European Partnership for Democracy

ELECTION-WATCH.EU

The EU's Artificial Intelligence Act and its Impact on Electoral Processes: a Human Rights-Based Approach

Armin Rabitsch and Sofia Calabrese

SEPTEMBER 2024

Artificial Intelligence and Democracy

Table of Contents

Abstract

This practitioner paper focuses on policy innovations brought by the Artificial Intelligence Act (AI Act) of the European Union (EU). In particular, it analyses the implications of the new rules on the integrity of electoral processes and assesses how the EU intends to regulate AI systems that pose risks to elections. The authors explore which AI systems would be in the scope of the AI Act under the high-risk category as 'AI systems intended to be used for influencing the outcome of an election or referendum', and assess the main risks posed to freedom of information, privacy rights, the independence and secrecy of the vote, and overall, the integrity of elections. The findings build on the EU-wide Election Assessment Mission (EAM) of the citizen observer network of Election-Watch. EU and European Partnership for Democracy's workshop on identifying AI systems posing risks to election integrity and related mitigation measures under the AI Act. This paper addresses the key question of how the EU's AI Act can be implemented to protect the integrity of elections, privacy rights and the freedom of expression against the impact of interference – especially mal-intended – by AI-supported actors and systems. The purpose is to provide policy guidance to the European Commission (EC) and European legislators by proposing mitigating measures related to the main risks identified.

1. European Legal framework covering Artificial Intelligence (AI) in elections

The EU has actively worked to establish a comprehensive regulatory framework for the digital space, including AI, in anticipation of the absence of global AI regulations in the near future. Nevertheless, several resolutions by United Nations (UN) bodies have reaffirmed that "the same rights people have offline must be protected online"[1]. The International Convention on the Right to Civil and Political Rights (ICCPR Art.2, 25, 26) enshrines the right to non-discrimination and participation of vulnerable groups in public life and requires the prevention of attacks on them, and upholds the right to privacy (Art.17)[2]. The right to political participation not only requires freedom of expression but, as stated by the UN Human Rights Committee, it also presupposes that "(v)oters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind"[3]. The UN established a High-level UN Advisory Body on Artificial Intelligence last year and the UN General Assembly adopted a Resolution seizing the opportunities of safe, secure and trustworthy AI systems for sustainable development this year.

The EU, however, passed several landmark legislative acts to regulate the digital space surrounding elections, including the AI Act, the Digital Services Act (DSA), the Digital Markets Act (DMA), the European Media Freedom Act (EMFA) and the Regulation on the Transparency and Targeting of Political Advertising (TTPA), enhancing the broader fundamental rights and safeguards framework, ahead of the June 2024 European

[1] UN GA resolution of 27 June 2016 on the Promotion, protection and enjoyment of human rights on the Internet", A/HRC/32/L.20, par 1, as well as; UN HRC Resolution 20.8 of 5 July 2012 and 26/13 of 26 June 2014 on the promotion and protection of human rights on the Internet, HRC resolutions 12/6 of 2 October 2009 on freedom of opinion and expression HRC resolution 28/16 of 24 March 2015 on the right to privacy in the digital age, GA resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age and 70/184 of 22 December 2015 on the information and communications technologies for development, amongst others.

[2] ICCPR 1966

[3] Human Rights Council General Comment 25, para. 19; See also: OSCE Representative on Freedom of the Media & Election-Watch.EU Policy Paper on AI's Impact on Freedom of Expression in Political Campaign and Elections, April 2021.

Parliament (EP) elections[4]. The new European legislation to regulate AI in online campaigning and elections (DSA, TTPA, AI Act) as well as the General Data Protection Regulation (GDPR) are explained in greater detail in the below paragraphs for a better understanding of the possible overlap, existing frictions between fundamental rights and progressive technology, as well as the possible gaps and challenges in enforcement.

1.1 The Digital Services Act (DSA)[5]

The DSA, in force since November 2022, was directly applicable throughout the EU from February 2024. It sets a robust framework for digital platforms, compelling them to ensure user rights, address disinformation, combat hate speech, and promptly remove illegal content[6]. The DSA covers several areas related to AI in elections, focusing on ensuring transparency, accountability, and the integrity of electoral processes.

The new European legislation applies to all providers that offer services in the EU regardless of their place of registration and singles out Very Large Online Platforms (VLOPs) as well as Very Large Online Search Engines (VLOSEs), which are platforms with more than 45 million average monthly active users in the EU[7]. The enhanced transparency rules provide for online platforms to disclose the number of removal orders issued by national authorities as well as all notices about the presence of illegal content highlighted by trusted flaggers. Assigned Member State (MS) authorities called Digital Service Coordinators (DSC) are required to enforce the DSA in MS while for VLOPs and VLOSEs the EC will be the enforcement body. The EC can apply fines up to six per cent of the worldwide annual turnover in case of breach of DSA obligations, failure to comply with interim measures or breach of commitments, as well as apply periodic penalties up to five per cent of the average daily worldwide turnover for each day of delay in complying with remedies, interim measures, and commitments[8].

[4] See Election-Watch.EU 2024 European Parliament Elections Assessment Mission Final Report (forthcoming Sept. 2024)

[5] See Election-Watch.EU 2024 European Parliament Elections Pre-Election Assessment Mission Report, February 2024.

[6] See EP: EU Digital Markets Act and Digital Services Act explained, updated August 2023.

[7] EC press release to DSA, 25 April 2023.

[8] EC. The enforcement framework under the Digital Services Act, as from 17 February 2024.

The DSA also prohibits targeted advertising only for minors (those aged 18 years or under) and forbids the use of sensitive information, such as sexual orientation, religion, or ethnicity, and aims to significantly expedite the removal of unlawful content. The DSA (Articles 14 and 27) mandates VLOPs to provide transparency about their content moderation, including the main parameters used for their recommender system and options for users to modify or influence these parameters. Providers of intermediary services must include information on the measures and tools used for content moderation, including algorithmic decision-making, in their terms and conditions to enhance transparency in how AI systems are used to manage online content.

The DSA (Article 34 & Recital 82) also provides for systemic risks assessment to include actual or foreseeable negative effects on electoral processes and public security. The establishment of crisis protocols to address risks to public security is also foreseen in the DSA (Article 48). It further provides for safeguards to address any negative effects on the exercise of the fundamental rights enshrined in the Charter, in particular the freedom of expression and information and the right to non-discrimination; which could include significant disinformation campaigns during elections. These protocols involve coordinated actions among platforms, authorities, and other stakeholders to manage and mitigate the impact of such crises on electoral integrity.

The new European legislation requires all online platforms to publicly report on how they use automated content moderation tools, the tools' error rates, and information about the training and assistance they provide to their content moderators[9]. For the first time, unified criteria exist for what are known as notice-and-action procedures, which determine when and if online platforms should be held accountable for the dissemination of illegal content. VLOPs and VLOSEs must conduct risk assessments including on any actual or foreseeable negative effect on electoral processes and civic discourse and submit them to annual independent third-party audits.

To bridge the gap until the TTPA becomes fully in force, and in order to ensure the integrity and security during the EP electoral period, the Commission issued under the DSA, the Guidelines on the mitigation of

[9] AccessNow. The Digital Services Act: your guide to the EU's new content moderation rules, 17 March 2023.

systemic risks for electoral processes on 26 April 2024[10]. These measures aimed to create a safer and more transparent online environment, particularly during electoral periods, to safeguard democratic processes and ensure the integrity of public discourse.

1.2 The Regulation on the Transparency and Targeting of Political Advertising (TTPA)[11]

The EU Regulation on the TTPA[12] was drafted with the aim to enhance the transparency of political advertising and of AI-powered online campaigning[13], and to counter disinformation, as online news platforms are becoming increasingly important as the first source of news among EU citizens. While most of its provisions will take effect only in 2025, some limited elements were applicable already during the 2024 EP elections. The TTPA builds on the self-regulatory Code of Practice against Disinformation updated in 2022, which failed to solve many of the problems regarding political advertising, such as the lack of independent third-party oversight. The EU plans to incorporate the Code of Practice as a (non-binding) Code of Conduct against Disinformation as part of the DSA framework. Notably, X (formerly Twitter), an important platform for political debate, has withdrawn from the Code, and the EC has opened proceedings on whether X has breached the DSA[14].

The TTPA focuses on laying down obligations for providers of political advertising services, including the use of AI for microtargeting and amplification. Specifically, the regulation requires political advertisements to include clear information about their sponsors and the techniques used to target audiences, ensuring that citizens can identify political ads and understand why they are being targeted.

[10] DSA Art 35 on the mitigation of risk for VLOPs and VLOSEs. The European Commission in cooperation with DSCs, can issue guidelines in relation to specific risks, in particular to present best practices and recommend possible measures.

[11] See Election-Watch.EU 2024 European Parliament Elections Pre-Election Assessment Mission Report, February 2024.

[12] EC; Transparency and Targeting of Political Advertising Regulation Initiative.

[13] See also OSCE RFoM Policy paper on AI and freedom of expression in political competition and elections, 15 April 2021.

[14] In December 2023 the EC has opened formal proceedings to assess whether X may have breached the DSA.

The TPPA regulation (Chapter III) addresses the use of targeting and amplification techniques involving personal data, mandating that controllers provide additional information to help individuals understand the logic behind these techniques and the main parameters used. This includes the use of third-party data and additional analytical techniques, which often rely on AI technologies. Additionally, the regulation sets out transparency obligations for political advertising, such as retaining records of political advertising services, including financial details and sponsor identities, for five years. These records must be accessible to national authorities and accredited journalists but also to vetted researchers and CSOs, enhancing accountability and public scrutiny.

Various initiatives have been established to also safeguard the June 2024 EP elections against disinformation[15]. The EU East StratCom Task Force, identifies, analyses and assesses Foreign Information Manipulation and Interference (FIMI)[16] with the aim to facilitate a more targeted and effective response to FIMI to protect the EU's democratic processes, security and citizens[17]. The European Digital Media Observatory (EDMO) brings together organisations and experts as a European fact-checkers network. Among others, the Civil Society Organisation (CSO) network European Digital Rights (EDRi) monitors digital human rights, while the CSO DisinfoLab focuses on fighting disinformation.

1.3 The Artificial Intelligence Act (AIA)

The purpose of the AI Act (Article 1) is among others to ensure "a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights, including democracy, the rule of law and environmental protection, against the harmful effects of the AI systems in the Union". Adopted by the Council of the EU on 21 May 2024, the AI Act was published in the Official Journal (OJ) of the European Union on 12 July 2024. This date serves as the formal notification with the AI Act entering formally into force 20 days thereafter. According to the AI Act (Article 113) the prohibitions on unacceptable risk AI (Chapter I and Chapter II) will apply six months later, while notifying authorities (Chapter III Section 4), general purpose AI models (Chapter V), governance, confidentiality and penalties (Chapter VII & XII & Article 78 with the exception

[15] EP Resolution on the European Elections 2024, 12 December 2023.

[16] Speech by the High Representative/ Vice-President Josep Borrell, 23 January 2024.

[17] See also EP: Foreign interference in all democratic processes in the European Union, 2022.

of Article 101 (fines for General-purpose AI providers)) will apply after 12 months, and the rest after 24 months. Codes of practice must be published nine months after entry into force according to the AI Act (Article 56)[18].

The AI act was designed as a horizontal EU legislative instrument applicable to all AI systems placed on the market or used in the Union, based on Article 114 and Article 16 of the Treaty on the Functioning of the European Union (TFEU)[19]. The AI Act is part of the New Legislative Framework (NLF) system that aims to strengthen the internal market for goods based on existing systems and should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights, and product safety, to which this Regulation is complementary. Certain basic safety characteristics and essential requirements operationalised through technical standards apply[20].

The AI Act (Article 64) provides for the Commission to create the European AI Office to improve its knowledge and skills in AI and forms the foundation for a single European AI governance system. This office will be supported by the member countries of the EU, who will help it carry out its duties as outlined in the regulations.

The AI Act (Article 65) establishes a European Artificial Intelligence Board (the 'Board') composed of one representative from each MS. The European Data Protection Supervisor (EDPS) will participate as an observer, and the AI Office will attend meetings without voting rights. Other national and Union authorities, bodies, or experts may be invited to meetings when relevant. The Board's rules of procedure, including the selection process, mandate duration, Chair tasks, voting arrangements, and organisation, will be adopted by a two-thirds majority of Member State representatives. The Board will establish two standing sub-groups and additional sub-groups may be formed to examine specific issues, and representatives from the advisory forum may be invited as observers. A first high-level meeting of the upcoming AI Board took place on 19 June 2024.

Further, the AI Act (Article 67) establishes an advisory forum to provide technical expertise and advice to the Board and the Commission and

[18] AI Act Recital 179.

[19] EP EPRS AI Act Briefing, March 2024.

[20] EC DG CNECT, Risk management logic of the AI Act and related standards, 30 May 2024.

contribute to their tasks under this Regulation. The forum's membership shall represent a balanced selection of stakeholders, including industry, start-ups, small and medium-sized enterprises (SMEs), civil society, and academia, ensuring a balance between commercial and non-commercial interests, and within commercial interests, a balance between SMEs and other enterprises.

The EC has to appoint members from among stakeholders with recognised expertise in AI. Members will serve a two-year term, extendable by up to four additional years. Permanent members of the forum shall include the Fundamental Rights Agency, the European Union Agency for Cybersecurity (ENISA), the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI).

The forum will draw up its rules of procedure, elect two co-chairs from among its members for a two-year term, renewable once, and meet at least twice a year. It may invite experts and other stakeholders to its meetings, prepare opinions, recommendations, and written contributions at the request of the Board or the Commission, and establish sub-groups for specific questions related to the Regulation's objectives. The forum shall prepare an annual report on its activities, which will be publicly available.

Beginning of July 2024, CSOs, including Election-Watch.EU and EPD released recommendations for the AI Act advisory forum requesting guaranteed representation of righty-based and diverse expertise not limited to computer science, and to develop terms of reference for the forum and ensure a clear and transparent selection process with an equal number of members of CSOs as other types of stakeholders[21].

1.4 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), put into effect in 2018, regulates the collection, storage, and processing of personal data. It is an important component of EU privacy law and human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. Though it was drafted and passed by the EU, it also governs the transfer of personal data outside the EU, so long as they target or collect data related to people in the EU. The GDPR imposes robust data protec-

[21] Access Now, ECNL, ICCL Enforce, et al: Civil society recommendations for the AI Act advisory forum, July 2024.

tion obligations on the use of AI in elections and political campaigns for persons. These rights include the right to access their data (Article 15), the right to rectification (Article 16), the right to erasure ('right to be forgotten', Article 17), the right to restrict processing (Article 18), the right to data portability (Article 20), and the right to object to data processing (Article 21).

These rights ensure that individuals can control how their personal data is used by AI systems. The GDPR (Articles 7 & 12) mandates that consent must be freely given, specific, informed, and unambiguous, and that AI systems must be transparent about how personal data is used, ensuring that individuals are aware of how their data is being processed and for what purposes. The GDPR (Article 22) states that individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which is particularly relevant for AI systems in political campaigns that might profile voters to target them with specific messages.

When AI systems are likely to result in a high risk to the rights and freedoms of individuals, data controllers must conduct Data Protection Impact Assessments (DPIAs, Article 35). Further, the GDPR regulates the transfer of personal data outside the European Economic Area (EEA). AI systems used in political campaigns that involve cross-border data transfers must ensure that such transfers are made to countries with adequate data protection laws or are otherwise safeguarded by appropriate mechanisms, such as standard contractual clauses or binding corporate rules (Articles 44-50)[22].

2. The June 2024 European Parliament elections

In this chapter, the role of AI in the recent EP elections is analysed to better understand the level of AI used in political campaigns and elections. While in most MS the DSC was not yet fully operational and the AI Act has not been in force it provides examples of the use of AI tools in specific circumstances.

While AI will change the whole concept of political communications fundamentally, so far only two MS (EL, IE) have national legislation providing for the labelling of AI-generated content and require disclaimers, as

[22] See also EDPS Case Law Digest. From Lindqvist to Schrems II: case law of the CJEU on transfers of personal data to third countries, 2021.

underlined in Election-Watch.EU's Preliminary Statement[23]. According to its network of election observers and experts across the 27 MS only in seven MS was there any use of AI-generated content detected in online campaigning (DE, DK, ES, HR, IE, PT, SE).

In Germany, the most prominent case has been a deep fake video created by left-wing activists, which shows Chancellor Scholz calling for an Alternative für Deutschland (AfD) party ban. In general, however, politicians and groups associated with the AfD seem to be most likely to use deep fakes for their own purposes. One example is the mass sharing of deep fake audios with the aim of discrediting the public broadcaster TV (Tagesschau) news programme.

In Ireland, it was also evident that some fringe parties and candidates used AI-generated content extensively. For example, an analysis by DCU FuJo Institute found that The Irish People Party used AI-generated imagery to create posters and to give the impression of support from real people. For example, the party ascribes names, addresses, occupations, and supportive quotes to AI-generated images of people. More generally, AI has been used to create inflammatory images in relation to immigration and homelessness. Some of these images have attracted considerable commentary and have been debunked by TheJournal.ie according to a response by EDMO.

In Spain, the political party Ciudadanos unveiled an AI-generated campaign poster for the Catalan parliamentary elections, which took place four weeks ahead of the EP elections. The poster showed the former president of the Catalan government, Carles Puigdemont, who took refuge in Belgium six years ago, and Spanish Prime Minister, Pedro Sánchez, shaking hands,such a meeting never took place. The poster had the slogan "detenlos", which can be translated as "stop them" or "arrest them".

In Portugal, AI-generated content was mostly satirical or political memes, not clearly intended to deceive. The Digital Service Coordinator (DSC) in Bulgaria shared cases of fake information being used for the propagation of drugs or weight loss programmes using the identity of popular figures such as journalists but not for influencing the election campaign. This is similar in other MS like Austria, or Croatia, where the president, Zoran Milanović, who was not a candidate, appeared in several AI-generated

[23] Election-Watch.EU it will present its final report with findings and recommendations to strengthen European electoral integrity and to enhance democratic practices beginning of autumn 2024.

videos advocating for (scam) investments in the energy sector.

EDMO and in Czechia CEDMO fact-checkers stated that the share of disinformation created through AI in the total number of false news circulating in the public space is still relatively low at around 5 per cent. As part of a research project Democracy Reporting International (DRI) revealed that AI chatbots are less reliable than search engines in providing users with electoral information, as ChatGPT 3.5 & 4, CoPilot and Gemini responded to common questions about the European elections with some totally or partially incorrect answers.

3. Enforcement, necessary clarifications, and gaps

Until the full entry into application of the AI Act, the Digital Services Coordinators (DSC) and Digital Services Board will play a valuable role in the framework of the DSA – which also contains rules relevant to countering AI's impact on elections. However, the DSA was not transposed into relevant national legislation as in eleven MS (BG, CY, CZ, EE, ES, HR, IT, NL, PL, PT), or only partly transposed as in four MS (LT, LU, SK, SE) during the time of the June 2024 EP elections. The DSC was not yet appointed in five MS (BG, EE, LT, PL, SK). On 24 April, the EC took decisive action to hold MS accountable by opening infringement procedures against six MS (CY, CZ, EE, PL, PT, SK) for failing to appoint DSCs or provide them with sufficient powers and resources.

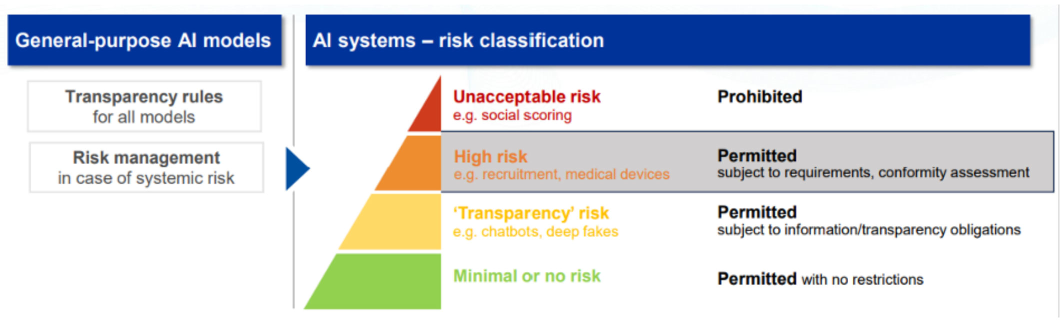
Furthermore, on 30 April, the EC initiated formal proceedings to investigate Meta on the following aspects: non-compliance with DSA obligations (including deceptive political advertising and disinformation), transparency of political content, election monitoring tools for researchers (with the main focus on the discontinuation of Meta's social media monitoring tool CrowdTangle and the lack of an adequate replacement ahead of the EP elections) and flagging illegal content. This is part of the broader effort to ensure the integrity of the upcoming European elections and to enforce the provisions of the DSA. On 15 August the Commission sent a further information request to which Meta must reply by 6 September 2024. Based on the assessment of the replies, the Commission will determine the next steps. However, there are no legal deadlines for concluding formal proceedings, even during the election period. The duration of an in-depth investigation depends on several factors, including the complexity of the case.

This paper analyses the impact of the AI Act on elections, considering the additional detailed EU implementing acts and guidelines arising from the

new EU digital space regulatory framework. Adopting a human rights-based approach to AI in elections, it emphasises protecting freedom of information, privacy rights, the independence and secrecy of the vote, and the overall integrity of elections. The paper provides policy guidance to the European Commission in preparing secondary legislation.
The AI Act specifies that "depending on the circumstances regarding its specific application, use, and level of technological development, AI may generate risks and cause harm to public interests and fundamental rights that are protected by Union law. Such harm might be material or immaterial, including physical, psychological, societal or economic harm."[24]

The EC has classified the risk of AI systems into four categories:

1. prohibited due to unacceptable risk, e.g. social scoring,
2. permitted high risk but subject to requirements and conformity assessment, e.g. recruitment,
3. permitted (limited) "transparency" risk but subject to information/ transparency obligations, e.g. chatbots, deep fakes
4. permitted minimal or no risk with no restrictions.



General-purpose AI models

Transparency rules
for all models

Risk management
in case of systemic risk

AI systems – risk classification

Unacceptable risk e.g. social scoring	Prohibited
High risk e.g. recruitment, medical devices	Permitted subject to requirements, conformity assessment
'Transparency' risk e.g. chatbots, deep fakes	Permitted subject to information/transparency obligations
Minimal or no risk	Permitted with no restrictions

Table 1: AI systems risk classification[25]

The AI Act's definitions indicate a broad approach to defining harm, encompassing various forms of physical, psychological, and societal impacts. The intent is to prevent AI systems from engaging in practices that can significantly damage individuals' well-being, exploit their vulnerabilities, or undermine fundamental societal values like fairness, non-discrimination, and democratic integrity.

[24] EU, AI Act, 14 May 2024, p.5.

[25] EC, DG CNECT, Risk management logic of the AI Act and related standards 30 May 2024

Article 5 Prohibited AI Practices (AI Act Article 5.1a & 5.1b)

1. The following AI practices shall be prohibited:

(a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

The AI Act mentions (Article 1 & Recital 1, 2, 8, 48, 62, 120, 136, Annex III) its objective of the protection of democracy and the rule of law as well as the protection of fundamental rights – as the right to vote and to stand as a candidate in elections to the EP - included in the Charter of Fundamental Rights of the EU (Article 39). The AI Act (Recital 48) also sets criteria to define high-risk AI systems, including among others the risks to harm fundamental rights, and notably the right to vote. However, the act does not mention several categories where AI systems that have an impact on elections could feed into.
AI systems that have the potential to influence elections might be considered under four different categories:

The AI Act mentions (Article 1 & Recital 1, 2, 8, 48, 62, 120, 136, Annex III) its objective of the protection of democracy and rule of law as well as the protection of fundamental rights – as the right to vote and to stand as a candidate in elections to the EP - included in the Charter of Fundamental Rights of the EU (Article 39). The AI Act (Recital 48) also sets criteria to define high-risk AI systems, including among others the risks to harm fundamental rights, and notably the right to vote. However, the act does not mention several categories where AI systems that have an impact on elections could feed into.

AI systems that have the potential to influence elections might be considered under four different categories:

1	**Prohibited AI systems**: Several provisions might be seen as implicitly including AI systems that might impact elections, namely the ones on subliminal techniques (Article 5.1a); exploiting vulnerabilities to distort the behaviour of a person (Article 5.1b); and categorisation of natural persons based on political opinions (Article 5.1g).
2	**High-risk AI systems according to Annex III (8b)**: AI systems potentially impacting elections are explicitly mentioned here as *"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."* Some possible examples could be: AI systems used to deliver political advertising, profile voters; including with microtargeting and amplification techniques; AI systems used to process or count voting ballots or maintain voting lists; AI systems used to identify cybersecurity attacks against IT systems allowing elections to take place; Chatbot-based AI systems to provide voter assistance; AI systems to perform voter data analysis and predictive analytics; AI systems used to counter biased content and for electoral content moderation. High-risk AI systems need to comply with a series of requirements included in Articles 8-15 of the AI Act. Most notably, Article 9 mandates that providers of AI systems establish a risk management system and related mitigation measures. As the article mentions risks posed to fundamental rights, this would include the right to vote as well.
3	**Limited risk AI systems**: Some of the systems mentioned in this category (Article 50), such as chatbots, deep fakes and general-purpose AI models could also have an impact on elections.

4	**General purpose AI systems posing systemic risks as outlined in Article 51**: This category could definitely be linked to elections because systemic risks are defined in Article 3 (65) as "*a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the internal market due to its reach, and with actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain.*" As the right to vote is a fundamental right under Article 39 of the Charter, some AI systems posing risks to elections could also be included under this category.

Overall, the AI Act provisions regarding the use of AI systems to influence elections open many questions regarding the nature of the systems in scope, as well as the assessment of risks and related mitigation measures. The main questions raised are the following:

1. Which AI systems posing risks to elections would be prohibited under the AI Act? How to identify specific use cases?
2. Which AI systems posing risks to elections would be high risk under the AI Act? How to identify specific use cases?
3. Could limited risk AI systems pose risks to elections? Would they be considered high-risk in that case?
4. What are the main risks posed by AI systems intended to be used to influence elections? What would be the most effective mitigation measures?

Answering these questions is crucial. Otherwise, on the one hand, relevant AI applications could be left out of the scope of the new rules, and on the other hand, rules could be misused against harmless AI applications. Some of these questions will also be addressed throughout the implementation, in particular with the Guidelines on high-risk and non-high-risk use cases on AI systems (under Article 6.5) and the Guidelines on prohibited practices referred to in Article 5 (according to Article 96.1(b)).

4. Recommendations

This Policy paper aims to provide guidance to the EC, the EP and regulators ahead of the envisaged implementing acts stemming from the EU's AI Act, especially in relation to transparency and accountability in AI's impact on elections.

While we have analysed the main risks of AI in elections, provided questions for discussions to feed into the upcoming guidelines on high-risk and non-high-risk use cases as well as on prohibited practices, and acknowledged the robust progress by the EU to regulate the digital space including of AI in elections with a human rights-based approach in mind, this document also underlines the need for further research, with a particular focus on:

1. AI systems posing risks to elections to be included in the AI Act's scope;
2. Main risks posed to election integrity by these systems, including privacy rights, secrecy of vote and freedom of information; and
3. Mitigation measures to these risks.

The following recommendations constitute a basis for discussion with key stakeholders, not only to mitigate the risks but also to ensure coherence and human rights compliance in the implementation of these acts in the context of elections. These recommendations are addressed to specific key actors in view of conducting specific validation workshops to ensure complementarity and ownership in the responsibilities to take. On the one hand, the European Commission is responsible for drafting the guidelines to further provide guidance on AI Act implementation and enforcement. On the other hand, CSOs which are key players in the process, as they are watchdogs, including a human rights-based approach, provide good practices and detect gaps in the implementation.

For the European Commission:

- Consider a moratorium for the use of AI systems in electoral campaigning to better understand the societal and political impact, given the rise of political forces questioning and/or undermining key democratic principles of established democracies.
- Draft provisions and guidelines on fundamental rights impact and risk assessments of the use of AI in electoral processes, to assess potential individual and societal harm.

- Elaborate the definition of individual/societal harm in elections given that one vote could make a difference in elections.
- Provide a definition and/or examples of the ‘significant harm’ concept, as per Articles 5.1a and 5.1b (see Annex), taking into consideration societal harm and financial loss.
- Clarify the link between the AI Act provisions with the DSA and the GDPR and the potential added value of the AI Act.
- Evaluate whether AI systems could be prohibited ex-post. The European Commission should also define ‘intentionality’ as part of Annex III 8b (see Annex) and clarify whether it would stem from the producer or from the user. In considering high-risk AI systems ‘intended’ to be used to influence elections, infer intentions from consequences, with a broad understanding of intention as due diligence rather than strict intentionality.
- Further examine specific AI applications in the light of Annex III 8b (e.g. microtargeting and ad delivery techniques) and related assessment approaches for election-related impacts.

For Civil Society Organisations:

- Provide the EC with examples and case studies to inform the guidelines that are being drafted on prohibited and high-risk systems. In particular, consider bringing forward examples of past incidents involving AI leading to real harm to help demonstrate the ‘significant harm’ under Articles 5.1a and 5.1b.
- Obtain more evidence on how certain potentially prohibited AI systems influence voting behaviours.
- Consider opportunities to feed into the debate, practice and body of knowledge around risk assessments and standards for high-risk AI systems related to elections.
- Develop and test good practice templates and examples of fundamental rights impact/risk assessment for the usage of AI in elections to protect and uphold the democratic process.

Annex: AI Act provisions relevant for elections

Recital 62: “Without prejudice to the rules provided for in [Regulation 2024/900 on the transparency and targeting of political advertising], and in order to address the risks of undue external interference to the right to vote enshrined in Article 39 of the Charter, and of adverse effects on democracy, and the rule of law, AI systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda should be classified as high-risk AI systems with the exception of AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistical point of view.”

Recital 120: “Furthermore, obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.”

Recital 136: “The obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation. The requirement to label content generated by AI systems under this Regulation is without prejudice to the obligation in Article 16(6) of Regulation 2022/2065 for providers of hosting services to process notices on illegal content received pursuant to Article 16(1) and should not influence the assessment and the decision on the illegality of the specific content. That assessment should be performed solely with reference to the rules governing the legality of the content.”

Annex III: High-Risk AI Systems Referred to in Article 6(2); 8. Administration of justice and democratic processes:

(a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts or used in a similar way in alternative dispute resolution;

(b) 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 organise, optimise and structure political campaigns from an administrative and logistic point of view.

European
Partnership for
Democracy

Cover image: © DedMityay
on Adobe Stock

Rue Froissart 123-133, 1040 Bruxelles

info@epd.eu | +32 2 733 2282

www.epd.eu