Applications of Artificial Intelligence in the Election Phase within the Iranian Electoral System

1. Davoud Mohebbi: Assistant Professor, Department of Public Law, Faculty of Law, University of Qom, Qom, Iran
2. Ali Amiri *: Master's Student, Department of Public Law, Faculty of Law, University of Qom, Qom, Iran

*Correspondence: a.amiri@stu.qom.ac.ir

Abstract

The development of artificial intelligence-based technologies has created new opportunities for the management and oversight of the electoral process. The election stage, from the start of voting to the counting and aggregation of results, is one of the most important stages of the electoral process because it directly affects the health, integrity, and validity of the votes. At this stage, artificial intelligence can improve the efficiency, speed, and integrity of the election process by predicting participation rates, optimally allocating ballot boxes, ballots, and human resources, managing unforeseen crises, monitoring vote-counting, analyzing election data, and identifying statistical anomalies. However, this technology faces challenges such as algorithmic error, bias in resource allocation, privacy violations, threats to vote confidentiality, lack of algorithmic transparency, data security risks, and the complexity of Legal responsibility arising from errors in intelligent systems. This study examines the opportunities and challenges of using artificial intelligence in elections in the Iranian legal system, using a descriptive-analytical method and library resources. Research findings show that artificial intelligence can play an effective role in promoting the health and efficiency of elections by optimizing the management of electoral resources and creating new capacities for monitoring and detecting anomalies; however, the legitimate and responsible use of this technology requires adherence to the principles of transparency, impartiality, accountability, human oversight, protection of personal data, and ensuring the confidentiality of votes. Therefore, the use of artificial intelligence during the election phase in Iran must be carried out within a legal and institutional framework that, while taking advantage of technological capabilities, protects citizens' electoral rights and the integrity of the voting process.

Keywords: Algorithmic Transparency, Artificial Intelligence, Electoral Monitoring, Holding Elections, Iranian Electoral System, Public Law.

Received: 12 May 2026
Revised: 15 August 2026
Accepted: 23 August 2026
Initial Publication: 28 August 2026
Final Publication: 01 September 2027

Citation: Mohebbi, D., & Amiri, A. (2027). An Examination of the Offense of Unlawful Occupation of National Lands in Iran and England. *Legal Studies in Digital Age,* 6(5), 1-12.

1. Introduction

Elections, as one of the most important mechanisms for citizens' political participation and the realization of the public will, require adherence to principles such as integrity, transparency, impartiality, security, equality, and public trust. In this regard, the stage during which elections are held is particularly sensitive because, from the beginning of voting to the counting and

aggregation of results, executive and supervisory measures are directly related to the process of obtaining and counting citizens' votes, and any error, disruption, or intervention at this stage can affect the authenticity of votes and the validity of election results (Khosravi, 2009; Takhtaei, 2011). In the Iranian electoral system, the election stage includes a range of activities that begin with executive operations at polling stations, voter authentication, and receipt of votes, and continue with monitoring the voting process, preliminary counting, and sending results to aggregation centers. The geographical distribution of polling stations, the large volume of electoral data, and the need to manage human and logistical resources simultaneously have led to the use of modern technologies to increase efficiency and reduce human error. Meanwhile, artificial intelligence, with its ability to process large volumes of data and identify complex patterns, can play an effective role in managing electoral resources and monitoring vote counting and aggregation (Akbari et al., 2024). One of the most important applications of artificial intelligence during elections is predicting participation rates and optimally allocating resources. Intelligent algorithms can predict likely participation levels at different polling stations by analyzing historical data, demographic characteristics, and real-time information and, based on this, adjust the number of ballot boxes, ballot papers, and required human resources. This capability can prevent long queues, resource shortages, and the uneven distribution of facilities and improve the efficiency of election management (Akbari et al., 2024; Binns, 2024). Using intelligent models to simulate different scenarios and predict possible crises can also improve the electoral system's ability to handle unforeseen events (Gonzalez & Patterson, 2024). Another important application of AI at this stage is monitoring and analyzing results and detecting possible anomalies in vote statistics and the counting process. The vast volume of data generated across polling stations makes it difficult and time-consuming to review everything manually. AI can identify unusual patterns using data analysis and anomaly-detection methods and flag suspicious cases for closer inspection by human observers (Khosravi, 2009). The use of statistical analysis, clustering of polling stations, monitoring the temporal trend of results entry, and matching data recorded in the minutes with information from central systems are among the capacities that can help strengthen monitoring of the counting and aggregation process (Gonzalez & Patterson, 2024; Kettunen & Kallio, 2025; Susskind, 2024). Despite these capabilities, using AI during elections comes with significant legal and technical challenges. Algorithmic errors may lead to the incorrect identification of a polling station or the omission of a genuine anomaly, thereby affecting public confidence in the electoral process. Relying on historical data for automated decisions can also introduce algorithmic bias and result in an unequal distribution of electoral resources. On the other hand, using extensive data to manage and monitor elections raises the need to respect privacy and protect citizens' data (Fatemi, 2024; Habibi & Homayoun, 2016; O'Neil, 2016). At another level, the lack of algorithmic transparency and the transformation of intelligent systems into "black boxes" can limit independent evaluation and oversight of technological decisions (Carvalho & Rosa, 2024). Meanwhile, ballot secrecy is fundamental. Any use of artificial intelligence to monitor and analyze the electoral process should not allow a connection to be established between a voter's identity and their choice. Therefore, data analysis should be carried out at an aggregate level as much as possible, and the processing or storage of information that allows for the identification of individual votes should be prevented (Khosravi, 2009). Therefore, artificial intelligence at this stage must be designed to support electoral integrity and efficiency rather than becoming a factor that threatens electoral rights and public trust. Accordingly, the main issue of the present study is what opportunities artificial intelligence provides for improving the electoral process in the Iranian legal system and what challenges and legal requirements its use entails. The present study, using a descriptive-analytical approach, first examines the most important applications of artificial intelligence during elections, including predicting participation and allocating resources, as well as monitoring results and detecting anomalies; then analyzes the opportunities and benefits of these applications and the legal and technical challenges and risks arising from them; and finally examines the legal and institutional requirements necessary for the responsible, transparent, and accountable use of artificial intelligence in the electoral process in Iran.

2. Legal Basis for Using Artificial Intelligence in Elections

2.1. Laws Governing the Use of Artificial Intelligence in Holding Elections in Comparative Law

In comparative law, the "legal foundations" for the use of AI in areas of governance, particularly in sensitive areas such as elections, can generally be traced to three categories of regulation: (a) specific regulations on artificial intelligence, (b) general

regulations concerning fundamental rights and data protection, and (c) rules concerning the responsibility and accountability of the state and contractors. European policy reports and documents emphasize that the use of AI in the public sector should be formulated within the framework of a "risk-based regulatory approach"; that is, different obligations concerning transparency, human oversight, impact assessment, and auditing should be imposed depending on the level of risk to fundamental rights and public trust (European Commission, 2024, 2025). The AI administrative law literature also frames this transition as a "new paradigm" that shifts classical public administration rules toward data-driven accountability standards (Carvalho & Rosa, 2024; Crawford, 2024). In many applications, AI's data-centric nature immediately triggers debates over privacy and data protection laws. Global reviews of privacy and AI law show that legislators regard data protection not as a secondary issue but as a condition for the legitimacy of governance applications (Fitzgerald, 2024; Jasanoff, 2024). In various applications, AI's data-centric nature immediately activates debates over privacy and data protection laws. Global reviews of privacy and AI law show that comparative legislators regard data protection not as a secondary issue but as a condition for the legitimacy of governance applications (Fitzgerald, 2024; Jasanoff, 2024). From the perspective of responsibility theory, "shared responsibility" between the government, technical actors, and contractors is proposed as the legal basis for controlling the risks associated with decision-making systems (Smith, 2024). In comparative law, "algorithmic transparency" and "institutional accountability" are proposed as fundamental requirements for accepting intelligent systems in the public sector. This approach is particularly important for elections because any disruption in legal controllability can undermine public trust (Brunner, 2026; López-López et al., 2023; Martos, 2023; Wieringa, 2020). In conclusion, the comparative legal basis is not simply "permission to use" artificial intelligence, but rather a set of provisions, restrictions, and guarantees imposed on governance applications to protect fundamental rights and public trust.

2.2. Laws Governing the Use of Artificial Intelligence in Holding Elections in Iranian Law

In Iranian law, it can be said that a "specific comprehensive law" on AI in elections has not yet been established; however, reliable legal foundations can be derived from a set of existing rules: (a) rules and requirements of information technology and cybersecurity law, (b) rules concerning privacy and data protection, (c) rules concerning civil liability arising from system errors, and (d) studies and legal frameworks concerning electronic elections that can serve as a regulatory platform for AI applications in elections. Any electoral application of artificial intelligence faces cyber risks because it relies on data and networks. Iranian legal literature on cybersecurity and computer crimes emphasizes the need to ensure the confidentiality, integrity, and availability of data and systems and considers these requirements fundamental to digital services and processes (Aalipour, 2016). Familiarity with international cybercrime instruments and their underlying legal logic is also useful for designing prevention and response mechanisms in sensitive digital processes (Jalali Farahani & Bagheri Asl, 2007). The use of AI in elections often requires the personal data of voters and candidates. Accordingly, the legal basis should be sought in privacy rules and the liability arising from their violation. In Imami jurisprudence and statutory law, data privacy violations can give rise to civil liability, and this proposition plays a direct role in analyzing data-driven electoral applications (Haddadpour, 2022; Jafari & Rahbarpour, 2017).

Furthermore, studies on the status of data and privacy laws and regulations in Iran show that, even in the absence of a comprehensive law, scattered rules can form the basis for obligations concerning data collection, storage, and processing (Fatemi, 2024; Habibi & Homayoun, 2016). A key focus of the legal foundations is determining liability for errors or losses caused by automated and intelligent systems. In domestic literature, civil liability arising from the production and use of AI-based autonomous robots has been analyzed as an emerging issue and can also serve as a basis for analyzing the liability of intelligent electoral systems by analogy (Hekmatnia et al., 2019). At the public administration level, studies of AI administrative law emphasize the need for clear rules concerning liability, oversight, and risk control. An important part of the legal basis for AI applications in elections can be explained through studies of "electronic elections," since many of the relevant concerns—trust, auditability, security, vote authenticity, counting accuracy, and objection mechanisms—have already been formulated in this area (Binns, 2024; Michael, 2023). From this perspective, Iran's legal basis for AI in elections should be viewed as "layered": first, the security and cyber layer; then, the data protection and privacy layer; followed by the responsibility

and accountability layer; and finally, the digital election-specific rules layer, which has the potential to accommodate the expansion of intelligent applications. In conclusion, Iran's legal basis for the use of AI in elections is currently more "inferential and hybrid," relying on existing rules concerning information technology and cybersecurity, privacy and civil liability, and the administrative law literature on AI in Iran, which emphasizes the need for a legal and regulatory framework.

2.3. Application of Artificial Intelligence During Elections

Continuing the examination of artificial intelligence applications in the electoral process, after analyzing the pre-election phase (registration, verification, fake news detection, bot and troll identification, foreign influence analysis, and providing information to voters), it is now necessary to consider the election stage. This phase covers the period from the start of voting until the final announcement of the results. From the perspective of public law, it is the most sensitive point of contact between technology and electoral integrity because any disruption, error, or abuse at this stage can directly undermine the authenticity of votes and the legitimacy of the entire election (Khosravi, 2009; Takhtaei, 2011). In the Iranian electoral system, this stage mainly includes executive operations at polling stations (authentication, vote collection, monitoring, and preliminary counting), logistics management (distribution of ballot papers and ballot boxes), and sending count data to aggregation centers. Artificial intelligence can play a role in two main areas at this stage: first, predicting participation and optimally allocating resources, which helps manage polling stations and reduce irregularities; and second, monitoring and analyzing intermediate results and detecting anomalies, which enables early warnings to human observers. Both applications, if implemented in accordance with the principles of transparency, impartiality, and security, can increase electoral efficiency and integrity. However, if legal guarantees are ignored, they may become tools of distrust or manipulation.

2.4. Participation Forecast, Data-Based Allocation of Ballot Boxes and Human Resources

One constant challenge for election administration institutions—in Iran, the Ministry of Interior and provincial and municipal election headquarters—is the unbalanced distribution of resources among polling stations. In many electoral districts, some polling stations face a high density of voters, resulting in long lines, shortages of ballot papers, and fatigue among officials, while others experience very low turnout, resulting in wasted resources and idle human resources. This inequality not only undermines citizens' electoral experience but may also reduce participation due to discouragement caused by long lines or raise doubts about the integrity of the process (Akbari et al., 2024). Using historical, demographic, and real-time data, artificial intelligence can accurately predict participation levels at each polling station and, based on these predictions, optimize the allocation of ballot boxes, ballot papers, human resources, and other resources. This article describes the main applications, opportunities, challenges, and legal requirements in this area.

3. Main Applications of AI in Forecasting and Resource Allocation

1. **Predicting turnout at each polling station:** Machine learning algorithms, such as logistic regression, random forest, gradient boosting, or deep neural networks, are trained on data from several previous election periods. Input data include the number of registered voters in the precinct, past turnout patterns (the turnout rate in previous elections at the same polling station), population density (the number of residents over 18 years of age), access to public transportation, distance from the polling station to residential areas, weather conditions on polling day, local holidays, concurrent events such as examinations or celebrations, and even indicators extracted from social networks (the volume of election-related discussions, hashtag usage rates, and positive or negative public sentiment). The model produces a heat map of predicted voter density at different time intervals (morning, noon, and evening) for each polling station (Akbari et al., 2024; Binns, 2024). This forecast can be updated weeks before the election based on static data and on election day based on real-time queue data.
2. **Dynamic allocation of human resources and equipment:** Based on the output of the previous step, the intelligent system provides recommendations concerning the following: (a) the number of ballot boxes needed per polling station, rather than assigning one fixed ballot box to all polling stations, since some polling stations may require two or three ballot boxes; (b) the number of additional ballot papers needed to prevent shortages during the final hours; (c) the

number of executive officers responsible for authentication, ballot-paper delivery, and monitoring, as well as Guardian Council observers at each polling station; and (d) logistical distribution, including mobile ballot boxes for difficult-to-access areas. For this optimization, combinatorial optimization algorithms, such as genetic algorithms or simulated annealing, can be used to determine the best overall allocation while accounting for budget, time, and available resources (Kettunen & Kallio, 2025). Additionally, on election day, the system can provide dynamic recommendations for shifting staff or ballot papers from low-density to high-density polling stations by receiving real-time data from polling stations, including queue length, voting speed, and remaining ballot-paper stocks, through officers' mobile applications.

3. **Crisis and contingency management:** The intelligent system can simulate various crisis scenarios: (a) the sudden failure of a polling station due to a power outage or cyberattack; (b) a sudden crowd gathering that exceeds the polling station's capacity; and (c) the outbreak of a local conflict or protest. For each scenario, the system recommends "rapid response plans," such as transferring voters to an alternative polling station, activating a pre-equipped mobile polling station, or dispatching reinforcements. This capability increases the resilience of the entire electoral system (Gonzalez & Patterson, 2024).
4. **Analysis of the causes of reduced participation in specific areas:** If, after the election, it is determined that participation in a region was unusually low—for example, 20% below the national average—the AI model can prioritize possible explanatory factors by analyzing various variables, including socioeconomic status, distance from polling stations, the presence of rumors of fraud in that area, social media patterns, and local adverse events. This information can greatly assist election authorities in adopting corrective measures in subsequent periods, such as increasing the number of polling stations, changing polling station locations, and conducting targeted information campaigns (Akbari et al., 2024).

3.1. Opportunities, Benefits, and Potential Achievements

First: **Increasing efficiency and reducing costs.** Optimizing resource allocation can yield substantial direct savings through fewer unused ballot boxes and ballot papers, reduced staff overtime, and lower transportation costs, as well as indirect savings through increased participation, which can contribute to greater legitimacy and lower political and social costs. In Iran, where the election budget is financed from the Treasury, these savings are significant (Tavakoli-Rad & Sadat Miri, 2021).

Second: **Improving the voter experience and increasing turnout.** Voters are less likely to face long and chaotic lines. Comparative studies have shown that reducing waiting times from two hours to 20 minutes can increase turnout rates by 5% (Susskind, 2024). In Iran, where turnout rates are a concern for the government in some elections, this effect is significant.

Third: **Reducing psychological strain on executive agents.** Polling station officials, who are often selected from among civil servants or local trustees, are under severe time and logistical pressure on election day. A predictive and allocative system can automate many difficult decisions, such as identifying which polling stations require additional ballot papers, and allow officials to focus on their core tasks, including authentication, monitoring the integrity of voting, and counting. This can improve the quality of work and reduce fatigue-related errors (Kettunen & Kallio, 2025).

Fourth: **Pre-election simulation and rehearsal capabilities.** The intelligent model can conduct "election maneuvers" weeks before election day. By introducing different scenarios—for example, 40% or 70% turnout in a province—it can identify and correct logistical weaknesses before an actual crisis occurs. This preventive aspect is highly valuable (Gonzalez & Patterson, 2024).

Fifth: **Identifying system anomalies.** If the system predicts high turnout at one polling station but turnout is very low on election day, this discrepancy can signal a violation, such as voters being redirected to another polling station, or a practical problem, such as a blocked access road. In this way, the system not only improves allocation but also functions as an indirect monitoring tool.

3.2. Legal-Technical Challenges, Risks, and Hazards

First: **Dependence on data quality and completeness.** Prediction accuracy depends entirely on the quality, comprehensiveness, and currency of the input data. If historical data from past elections in Iran are incomplete or unreliable because of registration defects, such as inaccurate statistics on voter turnout at each polling station in previous years, or changes in electoral district boundaries between election rounds, the predictions will also be substantially inaccurate. Turnout predictions are also affected by factors such as last-minute political events—for example, the withdrawal of a popular candidate, the spread of a rumor of fraud, or a sudden national event—that are not present in historical data and cannot be predicted by the algorithm (O'Neil, 2016). Therefore, intelligent models must present an "uncertainty range," and humans must remain responsible for final decisions, such as authorizing the distribution of additional ballot papers.

Second: **The risk of political misuse of predictions.** If forecasts of turnout in different regions are made public or made available only to certain groups, such as political parties, candidates, or specific media outlets, before the election or even during the first hours of voting in real time, they can influence voter behavior. For example, publishing the claim that "turnout in Region A is very low" may encourage supporters of a particular candidate to vote in order to compensate or discourage opponents from voting. This "soft manipulation" or "predictive surveillance" contradicts the principles of impartiality and freedom of choice (Hernandez, 2024). In the Islamic Consultative Assembly Election Law, as amended in 1402, Article 83, Clause 19, "announcing the results before observing the legal formalities" is considered a crime; however, model-based forecasts do not fall under the category of "actual statistics" and are therefore not subject to this prohibition. This constitutes a serious legal loophole.

Third: **The complexity of liability in the event of a gross error.** If the intelligent system makes a serious mistake in its prediction—for example, if it predicts that polling station X will experience low congestion and, as a result, an insufficient number of ballot papers is sent there, but on election day congestion becomes extremely high and many voters remain unable to vote because ballot papers are unavailable—which institution is responsible? Is it the Ministry of Interior as the implementing authority, the company that designed the system, or the supervisory authority, namely the Guardian Council, which should have monitored the accuracy of the allocations? Traditional rules of civil liability, based on the Civil Code and the Civil Liability Law, are insufficient to answer these questions because proving "fault" or "defect" in complex learning systems is extremely difficult (Zakirinia, 2023). Contracts with technology companies should clarify what constitutes an "acceptable error," such as a maximum prediction error of 5%, and how damages resulting from an error will be compensated, such as through compensation to voters who were unable to vote or by holding a re-election at the affected polling station.

Fourth: **Privacy in real-time data collection.** If the system needs to receive instantaneous data from a polling station for dynamic allocation—for example, a national identification number associated with a voter standing in line or the precise time at which a vote is cast—such data contain sensitive location and identity information. The storage and processing of this data must be conducted in full compliance with data protection principles, including data minimization, anonymization, setting a short retention period such as 24 hours, and encryption during transmission and storage; otherwise, privacy violations may occur on a massive scale (Fatemi, 2024; Habibi & Homayoun, 2016). Particularly in Iran, where concerns about general government surveillance exist, any real-time data collection may be met with severe distrust.

Fifth: **The risk of algorithmic bias in resource allocation.** If the intelligent model systematically predicts that certain areas should receive fewer resources for statistical reasons—for example, because historical data from deprived or minority areas are incomplete—it can lead to unintended algorithmic discrimination against those areas. For example, if historical data show that turnout in a particular rural area has always been low because of remoteness, the model may predict low turnout in the next election and send an insufficient number of ballot papers. However, if turnout increases sharply because of a popular local candidate, that area may face a severe shortage, and voters there may effectively be deprived of their rights. This contradicts the principle of equal access to electoral facilities under Articles 19 and 20 of the Constitution (Rajaei & Amiri, 2025). Therefore, before implementation, the model should be audited for "distributive justice" and, if bias is identified, corrected by reweighting disadvantaged areas.

3.3. Legal and Institutional Requirements and Recommendations for Iran

The Iranian legal system currently neither explicitly permits nor explicitly prohibits the use of artificial intelligence to predict turnout and allocate resources. Articles 3 and 9 of the Presidential Election Law require the Ministry of Interior to "take the necessary measures to conduct the elections as well as possible." However, these measures do not expressly include predictive algorithms. To address this gap, the following suggestions are made:

1. **Amendment of the Election Executive Regulations:** An article should be added authorizing—and, where resources are available, requiring—the Ministry of Interior to use artificial intelligence-based forecasting and allocation systems, subject to compliance with standards of transparency, justice, and privacy (Mohebbi & Amiri, 2025).
2. **Establishment of a "Technical Committee" under the National Election Headquarters:** This committee should be formed with representatives of the Ministry of Interior, the Planning and Budget Organization, the Statistical Center of Iran, the Guardian Council, and academia, including experts in data mining and law. It should assume the following duties: determining permitted indicators and variables for prediction in order to prevent the inclusion of discriminatory variables, verifying the suitability of algorithmic models and input data, monitoring the allocation process, and addressing violations (Hosseinabadi & Zarefard, 2022).
3. **Transparency requirement:** The system should be designed so that observers and candidates can understand the "logic of the prediction" without disclosing personal data. A summary report on the accuracy of the predictions should also be published after the election.
4. **Training for executive agents:** Polling station officers should be trained to understand that the system's output constitutes a "recommendation" rather than a "final ruling." If they observe a discrepancy between the system's prediction and field conditions—for example, voter density substantially higher than predicted—they should request a review through rapid communication channels.
5. **Maintaining strategic reserves:** Even with the best forecasts, strategic reserves of ballot papers and human resources should always be maintained at the provincial level to enable rapid responses in the event of a forecasting error.

Overall, using AI to predict turnout and allocate resources has considerable potential to improve electoral efficiency and fairness in Iran, but it requires responsible design, full transparency, and strong oversight. Without these guarantees, this application could also become a tool for hidden discrimination and inefficiency.

Monitoring and Analyzing Results and Detecting Anomalies in Vote Statistics and Counting Processes to Provide Early Warning to Observers: One of the most sensitive moments of any election is the vote-counting and tabulation phase. During this phase, tens of thousands of polling stations across the country generate a huge volume of numerical data, including votes for each candidate at each polling station, invalid votes, the number of voters present, and other related information, and transmit it to provincial and national aggregation centers. The traditional method of manually reviewing this data by observers, including representatives of the Guardian Council, candidate representatives, and civil observers, is very slow, costly, and practically incomplete on a national scale. Human observers cannot simultaneously review thousands of numerical tables with statistical accuracy and detect subtle patterns of manipulation within the massive volume of ordinary data (Khosravi, 2009). Using big-data analysis and anomaly-detection techniques, artificial intelligence can identify suspicious patterns in real or near-real time and send rapid, targeted alerts to human observers so that they can focus on critical areas and avoid ineffective dispersion of supervisory resources. This section outlines the main applications, opportunities, challenges, and legal requirements in this area.

4. Main Applications of Artificial Intelligence in Monitoring and Detecting Electoral Anomalies

1. **Detecting statistical anomalies using Benford's Law and similar methods:** Benford's Law is a statistical rule according to which, in many naturally occurring datasets, the first digit of numbers follows a particular logarithmic distribution: the digit 1 appears approximately 30% of the time, 2 approximately 17.6%, 3 approximately 12.5%, and so on. Systematic and significant deviations from this distribution—for example, an excessive frequency of the digits 5 or 7 in the first position—can signal intentional manipulation or systematic fraud. Artificial intelligence algorithms can rapidly examine data from all polling stations, or entire counties, for conformity with Benford's Law and report

polling stations with unusual patterns to observers (Susskind, 2024). Although Benford's Law is not a definitive diagnostic tool, because not all datasets conform to it and some legitimate datasets may exhibit natural deviations, it can serve as a valuable early-warning mechanism when combined with other indicators, such as second- and third-digit analysis or the distribution of final digits in vote counts.

2. **Cluster analysis and outlier detection:** In this method, the intelligent model divides all polling stations into homogeneous clusters based on contextual variables, such as precinct population, ethnic and religious composition, socioeconomic status, literacy rate, historical participation patterns, and distance from the provincial center. It then defines a "normal" range of results for each cluster. For example, in a cluster of rural areas in Province X with populations between 1,000 and 2,000, Candidate A may typically receive between 40% and 55% of the vote, while the invalid-vote rate ranges between 2% and 4%. Any polling station whose results fall substantially outside this range—for example, where Candidate A receives 95% of the vote or the invalid-vote rate reaches 15%—is marked as "abnormal," and its file is sent to observers for priority manual review (Gonzalez & Patterson, 2024). This method has been used successfully in the presidential elections of Ukraine (2004), Kenya (2013), and some U.S. states to detect irregularities that subsequently led to recounts or the invalidation of votes in some polling stations.
3. **Monitoring the temporal trend of results:** The system can monitor result trends across polling stations over time and identify suspicious patterns. For example, if a group of polling stations, such as all polling stations in a county, submits its results with a significant delay relative to the regional average and then suddenly and simultaneously transmits them at a particular time, this may signal coordination outside normal procedures for the purpose of manipulation. If, at a particular polling station, a candidate's votes increase unusually during the final minutes of counting after preliminary results have been announced—for example, if 200 votes are suddenly added in favor of one candidate—the algorithm can issue an alert. Similarly, if counting speed at a polling station is unusually high or low relative to the average, this may indicate human error, such as excessively rapid counting associated with a higher probability of mistakes, or possible fraud (Kettunen & Kallio, 2025).
4. **Automatic matching with reference data:** The most advanced level of monitoring involves automatically matching data reported by the central system with primary data. For example, if candidate representatives or Guardian Council observers at polling stations capture images of handwritten minutes using a mobile application and transmit them to a secure system, an intelligent algorithm can extract the numbers from the images using optical character recognition (OCR), compare them with the figures reported by the polling station to the central system or entered by the aggregation-center operator, and immediately report any discrepancy, even a difference of a single vote, to observers (Hosseinabadi & Zarefard, 2022). In Iran, where minutes are paper-based and signed, this method can add an independent layer of security against errors or fraud at the data-entry stage.
5. **Detecting complex fraud patterns:** Some forms of fraud are carried out in a coordinated manner across multiple polling stations or multiple stages, such as the transfer of unused ballot papers between neighboring precincts or the transfer of votes from one candidate to another across several adjacent precincts. Network anomaly-detection algorithms can identify these coordinated patterns by analyzing hidden correlations among polling stations, including spatial connections, temporal relationships, or unusual similarities in results. For example, if two adjacent precincts that are demographically very similar produce opposite results—one showing 80% support for Candidate A and the other 80% for Candidate B—while their total vote counts exhibit an unusual relationship with a third precinct in the same area, this could indicate an "exchange of votes" (Binns, 2024).

4.1. Opportunities, Benefits, and Potential Achievements

First: **Increasing the speed and accuracy of supervision by combining artificial intelligence with centralized human supervision.** Human supervisors, including representatives of the Guardian Council, candidate representatives, and civil observers, cannot review tables from tens of thousands of polling stations with statistical accuracy within a limited period. Artificial intelligence can perform this task within minutes and flag only suspicious cases, usually a small proportion of polling stations, for in-depth human review. The combination of "AI as an initial filter + human supervision focused on high-risk cases"

can be far more effective than purely dispersed human supervision. This method can significantly increase supervisory efficiency (López-López et al., 2023; Martos, 2023).

Second: **Reducing baseless allegations of fraud.** One serious problem in Iranian elections, particularly the 2009 presidential election and some parliamentary elections, has been widespread and allegedly unfounded accusations of fraud, mainly by losing candidates or opposition political movements, which can undermine public trust and lead to instability. If a credible, independent, and transparent intelligent system, approved by all parties or at least by independent observers, analyzes the results and provides a documented report indicating that "no systematic anomalies were found" or that "only 0.1% of polling stations exhibited minor and justifiable anomalies," it can help neutralize such allegations by functioning as an impartial analytical mechanism. Conversely, if anomalies are discovered, the system can provide precise, documented evidence, including the polling station number, type of anomaly, severity of deviation, and comparison with similar polling stations, so that a targeted and rapid judicial investigation can be conducted (Susskind, 2024).

Third: **Post-audit capability to increase confidence or correct errors.** Even after the election has concluded and the results have been announced, observers, researchers, and losing candidates can use the system to re-examine the results. If the system is transparent—that is, if its algorithm and criteria are public and understandable and the input data are made available to independent auditors in a manner that preserves privacy—this review can increase public confidence in the results and provide a basis for corrective action, such as a recount or annulment, in the event of systematic errors resulting, for example, from a technical defect in a province's counting system (Brunner, 2026; Wieringa, 2020).

Fourth: **Reducing pressure on the Guardian Council and oversight bodies through intelligent prioritization of complaints.** In the Iranian electoral system, the Guardian Council, as an oversight body, receives a large volume of complaints from candidates and citizens after each election, many of which may lack sufficient evidence or be based primarily on subjective perceptions. An intelligent system can match complaints with statistical data and detected anomalies, assign higher priority to complaints supported by genuine anomalies confirmed by the system, and place complaints that lack statistical evidence and appear primarily political at a lower priority without rejecting them outright. This allows the Council to focus its limited resources on the most serious cases and accelerate the review process (Hosseinabadi & Zarefard, 2022).

4.2. Legal-Technical Challenges, Risks, and Hazards

First: **Detection errors.** The most important technical-legal challenge involves Type I errors (false alarms, in which an anomaly is declared when the result is actually normal) and Type II errors (failure to detect a genuine anomaly). Type I errors can cause unnecessary tension and distrust. Imagine that the system marks a normal polling station as "extremely suspicious," and opposition media subsequently report that "the government's monitoring system itself admits to fraud at polling station X." Even if the alert is later shown to have been erroneous, public trust may already have been damaged. Type II errors can be even more serious: if the system fails to detect organized fraud and votes favoring a candidate are confirmed without adequate monitoring, the legitimacy of the entire election may be called into question. No algorithm is entirely error-free. Therefore, the system should be designed with adjustable warning thresholds appropriate to the political sensitivity of the context, and each warning should be treated as an "invitation to human review" rather than a "conclusive determination of fraud." Observers should also be trained to investigate alerts without prejudgment (Carvalho & Rosa, 2024).

Second: **Algorithmic transparency and the risk of a "black box."** If the anomaly-detection algorithm is proprietary and confidential—for example, if it is designed by a private foreign or domestic company and its source code is not available for independent scrutiny—candidates and observers may have difficulty trusting it. Concerns may arise that the algorithm has been deliberately configured to ignore anomalies favoring the government or a particular political group while highlighting anomalies affecting opposing groups. Therefore, requiring meaningful algorithmic transparency, including publication or disclosure of architectural documentation, detection criteria, variable weighting, and, where necessary, source code for auditing by independent experts accepted by the parties, constitutes an important legal and political requirement (Brunner, 2026; Wieringa, 2020). In Iran, given the Guardian Council's sensitive role, one possible approach is for a domestic consortium of academic and governmental experts to design the system under the Council's supervision. The source code could be maintained

in a "closed-source but auditable" format accessible to a selected Council team and candidate representatives as an intermediate solution.

Third: **Algorithm or data manipulation by malicious actors.** A powerful internal or external actor may target not the voting data itself but the anomaly-detection algorithm. For example, a data-injection attack could cause "alarm fatigue" by generating a large volume of false alerts or minor alterations to genuine data, thereby burying genuine alerts among irrelevant ones. Alternatively, if attackers gain access to the source code or system outputs, they may identify blind spots in the algorithm and design fraudulent activity in a manner intended to evade detection—for example, by adding votes in a pattern that does not violate Benford's distribution (O'Neil, 2016). Countering these threats requires robust system design, frequent algorithmic updates, and appropriate security measures.

Fourth: **Conflict with the principle of ballot secrecy during counting.** Some advanced real-time monitoring methods may require access to individual voter data—for example, to identify patterns among voters at a polling station based on age, gender, or ethnicity. This would directly conflict with the principle of ballot secrecy, which is expressly recognized in Iran's Presidential Election Law and analogous provisions of other electoral laws. Each individual's vote must remain secret, and no person, including an observer, should be able to link a specific individual's vote to their identity. Therefore, any anomaly analysis should be performed at the aggregate level, such as the total number of votes for each candidate at a polling station, and no connection should be established between an individual's identity and their vote. The system should also neither store nor process individual-level information capable of revealing how a particular person voted (Khosravi, 2009).

Fifth: **Infrastructure and cybersecurity requirements.** The monitoring and early-warning system must connect to data from tens of thousands of polling stations across the country in real time. This permanent and widespread connectivity considerably increases vulnerability. A system outage in the middle of an election, even for a few hours, can be highly disruptive because it may generate rumors and distrust. Therefore, secure and resilient infrastructure—including a physical or virtual private network with end-to-end encryption, server redundancy across separate data centers, emergency power supplies, and a 24-hour cyber rapid-response team—is a fundamental prerequisite (Hassanbeigi, 2005). In Iran, given the experience of major cyberattacks on governmental infrastructure, including the Stuxnet attack on nuclear facilities and the 2021 attack on the fuel distribution system, this concern is particularly serious and must be considered in system design.

5. Legal and Institutional Requirements and Recommendations for Iran

The Iranian legal system is, in some respects, compatible with the Guardian Council's supervisory powers under Article 99 of the Constitution and ordinary laws. However, it contains legal gaps concerning the use of artificial intelligence to monitor results and detect anomalies. Currently, the Guardian Council can use tools it considers useful for supervision under the principle of supervisory independence. However, to avoid disputes and ensure transparency, it is necessary to adopt a specific regulation or directive specifying the following details:

1. **The institution responsible for designing and deploying the system:** The Guardian Council, as the supervisory institution, is most likely the primary custodian. However, it may delegate technical implementation to the Ministry of Interior or an academic consortium, subject to its direct supervision.
2. **The alert threshold and how it is determined:** It should be specified who has the authority to adjust the sensitivity of the algorithm. For example, it must be determined whether a "joint technical committee" consisting of representatives of the Council, the Ministry of Interior, and candidates sets the threshold or whether the Council alone has this authority. The threshold should be announced transparently before the election.
3. **Legal validity of system alerts:** It should be clarified whether a system alert constitutes "definitive evidence" of fraud or is merely "indicative" or preliminary evidence that must be confirmed through independent human review. The preferable approach is the latter: an alert should initiate an investigation rather than constitute a final determination.
4. **Ensuring algorithmic transparency and the possibility of independent auditing:** It should be clear how candidate representatives and civil observers can assess the reliability of the system's results. One recommendation is to select an "independent audit team" consisting of five experts approved by the relevant parties or the judiciary, who would have access to the source code and data and prepare a confidential report on the correctness of the system's performance. A summary of this report could subsequently be published without disclosing the source code.

5. **Decision-making in the event of disagreement between the system output and supervisors' manual review:** If the system warns that "polling station X is abnormal" but human inspectors conclude after a field inspection that "everything is normal," it should be determined who makes the final decision. One proposal is referral to a three-member panel consisting of a judge, a Guardian Council representative, and an independent expert, whose decision would be final.
6. **Pilot and gradual implementation:** Given the high sensitivity of this area, it is strongly recommended that the system first be implemented on a pilot basis in one or two medium-sized electoral districts, for example, one urban and one rural district, under strict supervision. Following comprehensive evaluation and correction of deficiencies, it could be expanded to a larger scale, such as an entire province, in the next general election and subsequently to the entire country (Takhtaei, 2011).

Overall, intelligent monitoring of results and anomaly detection through artificial intelligence constitute powerful tools for strengthening electoral integrity and restoring public trust. However, implementation without full transparency and independent oversight is not only ineffective but may itself become a new source of distrust and disagreement. The balance between the "power of algorithmic detection" and "preservation of privacy and ballot secrecy" must also be carefully maintained. In the Iranian legal system, given the contentious experience of past allegations of electoral fraud, investing in such a system and coupling it with transparency guarantees could constitute a significant step toward achieving "healthy and trustworthy elections."

6. Conclusion

The study showed that AI, by entering electoral processes, can significantly increase the accuracy, speed, transparency, and efficiency of election management and can play an effective role at all stages, from registration and authentication to electoral monitoring. However, this technology also brings significant legal challenges, including privacy violations, algorithmic bias, reduced transparency, ambiguity in accountability, and threats to fundamental rights and freedoms. Accordingly, AI in electoral processes can achieve desirable governance goals when used 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. As a result, the success of this technology in the electoral system depends more on an appropriate legal framework for regulating, monitoring, and ensuring its responsible use than on technical advances alone.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

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

References

Aalipour, H. (2016). *Information Technology Criminal Law*. Khorsandi Publications.

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

Binns, R. (2024). AI in Public Administration: Combating Corruption through Data Analytics. *Journal of Technology and Law*, *18*(3), 77-94.

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.
Crawford, K. (2024). AI and Administrative Law in the United States: Risks and Legal Gaps. *Yale Law Journal*, *133*(4), 210.
European Commission. (2024). *Artificial Intelligence and the Law: Regulatory Challenges in Europe*.
European Commission. (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.
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.
Haddadpour. (2022). Privacy of Individuals in Imami Jurisprudence and Subject-Matter Laws. *Opinions*, *25*(5), 43-56.
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.
Hosseinabadi, S., & Zarefard, M. (2022). Application of Artificial Intelligence in Electronic Surveillance and Increasing Transparency of Affairs.
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. (2007). 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, N. (2009). *Legal Aspects of Electronic Voting* Shahid Beheshti University, Faculty of Law].
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
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
Michael, A. (2023). *Artificial Intelligence, Democracy and Elections*.
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.484
O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group.
Rajaei, M., & Amiri, A. (2025). Public Law Challenges in Protecting Human Digital Rights in the Age of Artificial Intelligence. *Legal Studies in Digital Age*, *6*(5), 1-12. https://doi.org/10.61838/kman.lsda.484
Smith, J. (2024). Shared Responsibility in AI-Driven Government Systems. *International Journal of Law and Technology*, *11*(4), 89.
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.
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 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