elections-in-2024-what-we-learned-in-a-year-of-political-disruption>, accessed 4 June 2025

Wolfs, W., *Political Finance in the Digital Age: A Case Study of the European Union*, International IDEA (Stockholm: International IDEA, 2024), <https://doi.org/10.31752/idea.2024.26>

Wright, D., 'If you've been seeing more pro-Harris ads online lately, here's why', CNN, 30 October 2024, <https://edition.cnn.com/2024/10/30/politics/democratic-digital-advertising-future-forward/index.html>, accessed 4 June 2025

About the authors

Sofia Calabrese is a Digital Policy Manager at the European Partnership for Democracy. Her work involves all topics at the crossroads between digital policy and democracy, with a strong focus on political advertising, online platform regulation and artificial intelligence. She previously worked as a consultant in the Brussels-based public affairs consultancy Grayling, focusing mainly on platform regulation. Other experiences include a Schuman Traineeship at the Cabinet of the President of the European Parliament. She holds a double master's degree in Italian and French Law from the University of Milan and the University of Toulouse.

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. Prior to joining International IDEA, she worked on issues related to democracy, the rule of law and constitutional rights at various institutions and international organizations, including the Permanent Representation of Germany to the EU, the European Parliament, and the Max Planck Foundation for International Peace and the Rule of Law.

About the Partners

European Partnership for Democracy

The European Partnership for Democracy is a network bringing together specialist organisations with a global remit to support democracy.

EPD works in different areas of democracy support, from youth participation to rule of law and from digital policy to election integrity, via its pillars of research, programmes and policy. As part of the policy pillar, EPD works closely with civil society partners, EU institutions, European governments and academia to promote policies inside and outside Europe that foster democratic societies and fundamental rights. This includes advocacy on foreign policy, digital policy, media freedom, online political advertising, the rule of law, citizen participation and inclusion in elections.

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>

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

European Partnership for Democracy
Rue Froissart 123-133
B-1040 Brussels
BELGIUM
+46 8 698 37 00
info@epd.eu
www.epd.eu

The 2024 global super election cycle put electoral integrity under unprecedented pressure. Across continents, rapid advances in digital technologies reshaped how campaigns were run, how information spread and how voters engaged. From AI-driven campaigns to disinformation and unregulated online advertising, rapid technological change exposed gaps in Europe's electoral policy framework and around the world.

This report analyses global lessons from the 2024 elections and offers a forward-looking roadmap for EU policymakers. It highlights structural gaps—such as legal fragmentation, weak enforcement mechanisms and the unregulated use of emerging technologies—and proposes practical steps for policymakers to refine, strengthen and future-proof the union's regulatory approach. Rather than focusing only on legislative fixes, the report calls for a coordinated and holistic strategy: robust law enforcement, complementary soft-law tools, and proactive offline interventions to strengthen and promote societal resilience.

ISBN: 978-91-8137-021-8 (PDF)