Bialystok Legal Studies
Białostockie Studia Prawnicze
2026 vol. 31 no. 1

sciendo

DOI: 10.15290/bsp.2026.31.01.07

Received: 09.06.2025
Accepted: 03.03.2026

Karolina Kiejnich-Kruk
Adam Mickiewicz University, Poland
kiejnich-kruk@amu.edu.pl
ORCID ID: 0000–0003–1551–5448

The AI Act: Challenges for Justice and Democracy in the Deployment of AI-Based Systems

Abstract: The entry into force of the AI Act will have a significant impact on the practices of both private and public actors. The Act identifies areas where there is a particularly high risk of the violation of fundamental rights, including the administration of justice and democratic processes. This article analyses the provisions of the AI Act for the use of AI systems in these areas, outlines the framework for their use and identifies the main risks to human rights. It considers the most important challenges arising from the AI Act in relation to justice and democratic processes, as well as the difficulties in interpreting the Act in this regard. It also proposes an approach that EU Member States can follow to adjust their national legal systems to meet these new challenges. It suggests that these challenges require a coherent process for the digitisation of justice that distinguishes between systems subject to high-risk AI regulation and those that can be implemented without such burdens. Regarding democratic processes, Member States must implement regulations that, first, promote transparency in the use of AI tools and, second, encourage cooperation with online platforms in monitoring them.

Keywords: AI Act, administration of justice, democratic processes, elections, artificial intelligence

Introduction

The Artificial Intelligence Act (the AI Act or the Regulation) (European Parliament and the Council, 2024) marks a significant milestone in the legal regulation of artificial intelligence systems in various social and economic sectors. It has a significant impact on both the private and the public sectors, including in relation to the administration of justice and democratic processes. Of particular relevance in this regard are its regulations concerning high-risk AI systems; the Act identifies these

areas as being particularly likely to give rise to human rights violations due to the use of AI technologies. Classifying a particular system into the appropriate category – prohibited, high-risk or not subject to these regimes – is crucial for the proper implementation and use of such a system. This is particularly important for safeguarding the fundamental rights of participants in the legal proceedings by implementing the right controls and minimising risks. Additionally, misclassifying a system may result in actors in the supply chain failing to comply with the obligations set out in the Regulation, which could lead to sanctions.

This article aims to analyse the provisions of the AI Act regarding the use of AI systems within the areas of the administration of justice and democratic processes, in order to outline the framework for their use and to detect the main risks to human rights arising from them. The paper presents an analysis of the most important challenges arising from the AI Act in the areas of justice and democratic processes, the difficulties in interpreting the Regulation in this regard, and the guidelines for EU Member States on possible policy directions for adapting their national legal frameworks to the identified challenges.

The first subsection of the paper outlines the reasons for categorising the above-mentioned areas as high-risk and the implications of this for public entities using AI systems in these spheres. The second subsection focuses on the administration of justice and considers the interpretation of the provisions of the AI Act in this domain, the challenges associated with the implementation of these provisions and the proposed national approach to emerging challenges. The third subsection provides an analysis of the provisions of the Act relating to democratic processes, the impact of new technologies on electoral processes, the risks involved and proposals for avoiding these risks. It also covers the tools currently available under EU law. The research is based on a formal analysis of the relevant legal norms. It also employs the dogmatic method, with a focus on the national and international literature on both the legal and the technical aspects of the use of AI systems in the areas of justice and elections.

1. High-risk AI systems: Requirements for public actors

A significant number of the AI systems used in the administration of justice and in democratic processes are considered to be high-risk. As indicated in Recital 61 of the Preamble of the AI Act, this is due to their potential impact on the rule of law, personal freedoms and the right to an effective remedy and access to an impartial tribunal. The aim of putting these systems in this category is to eliminate the potential risks of bias, error and the black-box effect (Brożek et al., 2024; Hassija et al., 2024). Therefore, while AI tools can support the independence of the judiciary or judges' decision-making processes, they should not replace them; final decision-making must remain a human-led activity. It is important to note that AI systems should not be

classified as high-risk if they are intended for purely ancillary administrative activities that do not affect the administration of justice in individual cases. Examples include systems used for anonymising or pseudonymising court decisions, documents or data, for communication between staff members and for administrative tasks.

Also, as indicated in Recital 62 of the Preamble, to prevent undue external interference with the right to vote, as well as any undesirable impacts on democracy and the rule of law, AI systems intended for use in influencing election or referendum outcomes or the voting behaviour of individuals should be classified as high-risk. The exceptions are systems which produce results that individuals are not directly exposed to, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view. Direct exposure therefore refers to the rights of individuals, including the right to vote, the right to privacy and the protection of personal data in the context of data analytics used to target media messages.

The legislation combines both the administration of justice and democratic processes into a single legislative unit, due to the same category of rights and values being at risk as a result of AI systems being used in these areas. These can be referred to collectively as 'country governance'. As indicated in the Preamble, the rights and values in question are democracy, the rule of law, individual freedoms and the rights to an effective remedy and to a fair trial.

Putting a system into the high-risk category has significant implications. Such systems occupy a central position in the Regulation; they have been given the most attention, and it has been recognised that they require specific regulation. The broad aim of the Regulation is to monitor, prevent and minimise the impact of AI risks, which apply at all stages of the supply chain, including system design and development, implementation, import, release and use. At the same time, the major responsibilities lie with the providers and deployers of these systems. Given the specificity of the areas in question, the entities responsible for deployment will be public bodies; their main obligations are set out in Articles 26 and 27 of the AI Act.

The purpose of this paper is not to discuss all the obligations in this area, but it is reasonable to point out the most important ones and those that raise the most doubts. Article 26(1–4) imposes the following obligations on entities applying high-risk AI systems:

1) taking technical and organisational measures to monitor the compliance of the operation of the AI system with the user manual;
2) entrusting supervision to natural persons who have the necessary competence, training and authorisation, as well as the necessary support; and
3) to the extent that the entity exercises control over input data, ensuring the adequacy and sufficient representativeness of input data in relation to the intended use of the high-risk AI system.

Technical and organisational measures include, for example, the creation of appropriate procedures in the event of irregularities being detected by any user, regular internal audits to verify compliance with the user manual, regular training for employees and the introduction of automatic alerts in the event of results that deviate significantly from the average. Supervisory duties involve introducing a 'human-on-the-loop' principle rather than the 'human-in-the-loop' principle (Pinto et al., 2013). This means that a human has the role of controlling the operation of the system, not actively interacting with the system, by providing feedback on the correctness of the results as a permanent element of the learning process. At the same time, this supervision must be real, not just apparent; the supervisor must have the appropriate competences, training and authorisation, and must have knowledge and experience in the field of high-risk AI systems, covering applicable standards and existing threats to the violation of those standards, risks of irregularities and proper reactions to the detection of risks. It is desirable for supervisors to be changed on a regular basis, as research shows that individuals tend to become tired or distracted when working with autonomous systems (Weitkunat & Bestle, 1990), so they cannot actively monitor AI systems for long periods without the risk of undetected irregularities increasing. This is also related to a psychological effect, with individuals assuming that these systems cannot fail or 'make a mistake', even though this happens more often than not (Weitkunat & Bestle, 1990).

With regard to input data, the user is required to ensure that the input data is adequate and sufficiently representative for the purpose of the high-risk AI system. 'Input data' refers to the data provided to or directly obtained by the AI system on which the system bases its generation of results (Article 3(33) of the AI Act). Typically, the system's design specifies the input data required to obtain a result.

Article 27 establishes the obligation to conduct an impact assessment on fundamental rights in connection with the implementation of a high-risk AI system. Identifying the risks to fundamental rights is a crucial first step in addressing such risks, for example by enabling the adoption of appropriate mitigation measures. This issue has already been discussed by scholars (Fülöp & Poindl, 2025; Mentelero, 2024), but it seems sensible to point out the most important issues in this regard. The risk assessment should relate to the fundamental rights listed in the AI Act; key rights that may be at risk are identified in Recital 48 of the Preamble. The specific fundamental rights against which the assessment should be conducted depend on the specifics of the operation of the given system and the area in which it is to be used. For example, based on an analysis of selected AI applications in the public sector, the EU Agency for Fundamental Rights (FRA) has identified the specific impact of AI systems on human dignity, the right to privacy and protection of personal data, the right to equality and non-discrimination, the right to an effective remedy and access to an impartial court, the right to social security and social assistance, consumer protection and the right to good administration (FRA, 2020, pp. 57–86). In practice, however, these assessments are often informal. According to the FRA, providers and deployers tend to focus on a

limited number of potentially affected rights, most notably privacy and data protection, and occasionally non-discrimination and access to an effective remedy (FRA, 2025, p. 34). There is little awareness of more specific rights that may be relevant in different sectors. For instance, in the research conducted by the FRA, none of the respondents working in law enforcement mentioned the presumption of innocence or the right to defence (Article 48 of the Charter) (FRA, 2025, p. 36). This suggests that Fundamental Rights Impact Assessments (FRIAs) need to be carried out more effectively, with greater awareness of the full range of fundamental rights that may be affected by AI systems in specific contexts and of how these rights relate to the use of AI. One way to achieve this would be to guide those conducting the assessments towards the rights most likely to be impacted based on the characteristics of the AI system and its deployment context (FRA, 2025, p. 43).

Of particular importance in the context of systems used in the administration of justice and democratic processes is that the risk assessment should indicate specific mechanisms for counteracting threats and ways of responding to their occurrence, as required by Article 27(1)(e) and (f) of the AI Act. It is important that these mechanisms are not only formally established but also have a real impact on detecting and correcting potential errors and on reducing the risk of results being automatically approved without prior verification. In addition to providing ongoing supervision, it is important to conduct regular audits and to analyse the effectiveness of the supervisory measures that have been implemented. Another important aspect is to enable people about whom decisions are made by AI to obtain information about the system's operation and the legal measures available if they want to challenge the outcome of a decision.

As can be seen, extensive obligations are held by the deployers of high-risk AI systems, and these are only a few of them. Hence a temptation to classify a system as limited-risk instead of high-risk may be present. This issue will be discussed in detail later in this paper, as it is one of the main challenges for Member States in the area of market surveillance.

2. The administration of justice

Regarding the administration of justice, a high-risk AI system is one that is intended to be used by or on behalf of a judicial authority to assist it in researching and interpreting facts and the law and applying the law to a concrete set of facts, or used in a similar way in alternative dispute resolutions. This category refers to judicial authorities, which means courts. The The scope of application indicates that systems intended for use by judges and registrars, as well as by assistants and judicial trainees involved in adjudicatory support activities, are covered. The Court of Justice of the European Union has analysed the concept of a 'judicial authority' in the context of

whether a public prosecutor is a judicial authority entitled to issue a European Arrest Warrant. The organisation of the public prosecutor's office varies between Member States; in some, the prosecution service has strong links with the executive and may be subject to government instruction, while in others, it is independent, with prosecutors forming part of the judiciary. In these jurisdictions, prosecutors are considered to be organs of the judiciary (Judgment of the CJEU, 2019a; Judgment of the CJEU, 2019b; Perrodet, 2002).

Systems that replace judicial authorities in decision-making or other activities performed in the adjudication process, such as the assessment of legal definitions, the reconstruction of facts or the assessment of evidence, are prohibited. Nevertheless, systems can be used to support adjudicators in this respect. The Regulation identifies four areas of application, indicating that these kind of systems should be considered high-risk: research and interpretation of facts; research and interpretation of the law; application of the law to a specific factual situation; and use in a similar way in alternative dispute resolutions. However, the meaning of these terms is not entirely clear and needs to be discussed. AI systems that examine and interpret the facts in criminal, civil, administrative or other proceedings recognise certain patterns in a training dataset and predict whether a given set of facts indicates, for example, that a criminal offence has been committed, a contract has been performed improperly or an erroneous administrative decision has been issued.

Systems used for the examination and interpretation of legal provisions provide links between provisions or legal acts and present relevant case law, interpretations or lines of jurisprudence. They can also independently find the meaning of a provision based on learned interpretations of the same concepts in other provisions of the same or other legal acts, and in available legal definitions (Binkowski, 2023). In general, the vast majority of AI used in the legal industry is operated by law firms, their clients and, albeit less frequently, law-enforcement agencies. These tools are sometimes intended for use by courts; an example is a tool that was developed in France for anonymising court decisions (Vucheva et al., 2020, p. 189). However, as indicated above, this tool would not be considered a high-risk system under the AI Act. Applying the law to a specific factual situation involves subsumption (Cyras & Lachmayer, 2023, pp. 187–190; Zienowicz, 2019). Thus high-risk AI systems will be those that determine, on the basis of factual input, a proposed legal definition, a prohibited contractual provision or a liability regime, for example.

AI systems used in a similar manner in alternative dispute resolution are also high-risk. The Polish Ultima Ratio platform, for example, is an electronic arbitration court operated by the Electronic Arbitration and Mediation Centre at the Association of Notaries of the Republic of Poland in Warsaw that deals with the recognition of commercial disputes in domestic and international trade. Currently, work is underway to introduce an AI system to support the arbitrators. This system will automatically prepare a draft award, with its reasons. To this end, the system will process

into data the statements of the parties which are collected during the proceedings. Using mechanisms for grouping similar cases, it will be able to predict the most likely outcome of a given case. It is also intended that the system will support the arbitrator throughout the proceedings by providing information on the course and outcome of similar cases and presenting excerpts from the reasoning in other awards (Ultima Ratio, n.d.). However, there are disputes over whether arbitration courts are part of the administration of justice (Bookman, 2021). The EU concept of judicial authority suggests that it is most likely that this issue is decided on a case-by-case basis, depending on the design of the national legislation, the status of the authority and the EU instrument to be assessed.

It should be noted that although the judicial area is recognised as being particularly vulnerable to the infringement of individuals' fundamental rights, the AI Act identifies only a few categories of tools that should be considered high-risk within this space. These are systems that have an impact, or are likely to have an impact, on the decision-making processes in a case before a court. This interpretation is also indicated by the wording of Article 6(3) of the AI Act. These systems pose a far greater threat to the rule of law (Kouroutakis, 2024) and the right to a fair trial than others, because impartiality and independence in the judiciary are fundamental to both of these values (see Article 6(1) of the European Convention on Human Rights and Article 47 of the Charter of Fundamental Rights of the European Union). Where judicial decisions are influenced by analyses produced by AI systems, the independence of the judiciary may be undermined. Such analyses can reflect design choices made by the private companies that develop these systems, as well as variables that, under the rule of law, should not influence judicial decision-making. As a result, external interests, including those of private technology providers involved in the design of the systems, may indirectly affect judicial outcomes, thereby calling into question the independence of the judges. Many systems based on AI technology fall outside the above category, despite their use by the judiciary being advocated by doctrine, practitioners and policymakers (Abiodun & Lekan, 2020; Aini, 2020; Donohue, 2019; Lupo, 2019; Perry, 2017, p. 29). These include, for example, systems for the transcription of hearings or machine translation, which should be considered as general-purpose AI (Kiejnich-Kruk, 2024, 2025).

Bearing in mind the considerations presented so far, the recommendations addressed to policymakers focus on three key areas: a framework for the oversight and verification of the risk classification of AI systems by deployers; appropriate training for deployers; and a 'building blocks' strategy in the digitalisation of the judiciary. First, the research indicates that human rights risk assessments are often conducted in an informal manner, and deployers may be unaware of the specific risks posed by a given AI system. Consequently, such systems may be misclassified: the most significant risk arises when a system is incorrectly classified as limited-risk rather than high-risk. In the judicial context, this danger is particularly acute. This stems from

Article 6(3) of the AI Act, which requires an assessment of whether a system poses a significant risk to the fundamental rights of individuals, including cases where the system is deemed not to meaningfully impact the outcome of the decision-making process. As decision-making lies at the core of the administration of justice, such assessments require particular caution and careful consideration; therefore an effective system of verification and oversight must be established to ensure that AI systems used within the judiciary are correctly classified. The AI Act provides supervisory (and supportive) mechanisms at multiple levels, and notably establishes oversight by both EU and national authorities, as well as reference tools prepared by the European Commission, such as the database provided for in Article 71 and the guidelines under Article 6(5). However, at the national level, defining the powers of market surveillance authorities precisely is particularly important. Whether these authorities exercise genuine, substantive control over the classification of systems as high-risk or merely conduct formal, superficial reviews depends on the national legislature.

The second area is closely linked to the first. There is a pressing need for accessible training and practical guidelines for deployers, who, unlike providers, may have limited knowledge of AI systems and their potential impact on various rights and interests; research in this field confirms this. Therefore properly structured training is necessary to raise awareness among deployers of potential human rights risks and to ensure that risk assessments are carried out appropriately to correctly classify systems. This training should also cover other obligations set out in the AI Act, such as conducting FRIAs, event documentation, serious incident reporting and properly implementing human oversight requirements.

Third, initiatives that introduce artificial intelligence into the judiciary are desirable and worthy of support, whether to assist with decision-making or to streamline administrative tasks. However, in countries where the digitalisation of the judiciary is still in its infancy, financial and human resources should initially be allocated to the foundational phases of computerisation. This includes digitalising case files, implementing systems for electronic signatures, developing tools for anonymising judgments and calculating procedural deadlines, integrating public administration systems, establishing secure electronic communication channels, transcribing hearings and trials, and providing support for machine translation (Vucheva et al., 2020, Annex II). Although these systems use AI technologies, they are not primarily designed to support judicial decision-making and therefore do not fall within the high-risk categories discussed above. Consequently, they are not subject to the stringent requirements applicable to high-risk AI systems under the AI Act. Implementing such systems will enable the effective implementation of further projects. It is not possible to skip any of the stages of computerising justice, either technologically or socially, so it is therefore necessary to build the foundations and components of the systems according to the schedule that is adopted. This avoids duplication of errors, which can occur if a technological solution implemented in multiple products is not simultaneously verified. It also enables the system

to address the challenges associated with the implementation of high-risk AI systems, including cybersecurity, data protection, reporting, human oversight and risk minimisation (Kiejnich-Kruk, 2025).

3. Democratic processes

The second category relates to AI systems designed to influence election or referendum outcomes or the voting behaviour of individuals but does not include AI systems with results that individuals are not directly exposed to, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view. Some possible examples of AI-based tools in electoral processes could be AI systems used to deliver political advertising or profile voters, including microtargeting and amplification techniques, to process or count ballots or maintain voting lists, to identify cybersecurity attacks, to perform voter data analysis and predictive analytics, to counter biased content, to moderate electoral content and to provide assistance to voters with chatbot-based systems.

According to a UNESCO guide (Krimmer et al., 2022, p. 20), AI has the potential to enhance electoral processes. AI-based tools can reach a significant number of voters and engage them through personalised communication tailored to their individual preferences and behaviours. AI-based chatbots can provide real-time information about voting locations, candidates' manifestos and voting procedures, thereby making the electoral process more accessible and transparent. However, technological developments are also creating previously unknown threats to democracy and electoral processes. Concerns relating to future elections, including those anticipated for 2028 (USA), are already being discussed in the public sphere (Booth, 2026) and primarily concentrate on two areas: deepfakes and microtargeting. These practices will first be examined in detail, followed by an analysis of their implications for fundamental rights. Building on this assessment, a set of policy recommendations will be formulated.

On a large scale, the generation of false content – deepfakes – in political advertisements has become a means of misleading the public about candidates' claims and positions and about whether certain events actually took place. Under the AI Act, such content must clearly identify the source as AI and disclose that it is artificially generated (see Article 50(4)). For example, during the last US presidential campaign a fake video was created showing President Biden urging his supporters not to vote in the primaries; a political opponent of the incumbent president admitted to creating and distributing the footage (Michałkiewicz-Kądziela, 2024). However, according to Election-Watch.EU, the use of AI-generated content in online campaigning has been detected in only seven EU Member States: Germany, Denmark, Spain, Croatia, Ireland, Portugal and Sweden. In Germany, the most prominent case involved a deep-

fake video created by left-wing activists which depicted Chancellor Scholz calling for a ban on Alternative für Deutschland (AfD). Overall, however, politicians and groups associated with the AfD appear to be the most frequent users of deepfake content for their own purposes; one example is the mass circulation of deepfake audio recordings aimed at discrediting political opponents (European Partnership for Democracy, 2024, p. 12).

AI technology enables the analysis of voter data, including demographics, social media activity and previous voting behaviour. Political campaigns use AI to create detailed voter profiles, enabling politicians to tailor their messages to specific groups, for example, targeting radical content at one group and moderate content at another. This targeted approach can significantly increase the effectiveness of a campaign strategy. AI-based sentiment analysis tools can scan social media platforms, news articles and other content to gauge public opinion on various issues and candidates. With this data, campaigns can adjust their strategies in real time without having to wait for poll results, which are often published late and are based on the views of a relatively small group of people. Predictive AI enables campaigns to use available data to microtarget voters with personalised advertising and fundraising requests (Krimmer et al., 2022, p. 92). On the one hand, such tools can level the playing field for smaller campaigns, increasing their reach and enabling them to engage new audiences. On the other, they can manipulate voters' emotions.

For example, allegations of voter manipulation have been raised in relation to the UK's EU referendum, also known as the Brexit referendum. An investigation into the referendum by the UK Information Commissioner's Office found that pro-Brexit campaign groups had misused Facebook users' personal data for political marketing purposes, targeting political content at people who did not wish to receive it (Day, 2020; Risso, 2018). Another example relates to the annulment of the 2024 presidential election in Romania; the Romanian Constitutional Court cited several reasons for its annulment decision, including third-party campaign financing and access to undisclosed and unregulated funds for digital campaigning. Other reasons were the use of non-transparent digital technologies and artificial intelligence in campaigning, which violates electoral law, and the increased online exposure of candidates, which exerts undue influence on voters beyond public control. The Court also cited weak oversight by election management bodies, which lacked the resources to effectively supervise online advertising spending carried out through digital networks and platforms (International Foundation for Electoral Systems, 2024).

The AI systems mentioned above are focused on the so-called microtargeting of specific messages, the analysis of social emotions and the analysis of a person's world view in order to direct the appropriate message to them (in terms of both content and form), but there are also systems that allow for the artificial generation of online traffic. Expressions of approval for particular content on social media accounts that do not belong to real people certainly influence the behaviour of voters and conse-

quently the outcomes of elections themselves. The real challenge for public actors in this field is to control and verify whether high-risk systems have actually been used. A lack of transparency by election staff in this regard may raise justified doubts.

Given these risks, AI systems that generate artificial materials for electoral campaigns, distribute these materials and select the voters to whom the materials will be presented are considered high-risk. These systems pose a particular threat to democracy and individual freedoms, such as freedom of speech and the freedom to vote in accordance with one's beliefs without external influence. As the Preamble to the AI Act refers to individual rights, it also involves the right to vote and the right to be elected (these systems can influence how and for whom a person votes). AI-driven profiling, targeted disinformation and deepfake content can influence public perception of candidates unfairly and distort competition. Such practices risk undermining the principle of equal opportunity in electoral participation and may compromise the integrity of the democratic process. In order to safeguard this fundamental right, legal and regulatory frameworks must ensure transparency in the use of AI in campaigning, prevent discriminatory or manipulative practices and provide effective remedies for candidates whose electoral rights have been infringed by AI-enabled interventions.

AI-driven microtargeting, particularly when facilitated by generative AI, raises substantial concerns relating to data protection, manipulation and accuracy. Both the selection of target groups and the platforms used to deliver political advertising risk creating or exacerbating inequities, as electoral management bodies (EMBs) may disproportionately reach certain subgroups of the electorate (Ali et al., 2019). Data protection and data minimisation have therefore become priority concerns. Electoral datasets must be representative, secure and restricted to what is necessary to ensure inclusivity without compromising individual rights. The General Data Protection Regulation's (GDPR) principle of data minimisation requires that only data which is necessary for a defined purpose be processed. Applying this principle in the context of AI development, particularly during the training phase, poses significant challenges given the data-intensive nature of effective algorithmic training: large datasets are often relied upon to reduce bias and enhance model performance, which may initially appear to be at odds with the requirement of data minimisation. However, the GDPR allows for a degree of flexibility in the interpretation of 'necessity', acknowledging that extensive data collection may be justified at early stages, provided that data volumes are subsequently reduced. Accordingly, AI developers are required to implement robust filtering and deletion mechanisms to ensure that unnecessary data is removed once the training process is complete (Renaissance Numérique, 2025).

The use of AI systems also heightens the risk of foreign interference in electoral processes: advanced AI tools can enable external actors to produce and disseminate highly targeted disinformation at scale, manipulate online discourse and impersonate domestic political figures or institutions with increased credibility. Through techniques such as deepfakes, automated social media accounts and AI-driven mi-

crotargeting, foreign actors may seek to influence voter perceptions, suppress turnout or undermine trust in democratic institutions. Such practices may undermine the integrity of elections, violate principles of sovereignty and infringe upon voters' rights to free and informed participation (Farantouris & Pipis, 2025, p. 12).

There are other threats to human rights. AI-based verification methods may wrongfully disenfranchise legitimate voters, and increasing policing at polling sites may suppress voter turnout rates, impact electoral outcomes and reduce trust in the process (Padmanabhan et al., 2023). Empirical evidence highlights these risks: the accuracy of signature-based or biometric matching systems may be quite low, creating a significant risk of disenfranchising eligible voters (Hussain et al., 2015). In addition, the deployment of large language model (LLM) chatbots in electoral management presents serious concerns regarding the reliability of information. EMBs must therefore undertake extensive testing and auditing to prevent hallucinations and the dissemination of false or misleading information (Rawte et al., 2023). Moreover, excessive reliance on AI systems for misinformation detection may cause EMBs to overlook emerging narratives or voter concerns, particularly on private messaging platforms where automated monitoring is limited (Juneja, 2024, pp. 12–30).

At the same time, AI-driven fact-checking tools can play a crucial role in countering false narratives. Ensuring that these tools are widely accessible and effectively integrated into electoral processes can help mitigate the risks posed by AI-enabled disinformation. Fairness and non-discrimination constitute key ethical considerations in this context. AI systems deployed in elections must be designed to avoid bias and to ensure that they do not disproportionately affect specific groups of voters; for example, AI-based predictive analytics or voter profiling may unintentionally reinforce existing societal biases. Consequently, regulatory oversight is necessary to mandate fairness audits, ensuring that AI systems treat all voter groups equitably and do not perpetuate discriminatory outcomes (Itumeleng & Esiefarienrhe, 2024, p. 3217). One should bear in mind that systems intended for administrative tasks, such as updating voter lists, verifying voters, reporting on resource allocation and campaign spending, and measuring voter turnout in real time, have been exempted from the Regulation.

Both detecting the use of a specific system and the procedure for associating that system with a given actor (the entity using the system) may prove to be very complex. At the same time, these steps are crucial for assessing whether the entity has fulfilled its obligations under the AI Act and, further, whether the system can be considered to have been used correctly from the point of view of the protection of fundamental rights. It seems that a national legislative policy should focus on the following elements:

Public authorities should establish a robust system of verification and oversight to ensure the correct classification of AI systems as prohibited, high-risk or limited-risk;

It is necessary to introduce legal requirements for transparent declarations (and limits) regarding the use of AI systems in the course of election campaigns and in

elections (or referendums) themselves, not only from the entities directly involved in their conduct (political parties or EMBs), but also from all related entities;

There needs to be collaboration with internet service providers, including traditional media and social media, in the control of content related to elections and referendums, the broadcasters of such content and related entities (accounts), and methods of use.

The most important questions are how to classify a given system as prohibited, high-risk or limited-risk, and how to identify appropriate responsibilities and risk-mitigation tools. As noted above, such assessments are often conducted in a relatively informal manner. Relevant actors may be inclined to assign systems to a lower-risk category, partly because this entails fewer regulatory obligations but also due to limited awareness of human rights-related risks. For this reason, public bodies have a crucial role to play in establishing effective control and verification mechanisms to ensure that AI systems are properly classified and that deployers comply with the obligations imposed by the AI Act. This area of concern closely resembles the one discussed above in relation to judicial processes.

In the second area, numerous stakeholders have called for a coherent legal and ethical framework (Juneja, 2024; Nikolich, 2025; TIAL, 2025). EMBs should assess AI use cases against existing administrative practices, focusing on areas where AI may enhance current processes, and should undertake comprehensive evaluations of both the costs and benefits of implementation. Where feasible, EMBs and political actors should ensure meaningful human oversight of AI systems and treat AI as complementary to existing strategies rather than as a substitute for them. At the same time, all actors involved should adopt high standards of transparency, interpretability and accountability, both for AI systems developed internally and for those supplied by external vendors. Any AI-generated content should be clearly labelled.

A further pressing concern relates to misinformation and disinformation campaigns targeting electoral administration. Such campaigns may aim to confuse voters regarding the timing, location or procedural requirements of elections, thereby undermining public confidence in the integrity and legitimacy of the electoral process. The use of AI to generate and disseminate disinformation, including through deepfake videos and automated bot networks, presents a serious ethical and regulatory challenge. AI technologies enable the rapid and large-scale spread of false or misleading information, potentially influencing voter behaviour and compromising democratic integrity. Regulatory frameworks should therefore include specific provisions to limit the use of AI in the creation and dissemination of disinformation.

In the third area, EMBs should conduct thorough and continuous audits of AI systems, covering security, performance and ethical compliance. National legislation should complement EU-level instruments, in particular the Digital Services Act (DSA). The DSA provides, inter alia, for retention orders and for the investigation of potential infringements of Articles 34(1), 34(2) and 35(1), which concern obligations

to mitigate systemic risks, including those linked to fraudulent use and coordinated inauthentic behaviour. Such tools were employed in the European Commission's investigation concerning the legality of the presidential elections in Romania in 2024.

Moreover, the European Commission has issued guidelines addressed to providers of very large online platforms and very large online search engines concerning the mitigation of systemic risks in electoral processes (European Commission, 2024). These guidelines should be taken into account when assessing platform conduct. It is therefore essential that such platforms cooperate with public authorities, in compliance with the law, in order to limit harmful practices affecting electoral processes.

It should also be noted that the interplay between the AI Act and the DSA has been widely analysed in academic literature. Very large online platforms and search engines may be subject to systemic risk-assessment duties under both the AI Act and the DSA simultaneously, particularly where general-purpose AI models are integrated into intermediary services. More broadly, concerns have been expressed that the cumulative effect of the EU's digital regulatory framework – including, for example, the GDPR, with its requirement to conduct Data Protection Impact Assessments (Hohmann & Kollár, 2025; Levitina, 2025; Sarra, 2025; Sartor & Lagioia, 2020; Ufert, 2020), alongside the FRIAs required under the AI Act – may disproportionately burden European AI innovators (Graux et al., 2025). Intermediary service providers, such as online platforms and search engines, that develop, deploy or integrate AI systems (for example in recommender systems or content-moderation tools) may face cumulative transparency and risk-assessment obligations. While these obligations are not contradictory, their combined effect may increase the regulatory burden. Nevertheless, from the perspective of human rights protection, overlapping obligations do not in themselves constitute a threat. The DSA's content-moderation framework and the AI Act's requirements for high-risk AI systems may intersect, particularly in relation to AI-driven moderation tools. Both the DSA and the AI Act require platforms to assess and mitigate systemic risks, including those arising from the use of AI systems.

EMBs should also bear in mind that private messaging and email services largely fall outside the DSA's hosting service regime. Consequently, AI-powered chatbots operating within such environments are not clearly subject to the same regulatory obligations as online platforms. This creates a regulatory gap and presents a challenge for public authorities, as providers of these services are not bound by obligations equivalent to those imposed on platforms with regard to the spread of misinformation and disinformation.

Conclusion

The EU legislature has classified certain AI systems deployed in the administration of justice and in democratic processes as high-risk. These areas were considered together during the legislative process, as they pose risks to similar values, interests and, above all, fundamental rights. The fundamental rights at risk in the deployment of AI systems across both judicial and electoral processes are the right to a fair trial, the right to an effective remedy, the presumption of innocence, equality of arms and the right to defence, as well as freedom of expression, the freedom to vote according to one's convictions without undue influence and the right to be elected.

A core challenge for justice systems lies in distinguishing, within the broader digitalisation of judicial procedures, which systems qualify as high-risk AI and which fall outside that category. The use of high-risk systems entails a range of obligations aimed at mitigating risks to fundamental rights. Accordingly, policymakers should prioritise the development of a robust oversight and verification framework to ensure accurate system classification, coupled with targeted training for deployers to support compliance with these obligations. Strengthening these mechanisms would significantly enhance the protection afforded to individuals whose cases may be influenced by the use of such technologies.

In the electoral sphere, the enforcement of ethical and legal safeguards governing the use of AI presents equally complex challenges. Given that many election-related risks stem from the dissemination of information – whether accurate or misleading – concerning candidates, voting procedures or the electoral process more broadly, and considering that online platforms constitute the primary venues for such content, effective cooperation with these platforms is essential. Although the obligations arising under the DSA, the AI Act and related digital regulations may impose considerable burdens on intermediaries, they remain justified from the standpoint of safeguarding human rights. A sensible policy direction would therefore involve establishing legal requirements for transparent declarations and clear limitations concerning the use of AI systems during electoral campaigns, together with structured collaboration with internet platforms in monitoring election-related content, identifying entities responsible for its dissemination and scrutinising the methods through which AI tools are employed.

This article does not seek to exhaust the complexity of the issues examined, nor do the challenges and recommendations presented constitute a comprehensive list. They are intentionally general in scope: the objective has not been to propose fully formed legislative solutions but rather to outline key directions for further reflection. The findings underscore the need for continued scholarly inquiry in this field, while the recommendations provided serve as a valuable point of departure for academic debate as well as for policymakers engaged in shaping the future regulatory landscape.

REFERENCES

Abiodun, O., & Lekan, A. (2020). Exploring the potentials of artificial intelligence in the judiciary. *International Journal of Engineering Applied Sciences and Technology*, *5*(8), 23–27.

Aini, G. (2020). A summary of the research on the judicial application of artificial intelligence. *Chinese Studies*, *9*, 14–28.

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes. *arXiv*. https://doi.org/10.48550/arXiv.1904.02095

Binkowski, K. (2023). Sztuczna inteligencja a wykładnia prawa – propozycja zastosowania systemów AI do ustalania założenia o racjonalnym prawodawcy. *ZeszytPrawniczy, U. A. M., 13*, 7–17.

Bookman, P. K. (2021). Arbitral courts. *Virginia Journal of International Law*, *61*, 179–184, 201–213.

Booth, R. (2026, 22 January). Experts warn of threat to democracy from 'AI bot swarms' infesting social media. *The Guardian*. https://www.theguardian.com/technology/2026/jan/22/experts-warn-of-threat-to-democracy-by-ai-bot-swarms-infesting-social-media

Brożek, B., Furman, M., Jakubiec, M., & Kucharzyk, B. (2024). The black box problem revisited: Real and imaginary challenges for automated legal decision making. *Artificial Intelligence and Law*, *32*, 427–440.

Cyras, V., & Lachmayer, F. (2023). *Essays on the visualisation of legal informatics*. Springer International Publishing.

Day, P. (2020). Cambridge Analytica and voter privacy. *Georgetown Law Technology Review*, *4*(2), 583–608.

Donohue, M. (2019). A replacement for Justitia's scales? Machine learning's role in sentencing. *Harvard Journal of Law and Technology*, *32*(2), 657–678.

European Commission. (2022). Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes Pursuant to Article 35(3) of Regulation (EU) 2022/2065 (Text with EEA Relevance) (C/2024/3014).

European Commission. (2024, 26 April). Communication from the Commission – Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes Pursuant to Article 35(3) of Regulation (EU) 2022/2065, C/2024/2537 (O. J. C C/2024/3014, 26.04.2024).

European Commission. (2024a). *Commission, online platforms and civil society increase monitoring during Romanian elections*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243

European Commission. (2024b). *Commission opens formal proceedings against TikTok on election risks under the Digital Services Act*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

European Parliament and the Council. (2022, 19 October). Regulation on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) (2022/2065) (O. J. L 277, 27.10.2022, pp. 1–102).

European Parliament and the Council. (2024, 12 July). Regulation Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No. 300/2008 (EU) No. 167/2013 (EU)

No. 168/2013 (EU) 2018/858 (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance) (2024/1689) (O. J. L, 2024/1689, 12.07.2024).

European Partnership for Democracy. (2024). *The EU's Artificial Intelligence Act and its impact on electoral processes: A human rights-based approach*. https://epd.eu/content/uploads/2024/09/AI-and-elections.pdf

Farantouris, N., & Pipis, T. (2025, October). *AI in the democratic sphere and the electoral process*. https://farantouris.eu/wp-content/uploads/2025/10/Research-Paper-AI-Disinformation-.pdf

FRA (2020). *Getting the future right: Artificial intelligence and fundamental rights*. Publications Office of the European Union.

FRA (2025). *Assessing high-risk AI: Fundamental rights risks*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2025-assessing-high-risk-ai-fundamental-rights-risks_en.pdf

Fülöp, T., & Poindl, P. (2025). Article 27. In C. N. Pehlivan, N. Forgó, & P. Valcke (Eds.), *The EU Artificial Intelligence (AI) Act: A commentary* (pp. 553–573). Wolters Kluwer.

Graux, H., Garstka, K., Murali, N., Cave, J., & Botterman, M. (2025). *Interplay between the AI Act and the EU digital legislative framework*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/778577/ECTI_ATA(2025)778577_EN.pdf

Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M., & Hussain, A. (2024). Interpreting black-box models: A review on explainable artificial intelligence. *Cognitive Computation*, *16*, 45–74.

Hohmann, B., & Kollár, G. (2025). Reflections on the data protection compliance of AI systems under the EU AI Act. *Cogent Social Sciences*, *11*(1). https://doi.org/10.1080/23311886.2025.2560654

Hussain, R., Raza, A., Siddiqi, I., Khurshid, K., & Djeddi, C. (2015). A comprehensive survey of handwritten document benchmarks: Structure, usage and evaluation. *EURASIP Journal on Image and Video Processing*, *2015*(1), Article 46. https://doi.org/10.1186/s13640–015-0102–5

International Foundation for Electoral Systems. (2024). *The Romanian 2024 election annulment: Addressing emerging threats to electoral integrity*. https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity

Itumeleng, M. M., & Esiefarienrhe, B. M. (2024). The impact of artificial intelligence, ethical implications and technologies on the electoral process. *E-Journal of Humanities, Arts and Social Sciences*, *5*(16), 3211–3219. https://doi.org/10.38159/ehass.202451641

Judgment of the CJEU of 27 May 2019 on the case of *Minister for Justice and Equality v. OG and PI*, C 508/18.

Judgment of the CJEU of 27 May 2019 on the case of *PF*, C-509/18.

Juneja, P. (2024). *Artificial intelligence for electoral management*. International Institute for Democracy and Electoral Assistance. https://doi.org/10.31752/idea.2024.31

Kiejnich-Kruk, K. (2024). Lost in translation: Implementation of the right to a translator through the use of machine translators in the light of EU and Polish Law. *Ruch Prawniczy, Ekonomiczny i Społeczny*, *84*(1), 61–81.

Kiejnich-Kruk, K. (2025). Building blocks – strategia cyfryzacji wymiaru sprawiedliwości. Perspektywa estońska. *Przegląd Sądowy*, *3*, 86–100.

Kouroutakis, A. (2024). Rule of law in the AI era: Addressing accountability, and the digital divide. *Discover Artificial Intelligence*, *4*, 115. https://doi.org/10.1007/s44163–024-00191–8

Krimmer, R., Rabitsch, A., Kužel, R., Achler, M., & Licht, N. (2022). *Elections in digital times: A guide for electoral practitioners*. The United Nations Educational, Scientific and Cultural Organization.

Levitina, A. (2025). Humans in automated decision-making under the GDPR and AI Act. *Revista CIDOB d'Afers Internacionals, 138*, 121–144.

Lupo, G. (2019). Regulating (artificial) intelligence in justice: How normative frameworks protect citizens from the risks related to AI use in the judiciary. *European Quarterly of Political Attitudes and Mentalities*, *8*(2), 75–96.

Mentelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review*, *54, article number: 106020*.

Michałkiewicz-Kądziela, E. (2024). The impact of deepfakes on elections and methods of combating disinformation in the virtual world. *Teka Komisji Prawniczej PAN Oddział w Lublinie*, *17*(1), 152–153.

Nikolich, A. (2025). A unified code of ethics and conduct for AI and trustworthy elections. In: B. Srivastava, A. Nikolich, A. Hickerson, & T. Koppel (Eds.), *Promise: Promoting AI's safe usage for elections* (pp. 279–290). Springer. https://link.springer.com/chapter/10.1007/978–3-031–89853-2_17

Padmanabhan, D., Simoes, S., & MacCarthaigh, M. (2023). AI and core electoral processes: Mapping the horizons. *AI Magazine*, *44*(3), 218–239. https://doi.org/10.1002/aaai.12105

Perrodet, A. (2002). The public prosecutor. In M. Delmas-Marty & J. R. Spencer (Eds.), *European Criminal Procedure* (pp. 415–455). Cambridge University Press.

Perry, M. (2017). iDecide: Administrative decision-making in the digital world. *Australian Law Journal*, *91*, 29–41.

Pinto, R., Mettler, T., & Taisch, M. (2013). Managing supplier delivery reliability risk under limited information: Foundations for a human-in-the-loop DSS. *Decision Support System*, *54*(2), 1076–1084.

Rawte, V., Sheth, A., & Das, A. (2023). A survey of hallucination in large foundation models. *arXiv*. https://doi.org/10.48550/arXiv.2309.05922

Renaissance Numérique. (2025). *Interactions and overlaps between the GDPR and AI Act, with Etienne Drouard*. https://www.renaissancenumerique.org/en/publications/interactions-and-overlaps-between-the-gdpr-and-ai-act-with-etienne-drouard/

Risso, L. (2018). Harvesting your soul? Cambridge Analytica and Brexit. In C. Jansohn (Ed.), *Brexit means Brexit?* (pp. 75–85). Akademie der Wissenschaften und der Literatur.

Sarra, C. (2025). Artificial intelligence in decision-making: A test of consistency between the EU AI Act and the GDPR. *Athens Journal of Law, 11*(1), 45–62.

Sartor, G., & Lagioia, F. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. *Publications Office of the European Union*.

TIAL (2025). *White paper #001: Safeguarding elections in the age of AI and synthetic content*. https://tial.org/publications/white-paper-001-safeguarding-elections-in-the-age-of-ai-and-synthetic-content/

Ufert, F. (2020). AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI? *European Papers*, 5(2), 1087–1097.

Ultima Ratio (n.d.). *Sztuczna inteligencja w Ultima Ratio. Czy roboty zastąpią arbitrów?* Retrieved 5 February 2025, from https://ultimaratio.pl/blog/sztuczna-inteligencja-w-ultima-ratio-czy-roboty-zastapia-arbitrow

Vucheva, M., Rocha, M., Renard, R., & Stasinopolous, D. (2020). *Study on the use of innovative technologies in the justice field – Final report*. https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634–11ea-991b-01aa75ed71a1/language-en

Weitkunat, R., & Bestle, M. (1990). Computerized Mackworth vigilance clock test. *Computer Methods and Programs in Biomedicine*, *32*(2), 147–149.

Zienowicz, T. A. (2019). Artificial intelligence i singularity w procesie stosowania prawa, *Prawo Mediów Elektronicznych*, *2*, 31–33.