

Opportunities and Challenges of Using Artificial Intelligence in the Pre-election Phase with an Emphasis on Iran's Legal and Electoral System

Davoud. Mohebbi¹, Ali. Amiri^{2*}

¹ Assistant Professor, Department of Public Law, Faculty of Law, University of Qom, Qom, Iran

² Master's Student, Department of Public Law, Faculty of Law, University of Qom, Qom, Iran

* Corresponding author email address: a.amiri@stu.qom.ac.ir

Received: 2026-06-01

Revised: 2026-08-04

Accepted: 2026-08-12

Initial Publish: 2026-08-19

Final Publish: 2027-07-01

The spread of artificial intelligence has created new capacities for managing and improving electoral processes. The pre-election phase is considered one of the most important areas of use for this technology due to its role in the registration and verification of candidate and voter information, authentication, data management, combating fake news and misleading information, and identifying false activities in cyberspace. The present study, using a descriptive-analytical method and utilizing library resources, examines the applications of artificial intelligence in the pre-election phase, with an emphasis on the Iranian legal and electoral system. The findings of the study show that the use of artificial intelligence can help promote the health and efficiency of electoral processes by increasing the speed and accuracy of information processing, reducing human errors, strengthening monitoring, identifying abnormal patterns, and combating the dissemination of misleading information. On the other hand, algorithmic bias, lack of transparency and explainability, privacy violations, threats to data security, liability arising from algorithmic errors, and the possibility of restricting fundamental freedoms are among the most important legal and technical challenges of this technology. An examination of the status of Iran's legal system also shows that, although some existing regulations have enabled the use of new technologies, the lack of a comprehensive, dedicated framework for regulating the use of artificial intelligence in electoral processes remains evident. Accordingly, the legitimate and responsible use of artificial intelligence in the pre-election phase requires ensuring algorithmic transparency, accountability, human oversight, protection of personal data, and respect for citizens' fundamental rights and freedoms.

Keywords: Artificial Intelligence, Digital Governance, Elections, Iranian Electoral System, Pre-election Phase, Public Law.

How to cite this article:

Mohebbi, D. & Amiri, A. (2027). Opportunities and Challenges of Using Artificial Intelligence in the Pre-election Phase with an Emphasis on Iran's Legal and Electoral System. *Interdisciplinary Studies in Society, Law, and Politics*, 6(4), 1-18. <https://doi.org/10.61838/kman.isslp.549>

1. Introduction

Digital transformation in recent decades has fundamentally transformed the ways in which public governance, the management of government affairs, and public service delivery are conducted. Meanwhile, artificial intelligence, as one of the most important emerging technologies, has gradually gained prominence in public administration and governance

systems owing to its ability to process large volumes of data, identify complex patterns, predict events, analyze information, and support decision-making processes. Therefore, governments and public institutions in many countries are seeking to utilize the capabilities of artificial intelligence to increase efficiency, enhance the quality of public services, improve transparency, and strengthen accountability in governance processes



(Brown & Smith, 2023; Suskind, 2024). Elections, as the most important mechanism for realizing citizens' political participation and one of the fundamental pillars of democratic systems, constitute a multilayered and complex process whose integrity requires adherence to principles such as transparency, impartiality, security, equality, accountability, and public trust. Meanwhile, technological evolution and the expansion of the digital space, while creating new capacities for more effective election management, have also generated new threats and challenges. The increasing volume of electoral data, the expansion of social networks, the growing sophistication of political campaign methods, the dissemination of fake news and misleading information, the activity of fake user accounts, the use of bots and trolls, the production of deepfake content, and the possibility of cyber interventions are among the factors that have exposed the integrity and reliability of electoral processes to new risks. Under such circumstances, artificial intelligence can be used as a tool to manage and analyze large volumes of data, identify unusual patterns, combat misleading information, and improve the efficiency of electoral processes (European, 2025; Wang & Lee, 2023). Among the various stages of the electoral process, the pre-election stage is particularly important and sensitive, as a significant proportion of the infrastructural measures and decisions affecting the integrity and credibility of elections are undertaken at this stage. Registration and verification of candidates' and voters' information and documents, authentication, management and analysis of electoral data, public information dissemination, identification of and response to fake news and misleading information, detection of coordinated and organized activities on social networks, identification of bots and trolls, and ensuring the security of information infrastructure are among the most important areas in which the potential use of artificial intelligence can be examined. The use of intelligent systems in these areas can increase the speed of information processing, reduce human errors, improve the accuracy of data verification, facilitate monitoring, and enhance the ability of responsible institutions to identify emerging threats. However, the introduction of artificial intelligence into this phase of the electoral process also raises fundamental legal and public law questions, including who is responsible for algorithmic decisions, how the transparency and

explainability of intelligent systems can be ensured, what mechanisms exist to prevent algorithmic bias and discrimination, the extent to which intelligent systems may access citizens' personal data, and how a balance can be struck between the need to ensure electoral security and the protection of privacy and fundamental freedoms (Carvalho & Rosa, 2024; Jasanoff, 2024; O'Neil, 2016). The importance of these issues becomes particularly evident when artificial intelligence is understood not merely as a technical tool but as an integral component of public governance and the administration of electoral processes. The use of algorithmic systems in electoral processes may directly or indirectly affect the legal rights and interests of candidates and voters. For instance, algorithmic systems employed to verify information, detect anomalies, or identify potentially misleading content may produce erroneous classifications that affect the treatment of electoral materials or the exercise of political rights. Similarly, natural language processing systems may incorrectly classify legitimate political expression as disinformation, while social network analysis systems may misinterpret ordinary user activity as coordinated or organized behavior. Under such circumstances, insufficient algorithmic transparency, limited explainability, and the absence of effective mechanisms for human oversight and review may undermine the rule of law and administrative accountability. From this perspective, the legitimacy of AI-based technologies in electoral governance depends not only on their technical efficiency but also on their conformity with the legal principles governing public-sector AI, particularly transparency, accountability, human oversight, and the protection of individuals affected by algorithmic decisions (Pavlidis & Kastanas, 2026). On the other hand, the use of artificial intelligence in the pre-election phase can also be considered from the perspective of realizing the right to political participation and the right to self-determination. Elections can truly reflect the will of citizens only when voters have equal access to reliable information and can make informed decisions without being influenced by organized operations designed to disseminate misleading information or manipulate public perception. In this context, artificial intelligence can help improve the quality of political participation by analyzing vast amounts of information, identifying patterns in the dissemination of fake news, detecting

fake accounts, and providing evidence-based warnings. However, if these same capacities are used without appropriate supervision and legal safeguards, they may become tools for extensive surveillance, engineering public perception, restricting freedom of expression, or controlling citizens' political behavior. Therefore, the legal value of using artificial intelligence in elections can be assessed not only in terms of its technological capabilities but also according to the extent to which this technology can enhance citizens' free, informed, equal, and trustworthy participation (López-López et al., 2023; Martos, 2023; Tavakoli-Rad & Sadat Miri, 2021). In this context, algorithmic transparency and accountability are among the most important public law requirements for the use of artificial intelligence in electoral processes. Whenever an intelligent system is used for registration, information verification, fake-news detection, abnormal-behavior detection, or cyberspace monitoring, it must be possible to evaluate and audit its performance. Moreover, if the system's output affects the rights of a candidate or voter, the affected individual must be able to understand the basis of the decision and have access to effective mechanisms for objection and review. From this perspective, transparency in the electoral system does not simply mean the dissemination of information but also encompasses traceability, explainability, and the possibility of monitoring technological processes (Brunner, 2026; Tavakoli-Rad & Sadat Miri, 2021; Wieringa, 2020). In addition, protecting personal data and respecting privacy are essential requirements for using artificial intelligence in the pre-election phase because many applications of this technology require the collection, processing, and analysis of significant amounts of citizens' identity-related, personal, and sometimes sensitive data (Fitzgerald, 2024; Jafari & Rahbarpour, 2017). In the legal system of the Islamic Republic of Iran, the use of artificial intelligence in the pre-election phase must be evaluated within the framework of constitutional principles, electoral laws, regulations governing computer crimes, and rules concerning citizens' rights and freedoms. Although existing laws provide certain capacities for using new technologies in the management and monitoring of electoral processes, the absence of a comprehensive and dedicated framework for regulating the use of artificial intelligence raises serious questions regarding the limits of the competence of electoral institutions, liability

arising from algorithmic errors, the protection of personal data, procedures for objecting to decisions based on artificial intelligence, and the limits of intelligent surveillance of cyberspace. This issue is particularly important in the fields of fake-news detection and social-media monitoring because the extensive use of intelligent systems without clear legal limits and effective human and judicial oversight may conflict with the rights to freedom of expression and privacy and with the prohibition of unlawful interference in citizens' communications. In this context, Article 25 of the Constitution also emphasizes the protection of the inviolability of communications and prohibits surveillance and interference with communications except as provided by law. Despite the expansion of domestic and international research on the use of artificial intelligence in elections, a significant proportion of existing research has focused primarily on the technical aspects of this issue. A coherent examination of the applications of artificial intelligence in the pre-election stage from the perspective of public law, particularly in relation to the characteristics and limitations of Iran's legal and electoral system, still requires further study and analysis. In fact, the central issue of the present research is not simply to examine the areas in which artificial intelligence can be used during the pre-election phase. Rather, the fundamental question is what opportunities these applications create for promoting the integrity and efficiency of elections, what legal and technical challenges and risks they generate, and to what extent the Iranian legal system has the capacity to respond to these challenges. Accordingly, the present study, using a descriptive-analytical approach and library resources, examines the opportunities and challenges of using artificial intelligence in the pre-election phase, with a focus on the status of Iran's legal and electoral system. In this regard, first, the most important applications of artificial intelligence at this stage are examined, including registration and information verification, the detection of fake news and misleading information, and the identification of bots and trolls. Next, the opportunities and potential benefits of this technology for improving the speed, accuracy, transparency, and integrity of electoral processes are analyzed. Subsequently, the legal and technical challenges and risks arising from its use are examined, including algorithmic bias, privacy violations, lack of

transparency, liability arising from errors, cyber threats, and the possibility of restricting freedom of expression. Finally, considering the principles of public law and the requirements of the Iranian electoral system, the need to establish a rights-based framework for regulating the use of artificial intelligence in the pre-election phase is emphasized a framework that, while utilizing the capabilities of this technology, ensures transparency, accountability, human oversight, protection of citizens' fundamental rights, and public trust in the electoral process.

2. The Concept of Artificial Intelligence

2.1. Conceptual Definition and System-Oriented Approach

In public law and digital governance, "artificial intelligence" refers not merely to a single software program or tool but rather to systems that rely on data and computational methods to perform tasks that, in conventional settings, would have been considered to require human analysis, such as classification, prediction, recommendation, pattern discovery, generation of linguistic and visual outputs, and, in some cases, administrative decision support. From this perspective, in the Iranian public administration literature, artificial intelligence is presented as one of the drivers of the transition from e-government to digital governance—a transition in which "data-driven decision-making" and "intelligent automation of processes" are emphasized (Tavakoli-Rad & Sadat Miri, 2021). On this basis, Iranian research on public administration has also introduced artificial intelligence as an "empowering" technology for improving service quality and government efficiency. However, such research has warned that efficiency without legal guarantees of transparency, accountability, and respect for citizens' rights can lead to serious governance challenges (Mahmoudi et al., 2025; Mutawa & Rashid, 2020).

2.2. Determinant Legal Features in Governance Applications

In public law research, "artificial intelligence" is particularly relevant when it is used as a tool of governance and public administration. In these applications, several characteristics play a decisive role:

A. Accountability and decision attribution. The greater the system's contribution to the output, the more complex the design of mechanisms for attribution and responsibility becomes (López-López et al., 2023; Martos, 2023; Mehdi, 2025).

B. Transparency, explainability, and the possibility of oversight. The challenge of legal oversight of the "output logic" and the possibility of effective objection are among the most central issues in the administrative law of artificial intelligence (Carvalho & Rosa, 2024; Hosseinabadi & Zarefard, 2022).

C. Privacy and data security. The collection and analysis of citizens' data, particularly on a large scale, can lead to invasions of privacy and, in the absence of appropriate safeguards, trigger civil liability (Fitzgerald, 2024; Jafari & Rahbarpour, 2017).

D. Risk of bias and discrimination. Data and design biases can lead to discriminatory outcomes and may be inconsistent with the principles of administrative justice and citizen equality (O'Neil, 2016; Susskind, 2024).

2.3. The Concept of the Electoral System

2.3.1. Definition of the Electoral System as "the Legal-Institutional Framework of Electoral Administration"

In the strict sense of public law, the "electoral system" is not limited to the voting stage. Rather, it comprises a set of legal rules, executive and supervisory institutions, processes, and guarantee mechanisms encompassing everything from the design and announcement of elections to registration, campaigning, voting, vote counting, announcement of results, and handling of complaints. In this sense, the electoral system forms part of the "public administration system." Any technological change, including the introduction of artificial intelligence systems, must therefore be analyzed in terms of its compatibility with principles of public law, such as legitimacy, transparency, accountability, and the protection of citizens' rights (Tavakoli-Rad & Sadat Miri, 2021).

2.3.2. Main Components of the Electoral System

For research purposes, the electoral system can be divided into the following components, a classification that is also useful for analyzing electronic and digital elections:

A. Voting rights and voter registration rules. These include determining eligibility conditions, authentication requirements, and procedures for forming the voter list. In digital and electronic contexts, this component is heavily dependent on data, cybersecurity, and information protection (Fatemi, 2024; Habibi & Homayoun, 2016).

B. Nomination rules and competences. These include eligibility conditions, the candidate registration process, document verification, and review mechanisms.

C. Executive management of elections. This encompasses polling-station design, resource allocation, logistics, training, and executive processes; a topic that is linked in the digital governance literature to "process transformation" and "data-driven decision-making" (Akbari et al., 2024).

D. Monitoring, integrity assurance, and review mechanisms. These include monitoring the accuracy of the process, ensuring auditability, and providing mechanisms for complaints and objections. As processes become increasingly digital, the importance of "traceability" and "system security" increases, a point that has been seriously addressed in studies related to electronic voting (Takhtaei, 2011).

E. Information infrastructure and electoral cybersecurity. This is a cross-cutting component governing all stages and includes confidentiality, data integrity, accessibility, and responses to threats. The legal literature on security in cyberspace considers this dimension part of the prerequisites for public trust and the integrity of processes (Jalali Farahani & Bagheri Asl, 2008).

3. Theoretical and Legal Foundations

The introduction of artificial intelligence into "elections" must be analyzed in relation to two layers: first, the theoretical foundations that demonstrate why and how the use of this technology can serve the fundamental values of public electoral law; and second, the legal foundations that determine the limits of competences, duties, safeguards, and responsibilities governing its application. In the digital governance literature, smart technologies acquire legitimacy and effectiveness when situated within a transparent, accountable, and rights-based legal framework (Jabbari & Karim, 2024).

3.1. Guaranteeing the Right to Self-Determination

The right to self-determination, in the context of domestic public law, is reflected in the concepts of "popular sovereignty" and "the right to effective participation in public decision-making," and elections constitute the institutional mechanism for its realization. From this perspective, artificial intelligence has a defensible theoretical basis for entering electoral processes when it enhances effective participation; that is, when it reduces barriers to accessing the electoral process, improves the quality of information and the possibility of informed voter decision-making, and limits opportunities for manipulation and distortion of the public will. Within the framework of digital governance, one of the key goals is to "simplify and make public processes more intelligent" in order to enhance citizens' experiences and increase participation (Tavakoli-Rad & Sadat Miri, 2021). In elections, the same logic can justify the use of intelligent systems to guide voters, automatically answer official questions, remind them of requirements and deadlines, and facilitate equal access to reliable information, provided that these tools remain consistent with "administrative neutrality" and the prohibition of discrimination (Rajaei & Amiri, 2025).

The quality of political participation depends on citizens' level of access to accurate and reliable information. Artificial intelligence, particularly natural language processing, can be effective in filtering and classifying large amounts of data, detecting patterns of misleading-information dissemination, and providing evidence-based warnings. However, this same capacity, in the absence of legal safeguards, can be transformed into "public perception engineering" and manipulation of voter behavior. The literature on "accountability and transparency" in public governance emphasizes that the use of intelligent systems must be accompanied by measurable accountability and transparency mechanisms to ensure that citizens' rights are not undermined (Hernandez, 2024; López-López et al., 2023; Martos, 2023).

In contemporary theories of technological regulation, data-driven decision-making can reproduce inequality because biases in data and models may lead to the exclusion or marginalization of certain groups in the provision of information, monitoring, or distribution of electoral resources (O'Neil, 2016). From a public law

perspective, the theoretical basis of "guaranteeing the right to self-determination" requires that any electoral use of AI be assessed and controlled in advance for its distributive and discriminatory effects, which the administrative law literature on AI presents as a condition of legitimacy and respect for fundamental rights (Carvalho & Rosa, 2024; Gonzalez & Patterson, 2024).

As a result, the theoretical basis of the "right to self-determination" in relation to the use of AI in elections is not technology-centric but rights-centric: technology is justified only to the extent that it enhances free, informed, equal, and trustworthy participation (López-López et al., 2023; Martos, 2023; Tavakoli-Rad & Sadat Miri, 2021).

3.2. Transparency of the Electoral Process

Transparency in elections is not merely a moral or administrative value; it is also one of the pillars of public trust and of the possibility of exercising citizen and institutional oversight over the "integrity of the process." In the transition from e-government to digital governance, transparency extends beyond the "dissemination of information" toward "the ability to trace, evaluate, and explain decisions and processes" (Tavakoli-Rad & Sadat Miri, 2021). For this reason, the use of artificial intelligence in elections is theoretically defensible only when it contributes to transparency or, at a minimum, does not undermine it.

If AI is involved in registration, validation, resource allocation, monitoring, or anomaly detection, it must be possible to trace the inputs, processing logic, and outputs so that a legal observer can audit their accuracy. The literature on "algorithmic transparency" in public governance considers transparency a condition of accountability and the possibility of legal control (Brunner, 2026; López-López et al., 2023; Martos, 2023; Wieringa, 2020). At the domestic level, studies on the implementation of AI in public administration emphasize the need for clear regulatory and legal mechanisms governing data-driven decision-making (Hosseinabadi & Zarefard, 2022; Jabbari & Karim, 2024). Transparency in elections is linked to the "right to objection and review." Wherever the output of an AI system directly or indirectly affects the rights of a candidate or voter for example, through delisting, security alerts, or anomaly detection a legally

comprehensible explanation must be provided to enable effective appeal and judicial or quasi-judicial review. This reflects the "rule of law in technological decisions," which is presented as a structural requirement in the AI administrative law literature (Carvalho & Rosa, 2024; Schneider & Klein, 2023).

Electoral transparency must also be compatible with privacy. From a legal perspective, the ability to provide transparent reports on system performance, including indicators, errors, criteria, and audit results, without disclosing personal data is one of the requirements for balancing "transparency" and "data protection" (Jafari & Rahbarpour, 2017).

Therefore, transparency as a theoretical basis for using artificial intelligence in elections entails the auditability of systems, the explainability of decisions, and the possibility of effective oversight alongside data protection (Brunner, 2026; Hosseinabadi & Zarefard, 2022; Tavakoli-Rad & Sadat Miri, 2021; Wieringa, 2020).

3.3. Ensuring the Speed, Accuracy, and Integrity of Electoral Processes and Results

Administrative efficiency in elections is both a managerial necessity and part of "public trust," because unjustified delays, human error, and implementation inconsistencies can undermine the integrity of the process and acceptance of the results. In the literature on e-government and public administration in Iran, artificial intelligence has been proposed as a tool for improving the quality of public services, increasing the accuracy and speed of decision-making, and reducing errors (Akbari et al., 2024; Mahmoudi et al., 2025).

Applications of AI in participation-data analysis, optimal facility distribution, polling-station workload prediction, and congestion management can increase the speed and orderliness of implementation. However, this speed has legal value only when it is consistent with "competence rules," "equality of opportunity," and "accountability" (Binns, 2024; Kettunen & Kallio, 2025).

Accuracy is important both in data validation, including voter and candidate registration, and in anomaly analysis and counting. However, in sensitive systems, "algorithmic error" can have legal consequences comparable to, and sometimes greater than, human error. Thus, the literature on AI regulation in public administration emphasizes quality-control standards, ex

ante evaluation, and ex post audit (Gonzalez & Patterson, 2024; López-López et al., 2023; Martos, 2023).

In elections, the accuracy of results is not solely a function of counting speed; it is also dependent on security, data integrity, and the system's resistance to cyber threats. Therefore, the relationship between artificial intelligence and "cybersecurity" is structural, and without considering the rules governing security in cyberspace and the risks of computer crime, claims regarding accuracy remain incomplete (Hassanbeigi, 2005). In addition, studies on electronic voting in Iran demonstrate that any reliance on digital tools requires strict standards for design, auditing, and legal trust-building (Takhtaei, 2011). Therefore, "speed, accuracy, and precision" as a theoretical basis are not merely technical functions; rather, they constitute public law objectives of electoral management that must be combined with security, accountability, and respect for citizens' rights (Hassanbeigi, 2005; López-López et al., 2023; Martos, 2023).

4. Application of Artificial Intelligence in the Pre-Election Phase

4.1. Registration and Verification of Information and Documents of Candidates and Voters

One of the first and most sensitive stages of any electoral system is the registration and eligibility-verification stage for candidates and voters. At this stage, a large volume of personal, identity-related, and governmental data, including identification documents, educational certificates, criminal records, security inquiries, and related information, must be collected, reviewed, and verified. In Iran's current traditional and semi-electronic system, this process is conducted mainly manually and with extensive human intervention, which, in addition to consuming considerable time and resources, is susceptible to human error, individual and institutional bias, and even possible corruption (Khosravi et al., 2022; Takhtaei, 2011). Artificial intelligence can transform this stage by providing data-driven, machine-learning-based solutions, but this transformation is not without risk. The main applications of AI in registration and verification can be categorized into several areas: (1) detecting fraud and document forgery using machine vision and matching security patterns; (2) biometric matching, including fingerprints, facial recognition, and iris

recognition, to prevent duplicate registration or identity fraud; (3) cross-validating information by connecting to government databases and performing automatic matching; (4) detecting statistical anomalies in registration patterns that may indicate attempts to infiltrate or manipulate the process; and (5) assisting human observers in decision-making by providing risk scores and evidence-based recommendations (Jabbari & Karim, 2024). In the Iranian legal system, the use of such systems must first comply with the principles and rules governing electoral registration, including the Presidential Election Law, approved in 1985 with subsequent amendments; the Islamic Consultative Assembly Election Law, approved in 1999; the Islamic City and Village Council Election Law, approved in 1999; and the relevant executive regulations. In addition, owing to the data-driven nature of these applications, the Computer Crimes Law, approved in 2009, and data-protection and privacy requirements must also be observed (Fatemi, 2024; Habibi & Homayoun, 2016).

4.1.1. Opportunities, Benefits, and Potential Achievements

From an opportunity perspective, the most important achievements of utilizing artificial intelligence at this stage are:

First: Increasing accuracy and reducing human error. Human errors in reading handwriting, manually matching a photograph with the document holder, or detecting subtle discrepancies in seals and signatures can lead to the erroneous rejection of a candidate's eligibility or the erroneous acceptance of an ineligible individual. Machine-vision and pattern-matching systems, when properly trained on sufficient and diverse data, can reduce diagnostic errors (Hosseinabadi & Zarefard, 2022). For example, in the 2020 Brazilian presidential election, the use of a biometric fingerprint-matching system in more than 70% of polling stations reportedly led to a substantial reduction in reports of identity fraud (Brown & Smith, 2023).

Second: Increased speed and reduced costs. The manual process of reviewing tens of thousands of registration files in Iran can take weeks or even months. Intelligent systems can significantly reduce this time without necessarily reducing the quality of review. This increased speed, in addition to saving public resources,

can also facilitate faster responses to problems and complaints (Foos, 2024; Simoes & MacCarthaigh, 2023).

Third: Uniformity and impartiality in implementation. Human decision-makers, whether consciously or unconsciously, may be influenced by biases, including political, regional, ethnic, or gender biases. Artificial intelligence systems, if trained on unbiased data and accompanied by effective mechanisms for monitoring their outputs, can apply uniform and objective criteria to all registrants. This feature can increase public trust, particularly in an electoral system in which qualification procedures have sometimes been criticized as susceptible to discretionary application (Rajaei & Amiri, 2025).

Fourth: Auditability and reviewability. The outputs of intelligent systems can be stored, reviewed, and retrospectively audited. If a candidate or voter objects to a disqualification, a legal observer can examine the basis on which the system reached that conclusion, including which documents, matches, and anomalies were considered. Such procedural transparency can contribute to fairer proceedings in Iran's judicial and quasi-judicial system, including supervisory boards and the Administrative Court of Justice (López-López et al., 2023; Martos, 2023).

4.1.2. Legal-Technical Challenges, Risks, and Hazards

However, alongside these opportunities, serious challenges and risks also arise:

The first and most important challenge: algorithmic bias. If the historical data used to train an AI model contain human or institutional biases—for example, if individuals with certain characteristics were disproportionately disqualified in previous years—the algorithm may unintentionally learn, reproduce, and potentially amplify those biases. This situation can lead to "statistical discrimination," which conflicts with the principles of equality and administrative justice (Mohebbi & Amiri, 2025; O'Neil, 2016). In the Iranian electoral system, given the complex history of qualification procedures, the risk of algorithmic bias against specific groups, political currents, or regions is significant, and a human-rights- and justice-based impact assessment should precede any implementation.

Second: The challenge of transparency and explainability. Many advanced AI models, particularly deep-learning models, are known as "black boxes"; that

is, their internal decision-making logic is not easily understood or explained to humans, including their designers. If an intelligent system rejects an individual's registration and human observers cannot explain, in plain and legally understandable language, exactly why the decision was made, the citizen's right to effective objection and defense may be violated (Carvalho & Rosa, 2024). In Iranian administrative law, Article 34 of the Constitution and related provisions of the Administrative Procedure Code guarantee access to judicial remedies; the "black-box" nature of an algorithm may undermine the effective exercise of this right.

Third: Privacy and data protection. Intelligent verification of information and documents requires access to large volumes of sensitive personal data, including biometric data, judicial and security records, and family and financial information. If such data are not adequately protected or can be accessed without authorization, citizens' privacy may be violated on a large scale (Jafari & Rahbarpour, 2017). In Iran, despite existing legal provisions emphasizing the protection of privacy, a comprehensive data-protection framework with strong enforcement guarantees remains a significant concern (Fatemi, 2024; Habibi & Homayoun, 2016). Furthermore, the possibility of combining and analyzing voter-registration data with other government databases, such as those of the Civil Registry, law-enforcement bodies, or intelligence institutions, raises concerns regarding "state hyper-surveillance" and the potential misuse of information for purposes beyond elections, such as exerting political pressure (Jasanoff, 2024).

Fourth: Civil and criminal liability arising from errors. Who is responsible for an erroneous output produced by an AI system? If the system mistakenly disqualifies an eligible candidate or confirms an ineligible individual, does responsibility lie with the system designer, the implementing institution, the supervisory authority, or a combination of these actors? (Hekmatnia et al., 2019). In electoral applications, the dimensions of this problem are particularly broad. Traditional principles of civil liability and jurisprudential rules may provide a basis for responsibility, but adapting these rules to automated and learning systems is complex. From a criminal perspective, proving the mental element, such as intent or criminal negligence, in

relation to an algorithmic error can also be difficult (Zakirinia, 2023).

Fifth: Technical dependency and cyber risks. The more registration and verification processes become dependent on intelligent systems, the more disruptive and costly cyberattacks—such as intrusions designed to alter databases, manipulate algorithms, or conduct denial-of-service attacks—may become. Cybersecurity literature in Iran (Hassanbeigi, 2005) and international experiences demonstrate that such threats are real and serious.

In Iran's legal system, the use of AI in electoral registration and verification requires amendments to or broad interpretations of certain laws, as well as the establishment of new regulations. In Iran's current legal system, although legal articles such as Articles 55 to 57 of the Presidential Election Law (approved in 1985) oblige the Ministry of Interior and the Guardian Council to "Checking the documents of the candidates," none of them explicitly imply the use of smart devices in this process, and this issue requires interpretation or the enactment of new laws. The Guardian Council, as a supervisory body, must also establish standards for the "reliability" and "neutrality" of intelligent systems. In addition, the Administrative Court of Justice, as an authority for handling complaints concerning administrative decisions, must invest seriously in "technical knowledge of algorithmic litigation"; that is, judges must be trained to evaluate the outputs of intelligent systems from a legal perspective (Hosseini et al., 2025). In conclusion, artificial intelligence in electoral registration and verification has the potential to significantly improve accuracy, speed, and impartiality. However, without strong legal guarantees concerning algorithmic transparency, elimination of bias, data protection, and clear allocation of responsibility, these technologies may also generate crises of legitimacy and public trust. To benefit from the opportunities and contain the challenges, the Iranian legal system needs either a "specific law on artificial intelligence in elections" or, at minimum, a "comprehensive regulation" based on a risk-oriented and fundamental-rights approach (European, 2025; Rajaei & Amiri, 2025).

4.2. Detecting Fake News and Misleading Information Using Natural Language Processing

In the digital age, perhaps no threat has jeopardized electoral integrity more significantly than fake news and misleading information. Social networks and domestic and foreign messaging platforms have created environments for the rapid and widespread dissemination of fabricated, distorted, or undocumented content that can directly influence voters' attitudes, beliefs, and behavior (Bashir & Ravi, 2025). In Iran's electoral system, given the high concentration of users on messaging applications such as Telegram, Soroush, Eitaa, and Bale, as well as social networks such as Instagram and X, combating fake news has become a vital necessity for ensuring "healthy and informed elections." However, manual and traditional countermeasures cannot adequately respond to the volume and speed of content production in the digital environment. At this point, natural language processing, as a branch of artificial intelligence that enables machines to understand, interpret, and generate human language, can play a key role. The main functions of artificial intelligence based on natural language processing in detecting fake news are:

- (1) **Content analysis:** examining writing style, the presence of internal contradictions, the use of exaggerated or provocative language, unreliable sources, and indicators of automated production.
- (2) **Source analysis:** examining domain authority, publication history, citation to credible sources, and website metrics.
- (3) **Dissemination-network analysis:** identifying virality patterns, the role of influential users, and the speed of dissemination on social networks.
- (4) **Cross-referencing with authoritative databases:** matching claims contained in questionable content with official reports from news agencies, statements by official institutions such as the Ministry of Interior, the Guardian Council, and election headquarters, and relevant fact-checking databases (Akbari et al., 2024; Bashir & Ravi, 2025).

4.2.1. Opportunities, Benefits, and Potential Achievements

Opportunities for using natural language processing to detect fake electoral news in Iran include:

First: Increasing the speed and scale of monitoring.

An intelligent system based on natural language processing can analyze millions of posts, comments, tweets, and messages on a daily basis and separate suspicious content from non-suspicious content. This capability enables broad coverage of Iran's cyberspace, a task that is practically impossible with the limited human resources available to monitoring institutions such as the FATA Police or electoral monitoring bodies (Brown & Smith, 2023).

Second: Reducing dependence on external sources.

Many international verification systems focus primarily on English-language and European-language content and may have limited awareness of Iran's cultural, political, and linguistic contexts. Developing domestic natural language processing systems trained on Persian-language texts, while taking account of dialects, local expressions, and sociopolitical humor, can improve recognition accuracy (Fatemi, 2024; Habibi & Homayoun, 2016).

Third: Transparency and documentation. The system's output can include "risk labels," such as "92% likelihood of being false," "contradictory sources," including links to credible reports refuting a claim, and "alert indicators," such as "invalid source" or "fabricated quotation attributed to an official." This information enables human observers, including legal experts, journalists, and civil-society activists, to make informed assessments and decisions. Such a structure is consistent with the principles of transparency and accountability emphasized in the theoretical foundations (Brunner, 2026; Wieringa, 2020).

Fourth: Proactive prevention. The system can identify patterns of fake-news dissemination at an early stage, even before they become viral, and send rapid alerts to platforms and monitoring institutions. This proactive capability differs fundamentally from traditional "after-the-fact" responses (Gonzalez & Patterson, 2024).

4.2.2. Legal-Technical Challenges, Risks, and Hazards

However, there are also numerous challenges associated with using natural language processing to detect fake electoral news in Iran:

First: The risk of censorship and violation of freedom of speech. The most serious legal challenge is misclassification; that is, an intelligent system may mistakenly label legitimate critical content, political

satire, or an analysis opposing the government as "fake news" or "misleading information." In the Iranian legal system, freedom of speech is protected within the framework of Articles 23, 24, and 25 of the Constitution, although subject to certain legal limitations. However, the expansion of automated "labeling" and "content removal" procedures without effective judicial oversight could become a mechanism for suppressing dissent and creating a "chilling effect" conducive to self-censorship (Hernandez, 2024). This risk is particularly significant in Iran, where the political and media environment has long faced challenges in this area.

Second: Incompatibility with cultural and political contexts. Natural language models trained exclusively on official news texts may fail to understand political humor, irony, indirect quotation, or common codes used in Iranian cyberspace. This inability to understand context can lead to widespread diagnostic errors. Furthermore, current intelligent systems may have difficulty distinguishing "intent"; that is, differentiating between the inadvertent dissemination of false information and the deliberate spread of fake news intended to cause harm (Susskind, 2024). From the perspective of Iranian criminal law, the psychological element, including intent or fault, is decisive in offenses involving the dissemination of falsehoods.

Third: Circumvention of algorithms by human actors. Professional producers of fake news, including both public and private actors, can learn how to craft their content to bypass intelligent-system filters by subtly modifying wording, using manipulated images with provocative text, posting in closed or private groups, or using deceptive hashtags. This creates a continuous "cat-and-mouse game" requiring AI systems to be regularly retrained (O'Neil, 2016).

Fourth: Conflict with privacy and the principle of proportionality. To effectively analyze fake-news dissemination networks, a system may require access to users' behavioral data, including comments, likes, shares, and group memberships. Such extensive surveillance may conflict with the principle of proportionality in public law and human rights. The European human-rights framework has repeatedly emphasized limitations on preventive surveillance of electronic communications without appropriate legal safeguards (Heydargholizadeh et al., 2015). In Iran, Article 25 of the Constitution expressly prohibits

inspection, interception, recording, disclosure, censorship, or withholding of communications except as provided by law. Therefore, any intelligent surveillance system used on social networks to detect fake news requires a clear legal basis and independent judicial oversight.

Fifth: Weak linguistic and technical resources for Persian. Large, labeled, and high-quality datasets for training NLP models in Persian are considerably more limited than those available for English. In addition, inconsistent transliteration practices, dialectal diversity, and informal writing styles in cyberspace can substantially reduce the accuracy of current models (Bashir & Ravi, 2025).

In the Iranian legal system, the use of artificial intelligence to detect fake electoral news raises significant questions under the existing legal framework. On the one hand, computer-crime regulations impose certain obligations concerning the prevention of dissemination of criminal content. On the other hand, no comprehensive upstream document has specified the extent to which such "prevention" may be automated or what legal safeguards must exist to prevent violations of freedom of expression and privacy. Constitutional guarantees, including those relating to freedom of expression and communications, make this area particularly sensitive. It appears that a balanced approach would be to use intelligent systems merely as "alert and prioritization tools" for human observers the "human-in-the-loop" approach rather than as automated mechanisms for content removal. An independent body, such as an AI Ethics Committee for Elections, could also be established to address complaints concerning misclassification (Carvalho & Rosa, 2024; Mutawa & Rashid, 2020).

4.3. Identifying Bots and Trolls on Social Networks

A "bot" refers to an account operated by automated software rather than by a human. A "troll" is a user, usually human but sometimes semi-automated, who operates to provoke, insult, spread misinformation, or disrupt online discussions. During elections, both actors—bots and trolls—can operate in a coordinated manner and on a large scale to saturate cyberspace, amplify false narratives, target opponents, and artificially create or reinforce a perception of "public demand" (Bashir & Ravi, 2025). Iran's electoral system is

no exception to this phenomenon, and reports of extensive bot activity on social media during past elections have been widely circulated. By analyzing behavioral and content patterns, artificial intelligence can identify and potentially neutralize such malicious accounts before they cause serious harm.

The main AI methods for identifying bots and trolls are:

(1) **Analysis of account characteristics:** follower-to-following ratios, account creation dates, similarity of biographies to those of other accounts, use of duplicate or fake profile pictures, and uninterrupted activity.

(2) **Content analysis:** frequent use of duplicate or copied text, sharing of the same links within short intervals, and lack of topic diversity.

(3) **Network analysis:** patterns of following, reposting, and mentioning, the formation of dense clusters of coordinated accounts, and artificial behaviors designed to increase likes and followers.

(4) **Temporal analysis:** posting patterns at specific times, such as sudden bursts of activity, and reaction times to events (Wang & Lee, 2023). Machine-learning models, such as random forests, support vector machines, and deep neural networks, can be trained on these features to distinguish suspicious accounts from ordinary human accounts.

4.3.1. Opportunities, Benefits, and Potential Achievements

Opportunities for using AI to identify bots and trolls in Iranian elections include:

First: Unparalleled scalability and speed. An intelligent system can analyze millions of user accounts in a short period and identify suspicious automated activity with a high degree of accuracy. This speed enables Iranian supervisory institutions, including the FATA Police, the Ministry of Communications, and election headquarters, to respond before waves generated by bots become a "virtual reality" capable of influencing public opinion (Brown & Smith, 2023).

Second: Detecting coordinated influence operations. Many election-related bot attacks are conducted as coordinated operations involving dozens or hundreds of accounts with different profiles, sometimes supporting one candidate and sometimes opposing that candidate, in order to drive public debate toward conflict and polarization. Intelligent systems using network analysis can identify such "coordinated bot networks" even when

each individual account appears to operate independently (Gonzalez & Patterson, 2024).

Third: Adaptive learning capability. As bot operators change their tactics, for example by modifying behavioral patterns to evade detection, AI models can be retrained using new data and their algorithms can be updated. This is a critical requirement because electoral cyber-conflict is dynamic and constantly evolving (Susskind, 2024).

Fourth: Contributing to transparency and trust. If a neutral entity, such as the Guardian Council or the Ministry of Interior, publishes documented, data-based reports concerning bot and troll activity in Iranian cyberspace without disclosing personal information, this could increase public confidence in the integrity of the process by demonstrating that supervisory institutions are actively responding to manipulation (López-López et al., 2023; Martos, 2023).

4.3.2. *Legal-Technical Challenges, Risks, and Hazards*

However, serious challenges and disadvantages also exist:

First: Type I errors, including mistaken identification of human accounts. An AI system may label a real human user whose behavior is somewhat "abnormal," such as a highly active political participant who posts around the clock or an older user who repeatedly posts similar content, as a bot. Deleting or restricting access to such accounts would clearly interfere with those citizens' rights to political participation and freedom of expression (Hernandez, 2024). In the Iranian legal system, this issue is particularly sensitive because accounts belonging to political minorities, civil activists, or critical journalists could potentially be restricted on the pretext of "being bots" without sufficient technical documentation.

Second: Algorithmic transparency and the possibility of appeal. If an account is identified as a "bot" by an intelligent system and subsequently blocked, the account holder should have the right to (a) know the basis on which the decision was made, including the relevant indicators and algorithmic criteria, and (b) object before an independent human authority and request manual review. The absence of such a mechanism may conflict with the right to effective legal remedies (Carvalho & Rosa, 2024).

Third: Circumvention by advanced bots. New generations of bots use advanced artificial intelligence techniques, including large language models and deepfake-image generation, to simulate human behavior. They may post irregularly, participate in diverse discussions, and even generate customized responses. Such bots, sometimes described as "social bots" or "sockpuppets," are increasingly difficult to distinguish from real human users (O'Neil, 2016). Therefore, relying solely on intelligent systems without human supervision is insufficient.

Fourth: Privacy and the scale of surveillance. Like fake-news detection, bot identification may require the system to access large amounts of user behavioral data. Even when such data are "anonymized," aggregation and analysis can reveal highly detailed behavioral patterns, including political preferences, social relationships, waking hours, and potentially psychological characteristics. Creating such a "behavioral profile" for social-media users, regardless of any specific suspicion or complaint, may conflict with human-rights principles, including the right to privacy (Jasanoff, 2024).

In the Iranian legal system, the use of artificial intelligence to identify bots and trolls in elections requires legislation explicitly specifying: (a) which institutions are authorized to use this technology; (b) what technical and legal standards, such as maximum permissible error rates, must be observed; (c) what judicial and civil safeguards exist to protect individuals in the event of erroneous identification; and (d) what will happen to collected data after the elections (Jabbari & Karim, 2024). Existing provisions concerning interception of communications may not directly cover this area because analyzing publicly accessible posts on social media does not necessarily constitute interception.

A practical suggestion is to establish a joint technical-legal committee consisting of representatives of the Ministry of Interior, the Guardian Council, the FATA Police, relevant cyberspace regulatory bodies, civil-society activists, and academics in public law and information technology to design intelligent systems and develop protocols for transparency, objection, accountability, and regular auditing (Takhtaei, 2011).

4.4. Using Artificial Intelligence to Analyze Information-Dissemination Patterns on Social Networks and Identify Foreign Influence Campaigns

In addition to domestic threats, the electoral systems of many countries face cross-border threats and foreign influence campaigns. Foreign state and non-state actors may interfere in a country's electoral process to undermine public trust, strengthen particular political currents, or create instability. Such interference is usually conducted through "covert influence operations" on social networks, including the creation of hundreds or thousands of fake accounts, dissemination of targeted narratives, amplification of specific content through bots and trolls, and exploitation of existing social divisions to maximize impact (Liang, 2024). Artificial intelligence, with its capacity to analyze network patterns and information flows at scale, can identify and track such campaigns.

The main functions of artificial intelligence in this field are:

- (1) **Geotagging and matching temporal patterns:** If a large volume of posts related to Iranian elections suddenly and in a coordinated manner originates from a specific time zone outside Iran, this may constitute an indicator of an externally organized operation.
- (2) **Cross-linguistic content analysis:** identifying narratives first published in a foreign language, such as English, Arabic, or Turkish, on platforms such as X or Facebook and subsequently translated into Persian and republished on domestic networks.
- (3) **Fake-account network analysis:** identifying clusters of fake accounts operating through deceptive profiles, for example, by using the names and images of real Iranians while exhibiting non-human behavioral patterns such as continuous activity, lack of genuine interaction, and repetitive content.
- (4) **Detection of polarization-oriented campaigns:** identifying patterns intended to maximize polarization between supporters and opponents and reduce social capital (Bashir & Ravi, 2025; Wang & Lee, 2023).

4.4.1. Opportunities, Benefits, and Potential Achievements

Opportunities for using artificial intelligence to detect foreign influence in Iranian elections include:

First: Strengthening national independence and security. Iran has long been exposed to information and

cyber threats from foreign actors. The ability to detect and counter foreign influence campaigns in elections, in addition to safeguarding the integrity of the domestic process, is important for national sovereignty and national security (Liang, 2024). Domestic intelligent systems may also be better positioned to analyze the specific linguistic and behavioral patterns of Iran's cyberspace.

Second: International transparency and public diplomacy. If Iran can publish documented and data-based reports concerning foreign interference in its elections, while observing relevant security and intelligence considerations, such reports may contribute to public diplomacy and international responses. This transparency may also increase domestic trust by demonstrating that government and electoral institutions are actively addressing external threats (López-López et al., 2023; Martos, 2023).

Third: Coordination with international platforms. Intelligent systems for detecting foreign influence could facilitate more effective cooperation with major platforms such as Meta, X, and Telegram, whereby Iranian authorities identify suspicious patterns and report them to the relevant platform, which may then act according to its internal policies, for example, by coordinating the removal of fake accounts. Such cooperation, although difficult because of sanctions and political tensions, remains conceivable (Brown & Smith, 2023).

Fourth: Creating deterrence. If foreign actors know that Iran possesses effective intelligent systems capable of detecting and documenting influence campaigns, they may refrain from carrying out such operations or reduce their scope and intensity. Deterrence in cyberspace is one of the functions of technological power (Hassanbeigi, 2005).

4.4.2. Legal-Technical Challenges, Risks, and Hazards

However, the challenges of using artificial intelligence to detect foreign influence in Iranian elections include:

First: Misdiagnosis and the risk of international tensions. If an intelligent system incorrectly labels a pattern of behavior for example, the activities of an Iranian opposition group abroad as a "foreign influence campaign supported by a foreign state," the resulting allegation could generate serious diplomatic consequences. Accusing a foreign state without strong

and verifiable evidence raises significant international-law concerns. Therefore, any claim of foreign interference must be based on robust evidence and should extend beyond simple statistical patterns (Liang, 2024).

Second: Abuse of the accusation of "foreign influence" to suppress domestic dissent. In closed or semi-closed political systems, accusations of "collaboration with foreigners" or "foreign influence" may be used to restrict domestic dissent and civil liberties. This risk also exists in Iran: critical political movements or civil and media activists could potentially be identified or restricted under the pretext of "foreign influence" without sufficient substantiated evidence. Distinguishing between "legitimate domestic criticism" and "foreign influence operations" is one of the most difficult legal and political challenges (Hernandez, 2024).

Third: Manipulation of indicators by professional actors. Professional foreign actors may understand the patterns intelligent systems are designed to detect and adjust their tactics accordingly, for example, by using intermediary servers in multiple countries, varying temporal patterns, and designing content to resemble domestic communications (O'Neil, 2016). This is a continuously evolving contest, and no intelligent system can claim complete resistance to circumvention.

Fourth: Limitations of Iranian cyber sovereignty. Despite Iran's efforts to develop national information infrastructure, a significant proportion of Iranian social-media traffic continues to pass through foreign platforms such as Telegram, Instagram, and X, whose internal infrastructures are not accessible to Iranian authorities. Consequently, Iranian intelligent systems designed to analyze patterns and identify external influence may be largely limited to publicly accessible data made available by these platforms and may lack direct access to metadata and internal content data required for more comprehensive analysis (Bashir & Ravi, 2025).

In the Iranian legal system, countering foreign influence in elections is supported by various upstream documents and laws concerning computer crimes and national security. However, the use of AI for this purpose requires clear and disciplined rules. Among other matters, it must be specified which institution is responsible for implementation, what evidentiary threshold is sufficient to establish "foreign interference," and what judicial guarantees exist to prevent abuse of

this authority. The preferable legal approach is to distinguish among three layers: (1) detection of suspicious patterns by AI, which is a technical task; (2) human and judicial assessment of evidence to determine foreign origin, which is a legal and intelligence task; and (3) a proportionate response, ranging from diplomatic to criminal measures, that must be undertaken by competent institutions in accordance with law (Gonzalez & Patterson, 2024; Hosseinabadi & Zarefard, 2022).

4.5. Using Artificial Intelligence to Provide Accurate and Reliable Information to Voters and Automatically Counter False and Misleading Information

The final key use of AI in the pre-election phase is not limited to behind-the-scenes functions such as verification or threat detection but extends to direct engagement with voters: providing accurate, timely, and personalized information and actively countering misinformation during electoral campaigns. In Iran's electoral system, which includes a sizable young and digitally literate population, this application can foster informed participation and enhance the integrity of the process.

The main artificial intelligence methods in this field are:

A) Automated question-and-answer systems: Designing intelligent conversational agents based on natural language processing and large language models that can answer common questions from voters, such as: "What documents are required for registration?" "Where is my polling station?" "Who are the candidates in my constituency?" "What are the differences among candidates' programs?" and "How can I register an objection?" These systems can operate 24 hours a day, support multiple languages, including Persian, Azerbaijani, Kurdish, and Arabic, and reduce pressure on election headquarters and call centers (Bashir & Ravi, 2025; Muppasani et al., 2023).

B) Information-recommendation systems: Based on a user's interests and search history, while respecting privacy, the system can recommend educational materials, candidate programs, expert analyses, and independent observer reports in a targeted manner so that voters can make more informed decisions. Such systems can also be designed to avoid the "filter bubble" that exposes users only to content consistent with their existing beliefs and instead present a diversity of viewpoints (Susskind, 2024).

C) Automatic labeling of suspicious content: As discussed in the preceding section, NLP systems can analyze posts, videos, and images in real time and, if they detect false or misleading information, display a warning label to the user, for example: "Reliable sources have not verified this claim; click for more information." Unlike content removal, which entails risks of censorship, this method seeks to preserve freedom of expression while making users aware of potential risks associated with the content. Experiences of major platforms during recent elections illustrate the potential role of such labeling mechanisms in reducing belief in fake news. (Carvalho & Rosa, 2024).

D) Sending proactive alerts: If an intelligent system detects that particularly dangerous content for example, false information regarding the date or location of voting or a rumor concerning widespread fraud is becoming viral, it can automatically send proactive alerts through text messages, in-app notifications, or banners on widely used websites to users who may be exposed to it. These alerts should include access to an authoritative source, such as the Ministry of Interior or the Guardian Council, for verification (Gonzalez & Patterson, 2024).

4.5.1. Opportunities, Benefits, and Potential Achievements

Opportunities for using AI to provide accurate and reliable information to voters and automatically counter false and misleading information include:

First: Increasing access and reducing the information gap. Automated question-and-answer systems can provide necessary information more equally, particularly to older, less digitally literate, or disadvantaged voters who may have limited access to diverse information sources. This strengthens the rights to information and informed participation (Mostafavi Ardebili et al., 2023).

Second: Saving the costs and time of executive headquarters. Manually answering millions of questions from voters across Iran would require thousands of trained employees, multiple call centers, and considerable financial resources. An intelligent chatbot developed by the Ministry of Interior's election headquarters could assume a significant proportion of this burden at lower cost, freeing human resources to address more complex issues (Tavakoli-Rad & Sadat Miri, 2021).

Third: Reducing the impact of misinformation in real time. Labeling and preventive-warning systems enable countermeasures to be initiated as false information begins to spread. On social media, response speed is crucial because a rumor can reach a nationwide audience within hours. Traditional approaches based on delayed denial are therefore increasingly ineffective. AI can help narrow this temporal gap (Wang & Lee, 2023).

Fourth: Increased public trust. When voters observe that electoral institutions are actively, intelligently, and transparently seeking to provide accurate information and counter misinformation without resorting to indiscriminate censorship, their confidence in the integrity and legitimacy of the overall process may increase. Trust is a vital asset of any healthy electoral system (Brunner, 2026; Wieringa, 2020).

Fifth: Collecting data for future improvement. Voter questions, search patterns, and recurrent content encountered by the system constitute valuable sources of data that can be used to improve public education, design campaigns, and potentially revise electoral laws and procedures in future cycles. This creates a "positive feedback loop" (Binns, 2024).

4.5.2. Legal-Technical Challenges, Risks, and Hazards

However, the challenges of using AI to provide accurate and reliable information to voters and automatically counter false and misleading information include:

First: The risk of the system itself providing incorrect information. Large language models are susceptible to a phenomenon commonly referred to as "hallucination"; that is, they may provide information with high confidence despite its factual inaccuracy. If an intelligent chatbot operated by an election headquarters mistakenly tells a voter, for example, that required documents have expired or that a polling location is closed on election day, the consequences could be serious. Therefore, using such systems without closed-loop human oversight and without connection to authoritative verification databases is highly risky (Susskind, 2024).

Second: Privacy and unwanted profiling. Information-recommendation systems that personalize content based on users' online behavior inevitably process large amounts of personal data, including search history, reading time, political interests, and potentially attitudes toward candidates. If such data are disclosed or misused,

this could constitute a serious breach of privacy. Furthermore, aggregation of these data could create highly detailed "political profiles" of individual citizens, which might subsequently be used for purposes beyond elections, including discriminatory or coercive purposes. This constitutes a serious concern in political systems characterized by extensive state surveillance (Jasanoff, 2024). In Iran, this concern is particularly significant because government and security institutions may have extensive access to data infrastructure.

Third: Algorithmic bias in recommended content. A recommender system may, consciously through design choices or unconsciously through biased training data, favor certain candidates, political currents, or viewpoints over others. For example, it may rank government-supporting content more prominently while suppressing critical material. This would conflict with the principles of administrative impartiality and equal opportunities in electoral campaigning (Carvalho & Rosa, 2024). In the Iranian legal system, although legislation may not explicitly refer to algorithmic impartiality, general principles of administrative law and election-campaign rules requiring government institutions to remain impartial can provide a basis for requiring designers to identify and eliminate systematic bias.

Fourth: Iran's linguistic and cultural diversity. Iran is a multilingual and multicultural country. An intelligent system trained exclusively on standard Persian may perform poorly in understanding inquiries in Azerbaijani, Turkic, Kurdish, Arabic, Baluchi, or local Persian dialects. This could lead to "unintentional discrimination" against non-Persian-speaking ethnic groups and regions and undermine equal access to information. Developing multilingual models is costly but necessary (Bashir & Ravi, 2025).

Fifth: Immaturity of technology for politically sensitive applications. Advanced chatbot technology has not yet reached a level at which it can be fully trusted in highly sensitive political areas, such as answering interpretive questions concerning electoral laws, candidate eligibility, or supervisory decisions. A system may provide ambiguous, incorrect, or potentially harmful answers when faced with sensitive questions. Until the technology is sufficiently mature and quality-assurance and auditing protocols are developed, it is preferable to limit the scope of such systems to factual

and non-interpretive questions, including guidance concerning procedures, times, locations, and neutral factual information, while leaving interpretive responses to trained human officials (López-López et al., 2023; Martos, 2023).

In the Iranian legal system, specific regulations should govern the use of AI in providing information to voters through chatbots, recommender systems, and labeling tools. Such regulations should address at least the following matters: (1) requiring full transparency concerning the artificial nature of the system so that users know they are interacting with a machine rather than a human; (2) designating the entity responsible for training, deploying, and updating the system, most likely the Ministry of Interior under the supervision of the Guardian Council; (3) ensuring impartiality and the absence of bias through regular and independent audits; (4) establishing human objection and review mechanisms for users who believe they have received incorrect or misleading information; (5) ensuring full compliance with data-protection and privacy requirements, particularly by avoiding retention of personal data beyond what is necessary and prohibiting its use for unrelated purposes; and (6) specifying civil and criminal liability in the event of damage resulting from system errors. One possible solution is the development of comprehensive digital-election communication regulations by the competent authorities (European, 2025; Hosseini et al., 2025).

5. Conclusion

The studies conducted indicate that AI, through its introduction into electoral processes, has created significant capacities for increasing the accuracy, speed, transparency, and efficiency of election management and can play an effective role across various stages, from registration and authentication to electoral monitoring. However, the development of this technology, alongside its opportunities, also generates significant legal challenges, including violations of privacy, algorithmic bias, reduced transparency, ambiguity in accountability, and threats to fundamental rights and freedoms. Accordingly, the use of AI in electoral processes can contribute to achieving desirable governance objectives when it is implemented within the framework of public law principles, including the rule of law, transparency, accountability, protection of citizens' rights, and

effective oversight of the performance of intelligent systems. Consequently, the successful integration of this technology into the electoral system depends less on technical advancement alone than on the existence of an appropriate legal framework for regulating, monitoring, and ensuring its responsible use.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

- Akbari, I., Vaezi, Aslipour, Abdolhosseinzadeh, Shahraini, & Seyed, M. (2024). Identifying and Modeling the Functions of Artificial Intelligence in Improving the Efficiency of the Administrative System and Providing Public Services. *Iranian Public Administration Studies*, 7(2), 111-147. <https://doi.org/10.22034/jipas.2024.401497.1607>
- Bashir, & Ravi. (2025). A Systematic Review of Strategic Governance Frameworks and Mechanisms of Artificial Intelligence in Studies from 2017-2025. *Cyberspace and Social Media Studies*, 2(3), 9-54. <https://doi.org/10.22083/cssms.2025.538964.1067>

- Binns, R. (2024). AI in Public Administration: Combating Corruption through Data Analytics. *Journal of Technology and Law*, 18(3), 77-94.
- Brown, E., & Smith, R. (2023). Artificial Intelligence in Public Administration: International Experiences. *Public Administration Review*, 83(5), 1456-1468.
- Brunner, E. (2026). *Algorithmic Transparency as a Due Process Requirement in Automated Decision-Making*. <https://doi.org/10.2139/ssrn.5997154>
- Carvalho, A., & Rosa, L. (2024). Artificial Intelligence and Administrative Law: A New Paradigm. *Cambridge AI Law Journal*, 5(1), 55.
- European, C. (2025). *AI and Fundamental Rights: Regulatory Approaches in the EU*.
- Fatemi. (2024). Theoretical Approaches Governing the Determination of the Scope of the Right to Privacy and Its Impact on the Principles Governing the Right to Privacy in the Digital Space. *Legal Research*, e187404. <https://doi.org/10.48300/jlr.2024.431431.2526>
- Fitzgerald, J. (2024). Privacy Concerns in the Use of AI for Anti-Corruption Efforts. *International Journal of Privacy Law*, 29(1), 55-70.
- Foos, F. (2024). The Use of AI by Election Campaigns. *LSE Public Policy Review*, 3(3), 1-8. <https://doi.org/10.31389/lseppr.112>
- Gonzalez, M., & Patterson, L. (2024). Regulating AI in Public Administration: Challenges and Policy Options. *Journal of International Public Policy*, 18(1), 23-41.
- Habibi, H., & Homayoun. (2016). The Right to Privacy in Social Networks. *Legal Research Quarterly*, 19(75), 39-64.
- Hassanbeigi, E. (2005). *Law and Security in Cyberspace*. Abrar Moaser International Studies and Research Cultural Institute.
- Hekmatnia, M., Mohammadi, M., & Vathighi, M. (2019). Civil Liability Arising from the Production of Autonomous Artificial Intelligence-Based Robots. *Islamic Law*, 15(60), 231-255.
- Hernandez, A. (2024). Ethical and Legal Challenges in AI-Driven Governance. *Ethics and Technology Review*, 11(2), 112-125.
- Heydargholizadeh, Abedini, & Raisi. (2015). Privacy and the Obligation to Respect It in the Jurisprudence of the European Court of Human Rights. *Islamic human rights studies*, 8(4), 23-41.
- Hosseinalbadi, S., & Zarefard, M. (2022). Application of Artificial Intelligence in Electronic Surveillance and Increasing Transparency of Affairs.
- Hosseini, M., Asiai, Faghih, L., & Farhang. (2025). Principles and Requirements of Exploiting the Capacity of Artificial Intelligence in Iranian Administrative Law and the Legal System of the European Union. *Quarterly Scientific Research Journal of Administrative Law*, 12(43), 43-75. <https://doi.org/10.66224/qjal.12.43.43>
- Jabbari, M., & Karim, V. (2024). Legal Issues of Implementing Artificial Intelligence in Public Administration: A Case Study of Iran. *International Journal of Administrative Law*, 32(1), 78-92.
- Jafari, & Rahbarpour. (2017). Civil Liability Arising from Data Privacy Violations in Imami Jurisprudence and Statutory Law. *Private Law Research*, 5(17), 43-74. <https://doi.org/10.22054/jplr.2017.7404>
- Jalali Farahani, A. H., & Bagheri Asl, R. (2008). Social Prevention of Cybercrimes. *Rahavard Noor Quarterly Journal of Information and Librarianship*(24), 41-58.
- Jasanoff, S. (2024). Data Privacy Laws and AI: A Global Review.
- Kettunen, P., & Kallio, J. (2025). Smart State and the Integration of AI in Public Sector Decision-Making. *International Review of Administrative Sciences*, 91(2), 312-330.

- Khosravi, Tayebitavkal, Mansourian, & Naserali. (2022). Challenges and Strategies of E-Government Towards Realizing Democracy. *Contemporary Political Essays*, 46(13), 59-83.
- Liang, P. (2024). Social Credit Systems and AI-Based Governance in China: A Comparative Study. *Harvard Law Review*, 137(2), 320-345.
- López-López, P. C., Barredo-Ibáñez, D., & Jaráiz-Gulías, E. (2023). Research on Digital Political Communication: Electoral Campaigns, Disinformation, and Artificial Intelligence. *Societies*, 13(5), 126. <https://doi.org/10.3390/soc13050126>
- Mahmoudi, Akbari, & Iman. (2025). *Governance of Artificial Intelligence (6): Application of Artificial Intelligence in Improving Public Services*. <https://doi.org/10.22034/report.mrc.2025.1404.33.3.20739>
- Martos, J. A. M. (2023). Inteligencia Artificial y Derechos de Participación Política. *De Lege Ferenda*(1), 34-55. <https://doi.org/10.30827/dlf.1.2023.28552>
- Mehdi, A. (2025). An Analysis of the Challenges and Legal Solutions for Implementing Artificial Intelligence in the Iranian Administrative System. (42), 205-229.
- Mohebbi, D., & Amiri, A. (2025). Legal and Ethical Challenges Related to the Use of Artificial Intelligence in the Administrative Justice System. *Legal Studies in Digital Age*, 4(1), 1-8. <https://doi.org/10.61838/kman.lsda.549>
- Mostafavi Ardebili, S. M. M., Taghizadeh, A., Rahmatifar, & Samaneh. (2023). The Impact of Artificial Intelligence on the International Human Rights System. *Law of New Technologies*, 8(4), 86-100.
- Muppasani, B., Pallagani, V., Lakkaraju, K., Lei, S., Srivastava, B., Robertson, B., & Narayanan, V. (2023). On Safe and Usable Chatbots for Promoting Voter Participation. *Ai Magazine*, 44(3), 240-247. <https://doi.org/10.1002/aaai.12109>
- Mutawa, M. A., & Rashid, H. (2020). *Comprehensive Review on the Challenges that Impact Artificial Intelligence Applications in the Public Sector* Proceedings of the 5th NA International Conference on Industrial Engineering and Operations Management,
- O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group.
- Pavlidis, G., & Kastanas, I. (2026). *Algorithmic Administration and the EU AI Act: Legal Principles for Public Sector Use of AI*. <https://doi.org/10.48550/arXiv.2604.22765>
- Rajaei, M., & Amiri, A. (2025). Public Law Challenges in Protecting Human Digital Rights in the Age of Artificial Intelligence. *Legal Studies in Digital Age*, 4(3), 1-7. <https://doi.org/10.61838/kman.lsda.549>
- Schneider, J., & Klein, M. (2023). Legal Implications of Artificial Intelligence in Administrative Systems. *Harvard Law Review*, 139(4), 789-804.
- Simoes, S., & MacCarthaigh, M. (2023). *AI and Core Electoral Processes: Mapping the Horizons*. <https://doi.org/10.48550/arXiv.2302.03774>
- Susskind, R. (2024). *Artificial Intelligence and the Rule of Law*. Oxford University Press.
- Takhtaei, B. (2011). *Analysis of End-to-End Electronic Voting Systems* Sharif University of Technology].
- Tavakoli-Rad, R., & Sadat Miri, H. (2021). Governance Transformation: From E-Government to Digital Governance. *Journal of Transcendental Governance*, 2(3), 115-162.
- Wang, Y., & Lee, M. (2023). Artificial Intelligence in Judicial Systems: A Global Perspective. *International Journal of Law and Technology*, 11(3), 90-108.
- Wieringa, M. (2020). *What to Account for When Accounting for Algorithms: A Systematic Literature Review on Algorithmic Accountability* Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, <https://doi.org/10.1145/3351095.3372833>
- Zakirinia, H. (2023). The Nature and Basis of Civil Liability Arising from Artificial Intelligence in Iranian and European Union Law. *Journal of Private Law*, 20(1), 135-152. <https://doi.org/10.22059/jolt.2023.356703.1007186>