Legal Challenges of Employing Artificial Intelligence and Data Processing in Situational Prevention of Cybercrimes under Iranian Positive Law

1. Hossein Tajik: Ph.D. candidate in Criminal Law and Criminology, Se.C., Islamic Azad University, Semnan, Iran
2. Mohammad Rouhani Moghaddam*: Department of Law, Se.C., Islamic Azad University, Semnan, Iran
3. Maryam Aghaei Bojestani: Department of Law, Se.C., Islamic Azad University, Semnan, Iran

*Correspondence: 5239772649@iau.ir

Abstract

The rapid growth of emerging technologies, particularly artificial intelligence and big data processing, has fundamentally transformed policies for the prevention of cybercrimes. Within the situational crime prevention approach, the objective is to reduce opportunities for the commission of crime through the deployment of technological tools; however, the use of intelligent systems in identifying criminal patterns, analyzing behavioral data, and predicting the occurrence of crime has generated complex legal and ethical concerns. Under Iranian positive law, although the Computer Crimes Act and higher-level regulatory instruments related to cyberspace refer in general terms to data security and privacy requirements, a comprehensive regulatory framework governing automated and algorithmic decision-making in preventive processes has not yet been developed. The present study adopts a descriptive–analytical approach and employs a library-based research method to examine the legal challenges arising from the application of artificial intelligence and big data in the situational prevention of cybercrimes. The findings indicate that the most significant challenges include the absence of explicit regulations concerning civil and criminal liability arising from algorithmic decisions, threats to privacy and data protection rights, lack of transparency and explainability in automated decision-making, and the risk of algorithmic bias or discrimination. Moreover, the tension between the efficiency of data-driven predictive mechanisms and the requirements of fundamental rights of citizens—such as the presumption of innocence and the rule of law—constitutes a central challenge. Accordingly, it is recommended that the Iranian legislator, drawing inspiration from international models such as the European Union Artificial Intelligence Act and the OECD Principles on Artificial Intelligence, enact specific regulations concerning data governance, algorithmic transparency, technical–legal auditing of artificial intelligence systems, and the establishment of an independent supervisory authority. The realization of such a regulatory framework can enhance the effectiveness of the cybercrime prevention system while safeguarding citizens' rights in the age of artificial intelligence.

Keywords: Artificial Intelligence; Big Data Processing; Situational Prevention of Cybercrimes; Legal Challenges

Received: 06 November 2025
Revised: 07 February 2026
Accepted: 14 February 2026
Initial Publication 15 February 2026
Final Publication 01 August 2026

Citation: Tajik, H., Rouhani Moghaddam, M., & Aghaei Bojestani, M. (2026). Legal Challenges of Employing Artificial Intelligence and Data Processing in Situational Prevention of Cybercrimes under Iranian Positive Law. *Legal Studies in Digital Age,* 5(4), 1-12.

1. Introduction

The rapid technological transformations of recent decades, particularly in the fields of artificial intelligence and big data processing, have not only reshaped traditional patterns of social and economic life but have also profoundly affected the structures of criminal justice systems and national criminal policies. The growing expansion of cybercrimes—including unauthorized access, online fraud, malware distribution, and phishing attacks—has made the reconsideration of preventive strategies increasingly imperative (Brenner, 2010; Wall, 2011). In this context, the utilization of emerging technologies grounded in artificial intelligence and big data analytics for identifying criminal behavioral patterns and predicting crime occurrence has attracted significant attention within advanced legal systems as an effective instrument of situational crime prevention (Clarke, 1997; Cornish & Clarke, 2003; Perry et al., 2013). Within situational prevention of cybercrimes, the principal objective is not the rehabilitation of offenders or the enhancement of social norms, but rather the reduction of crime opportunities through technological measures such as intelligent network monitoring, intrusion detection systems, algorithmic analysis of user behavior, and threat forecasting (Azizi, 2021; Felson & Clarke, 1998). However, this technological approach gives rise to fundamental legal questions: Can automated artificial intelligence decisions identifying suspicious individuals serve as a lawful basis for legal action? What are the boundaries of civil and criminal liability in cases of algorithmic error? Is the large-scale collection and analysis of user data compatible with the fundamental right to privacy? These concerns demonstrate that the application of artificial intelligence in cybercrime prevention is not merely a technical matter, but one that directly intersects with core principles of public and criminal law (Cath, 2018; Nemati, 2023).

On the other hand, the Iranian legal system has generally adopted a reactive approach in confronting technological developments. The Computer Crimes Act of 2009 and its supplementary regulations were, at the time of enactment, aligned with the initial conditions of cyberspace; however, with the emergence of new technologies such as machine learning, predictive analytics, and automated decision-support systems, significant regulatory gaps have become evident (Mousavi, 2022; Rahimi, 2020). Legal definitions of data, processing, and privacy remain ambiguous and incomplete, and no explicit provisions address algorithmic transparency, human oversight, or the legal liability of artificial intelligence developers and operators (Hosseini, 2021; Kazemi, 2022; Razavi, 2023). These deficiencies have resulted in the practical deployment of predictive technologies in cybersecurity without a clear statutory framework, thereby increasing the risk of infringement upon users' fundamental rights (Kazemi, 2023; Zamani, 2022).

The necessity of the present research stems precisely from this regulatory vacuum. On one hand, law enforcement and security institutions require intelligent tools and big data analytics to effectively combat cybercrime (Amiri, 2023; Ghadiri, 2021). On the other hand, the absence of clear rules governing the collection, processing, and utilization of personal data may lead to violations of citizens' rights and erosion of public trust (Ghasemi, 2023; Sharifi, 2022). Accordingly, this study seeks to identify and analyze the existing legal challenges and to propose solutions for establishing a coherent and balanced legal framework that reconciles technological efficiency with the protection of individual liberties.

The principal research question is as follows: What are the most significant legal challenges associated with the application of artificial intelligence and big data processing in the situational prevention of cybercrimes under Iranian positive law, and what reforms are necessary to address them? The research hypothesis posits that the current Iranian legal framework lacks sufficient regulations to govern automated decision-making based on artificial intelligence in the field of cybercrime prevention. The primary objective of this study is to elucidate and analyze the legal and ethical dimensions of utilizing artificial intelligence and big data in situational cybercrime prevention in Iran and to offer legislative and policy-oriented reform proposals. The significance of the subject may be considered from two perspectives: first, the theoretical dimension, which contributes to the development of technology law scholarship and the redefinition of classical criminal law concepts in light of automated decision-making (Safayi, 2020; Taheri, 2023); and second, the practical dimension, which may provide a foundation for drafting executive regulations and operational guidelines for the lawful and secure use of artificial intelligence technologies within judicial and law enforcement institutions.

From a substantive standpoint, the research focuses on the legal and regulatory aspects of employing artificial intelligence in cybercrime prevention processes and does not address the technical architecture of algorithms or classical criminological

analysis. From a territorial perspective, the study concentrates on the positive law of the Islamic Republic of Iran, with limited comparative reference to international instruments such as the Convention on Cybercrime (2001) (Council of Europe, 2001) and the European Union Artificial Intelligence Act (European Union, 2024; Smith, 2024). From a temporal perspective, the analysis is confined to the current status of national laws and policies up to 2025. The research methodology is descriptive–analytical, and data have been collected through library-based sources, scholarly articles, legal documents, and domestic and international regulations. In the analytical phase, a comparative–critical method is employed to evaluate the adequacy of Iranian legislation in relation to global standards, including international risk-management frameworks (Nemati, 2024; Nist, 2023; Oecd, 2019). This approach enables the identification of strengths and weaknesses within the domestic legal system and the formulation of practical reform proposals.

2. Definition of Artificial Intelligence (AI)

Artificial intelligence refers to systems capable of exhibiting responses analogous to intelligent human behavior, including the comprehension of complex situations, simulation of cognitive processes and reasoning patterns, successful adaptation, learning, and the acquisition of knowledge for problem-solving. In essence, artificial intelligence denotes the form of intelligence manifested by machines, as opposed to natural intelligence displayed by animals and humans. The term "intelligence" itself implies the capacity for reasoning, and whether artificial intelligence can genuinely attain reasoning ability remains a subject of scholarly debate. Leading AI textbooks define this field as the study of intelligent agents: systems that perceive their environment and take actions that maximize their chances of achieving designated goals (Russell & Norvig, 2021). Some sources describe artificial intelligence as machines that imitate cognitive functions such as learning and problem-solving; however, this anthropomorphic definition has been critically reconsidered within mainstream AI scholarship (Russell & Norvig, 2021).

Artificial intelligence constitutes one of the most significant scientific and technological achievements of the twenty-first century, influencing not only technical and industrial sectors but also legal and criminal justice systems (Cath, 2018). Unlike traditional computer programs that operate according to predetermined instructions, AI systems are capable of analyzing data, identifying patterns, adapting to new conditions, and improving their outputs autonomously (Russell & Norvig, 2021). This adaptive capacity distinguishes artificial intelligence from conventional technologies and renders it a strategic instrument in security, legal, and criminal domains.

From the perspective of criminal law, defining and identifying the functions of artificial intelligence is of heightened importance, as this technology can play a role both in the commission of crimes and in their prevention and detection (Brenner, 2010). Cybercriminals may employ AI algorithms to identify vulnerabilities in computer systems, while judicial and law enforcement authorities may use the same tools to analyze criminal behavior, forecast criminal activity, and identify perpetrators (Wall, 2011). Therefore, the definition of artificial intelligence in criminal law cannot be limited to its technical attributes but must also encompass its legal and criminological implications.

The functions of artificial intelligence may be categorized into three principal domains. First is the analytical function, encompassing the capacity to process and analyze vast quantities of data within a short timeframe. This capability enables legal and law enforcement institutions to identify criminal behavioral patterns within large datasets and to issue preventive alerts (Marr, 2018; Mohammadi, 2020). Second is the predictive function, particularly significant in situational prevention. Machine learning algorithms can analyze historical data to identify locations, times, or conditions with a heightened probability of crime occurrence, thereby facilitating targeted allocation of law enforcement resources (Maleki, 2022; Perry et al., 2013). Third is the decision-support function, whereby AI systems assist judges, prosecutors, and police officers in making informed decisions. In certain jurisdictions, AI-based systems are employed to assess recidivism risk to inform bail or parole decisions (Dressel & Farid, 2018).

Artificial intelligence tools applied within criminal justice encompass a wide spectrum. Machine learning enables algorithms to be trained on historical data and to improve performance when confronted with new datasets (Russell & Norvig, 2021). In

criminal contexts, machine learning is utilized to analyze patterns of online fraud, predict cyber intrusions, and detect suspicious behavior (Amiri, 2023; Ghadiri, 2021). Another significant tool is natural language processing, which allows computers to interpret and analyze human language. In criminal investigations, such systems may be employed to analyze messages, emails, or online communications linked to criminal activity (Russell & Norvig, 2021).

Moreover, artificial neural networks and deep learning techniques play a crucial role in identifying complex crime patterns. The detection of unlawful images or violent content on the internet has been facilitated through deep learning algorithms (Russell & Norvig, 2021). Computer vision technologies may also be used for identifying suspects through surveillance footage or facial recognition systems. The application of such technologies in metropolitan areas for identifying fugitives or suspicious individuals in public gatherings represents a clear example of their practical implementation (Goodman, 2015).

Finally, expert systems also occupy a specific position within the legal domain. These systems operate on predefined rule sets and input data to provide recommendations for resolving legal issues. Although their role within judicial systems remains limited, gradual development toward automated advisory systems or virtual legal assistants can be anticipated (Cath, 2018).

Artificial intelligence, in conjunction with the aforementioned tools, has enabled judicial and law enforcement institutions—through big data analytics—to monitor macro-level crime trends. Big data refers to vast volumes of structured and unstructured information whose analysis is not feasible through traditional methods. By examining such datasets, artificial intelligence can uncover hidden crime patterns and assist in the formulation of effective criminal policies (Marr, 2018; Mohammadi, 2020).

Accordingly, the definition of artificial intelligence cannot be confined merely to software technologies; rather, it is directly connected to functions and instruments capable of transforming the criminal justice system. From this perspective, artificial intelligence is not merely a technological development but a strategic instrument for reshaping criminal policy and crime prevention (Safayi, 2020).

Applications of artificial intelligence include advanced web search engines (such as Google and Bing), recommender systems (used by platforms such as YouTube and Amazon), human language understanding systems (such as voice assistants), autonomous vehicles, generative artificial intelligence systems capable of producing textual or artistic content, automated decision-making systems, and high-level strategic game systems. As machines become increasingly capable, tasks once considered to require "intelligence" are often removed from the definition of AI—a phenomenon known as the "AI effect." For example, optical character recognition is no longer regarded as artificial intelligence because it has become a routine and everyday technology. The use of artificial intelligence in domains such as medicine and education continues to expand (Russell & Norvig, 2021).

Artificial intelligence became an academic discipline in 1956 and has since experienced several waves of optimism followed by periods of disappointment and reduced funding—often referred to as "AI winters"—before technological breakthroughs revitalized research and investment. Throughout its development, AI research has explored and abandoned various approaches, including brain simulation, modeling human problem-solving processes, formal logic, large knowledge databases, and imitation of animal behavior. In the first decades of the twenty-first century, machine learning—heavily grounded in mathematical statistics—became the dominant paradigm in the field, demonstrating remarkable success in addressing complex industrial and academic challenges (Russell & Norvig, 2021).

Different branches of artificial intelligence research have focused on specific objectives and employed specialized tools. Traditional AI research goals include reasoning, knowledge representation, planning, learning, natural language processing, perception, and object manipulation. General intelligence—the ability to solve arbitrary problems—remains a long-term aspiration of the field. To address such challenges, AI researchers have applied integrated problem-solving techniques, including mathematical search and optimization, formal logic, artificial neural networks, and statistical and probabilistic methods. Artificial intelligence is also closely related to disciplines such as computer science, psychology, linguistics, and philosophy. The field rests on the assumption that human intelligence can be described with sufficient precision to be simulated by a machine—an assumption that has generated philosophical debates regarding the nature of mind and the ethics of creating intelligent entities. Scientific literature and future-oriented studies further suggest that artificial intelligence, given its transformative potential, may pose significant risks if not properly governed (Cath, 2018; Russell & Norvig, 2021).

The conceptual foundations of artificial intelligence were anticipated by philosophers and mathematicians who developed formal logic systems. With the invention of electronic computers in the mid-twentieth century, scientists were confronted with the possibility that machines might simulate intelligent behavior. Despite skepticism among certain thinkers regarding its feasibility, within a few decades chess-playing machines and other intelligent systems emerged across various industries. The field of artificial intelligence formally originated at the Dartmouth workshop in 1956, where pioneering researchers initiated foundational research programs. In the following decade, substantial investment—particularly in the United States—fueled the establishment of numerous AI laboratories worldwide. Early AI researchers expressed strong optimism regarding the future capabilities of machines. The term "artificial intelligence" itself was introduced to designate this new field of study, encompassing intelligent computation and hybrid systems composed of artificial components. The classification of AI systems into "strong" and "weak" categories has been proposed as a means of distinguishing between systems that merely simulate intelligent behavior and those hypothesized to possess genuine cognitive capacities (Russell & Norvig, 2021).

3. Definition of Situational Prevention

Crime prevention, as one of the fundamental approaches in criminal policy, has consistently attracted the attention of legal systems and criminological scholarship. Within this framework, situational prevention occupies a distinct position because its focus is neither on the rehabilitation of the offender nor on punitive reaction after the commission of a crime, but rather on modifying external circumstances and environmental conditions in ways that reduce the likelihood of criminal occurrence. The central premise of situational prevention is that many crimes occur not solely because of criminal motivation, but due to the existence of suitable opportunities for their commission; therefore, if opportunities for crime are reduced or access to criminal targets becomes more difficult, the overall rate of crime can be significantly decreased. This concept first emerged in the 1970s in England and subsequently expanded to other jurisdictions, becoming established as an independent approach within criminology and criminal policy (Clarke, 1997).

Multiple definitions of situational prevention have been proposed. In criminological literature, situational prevention is defined as a set of measures aimed at reducing opportunities for crime and increasing the risk of detection and punishment for offenders through interventions in the immediate physical or social environment of crime (Felson & Clarke, 1998). The Council of Europe, in its policy documents, has likewise characterized situational prevention as specific actions that, through modifications of environmental conditions—such as strengthening physical and organizational controls—lead to a reduction in the probability of criminal conduct (Council of Europe, 2001). In Iran, although the criminological literature in this area remains relatively recent, several criminal law scholars have defined situational prevention as "any non-penal measure that, by restricting the conditions facilitating crime, deters the offender from realizing criminal intent" (Najafi Abrandabadi, 2011).

The fundamental principles of situational prevention rest upon several core foundations. The first principle is the reduction of criminal opportunities. This principle assumes that criminal motivations will always exist and cannot be entirely eliminated; however, environmental conditions may be altered in such a way that the feasibility of committing crime is diminished. For instance, installing surveillance cameras in commercial premises reduces theft by limiting easy and risk-free access to property. The second principle involves increasing the cost of committing crime. If offenders anticipate that committing a crime will require substantial time and effort or entail technical and security obstacles, they may be deterred. In cyberspace, data encryption and secure network protocols exemplify this principle (Clarke, 1997). The third principle concerns increasing the likelihood of detection and apprehension. The presence of monitoring and tracking tools enhances offenders' perception that crime carries a high risk of identification and sanction. The fourth principle involves reducing the benefits derived from crime. If offenders perceive that even successful commission will not yield substantial gains, their motivation declines; for example, the rapid freezing of bank accounts used in online fraud schemes can significantly diminish criminal profit (Cornish & Clarke, 2003).

Additional principles include target hardening and displacement control, meaning that access to potential crime targets is made more difficult or risk-laden. Moreover, the simplification of surveillance and control—through strengthening law enforcement presence, utilizing intelligent technologies, and enhancing community participation—constitutes a further dimension of situational prevention. Collectively, these principles demonstrate that situational prevention operates on the basis

of instrumental rationality and cost–benefit calculation, aiming to alter the offender's cognitive assessment such that crime appears irrational or unprofitable (Clarke, 1997).

An important characteristic of situational prevention is that, unlike certain forms of social prevention requiring deep cultural, economic, or educational transformation and yielding long-term outcomes, situational measures often produce relatively rapid effects. For example, installing antivirus software or firewalls within a governmental organization can immediately enhance cybersecurity and reduce the risk of unauthorized intrusion. This feature has rendered situational prevention particularly significant in the field of cybercrime, where technical and environmental modifications may swiftly prevent large-scale harm (Wall, 2011).

Nevertheless, this approach is not without limitations. Critics argue that situational prevention may lead to crime displacement, meaning that offenders shift to alternative targets or platforms rather than abandoning criminal conduct altogether. For instance, blocking a non-compliant website may redirect users to similar platforms hosted in other jurisdictions. However, empirical studies suggest that although some degree of displacement may occur, the overall crime rate tends to decline and criminal activity becomes more costly and less efficient (Clarke, 1997).

In Iranian law, although the concept of situational prevention is not explicitly codified, numerous security and policing policies reflect its underlying principles. National preventive strategies frequently emphasize non-penal mechanisms designed to reduce opportunities for criminal conduct. In comparative practice, institutions such as federal investigative and national security agencies have invested heavily in cyber preventive tools grounded in situational principles. Intrusion detection systems and rapid-response cyber defense mechanisms exemplify measures that create barriers and timely warnings, thereby minimizing opportunities for criminal commission (Goodman, 2015).

In conclusion, situational prevention—grounded in its coherent definition and structured principles—constitutes an effective instrument for reducing criminal opportunities. While it does not replace other forms of prevention, it serves as a critical complement, particularly in the domain of cybercrime, where the digital environment inherently generates abundant opportunities for criminal exploitation and thus demands systematic environmental and technological safeguards.

4. Classification of AI-Based Situational Prevention Methods

Situational prevention of cybercrimes focuses on reducing opportunities for criminal conduct through the identification and elimination of technical and behavioral conditions that facilitate offending. In this context, artificial intelligence and big data processing serve as innovative tools capable of analyzing massive datasets and uncovering criminal patterns (Azizi, 2021). These technologies contribute to cybersecurity by forecasting criminal behavior, detecting intrusions, and analyzing user relationships within digital networks.

In general, four principal methods of AI-based situational prevention may be identified:

a) Crime Prediction through Machine Learning Models

The prediction of crime constitutes the primary and most significant application of artificial intelligence in situational prevention. In this method, data relating to past crimes—including time and location of occurrence, type of attack, and behavioral patterns of users—are input into intelligent systems in order to calculate the probability of recurrence or emergence of new criminal activity through machine learning algorithms (Safayi, 2020).

This approach, commonly referred to as predictive policing, is currently implemented in numerous security systems and, in cyberspace, operates through the analysis of network traffic data and the identification of anomalous user behavior (Maleki, 2022; Perry et al., 2013).

In Iranian law, although the Computer Crimes Act of 2009 makes reference to prevention in certain provisions, data-driven predictive mechanisms remain without a clearly defined legal framework, raising significant questions concerning liability arising from erroneous predictions (Rahimi, 2023).

b) Log Processing and Anomaly Detection

One of the principal data sources in cyberspace consists of system log files containing detailed information about user activities, connection times, types of access, and system modifications. Traditional analytical methods are insufficient for

processing such data, and only machine learning algorithms can effectively identify abnormal or suspicious behavior patterns (Ghadiri, 2021).

For instance, clustering algorithms or unsupervised learning techniques may be employed to detect anomalies within network traffic, enabling early identification of attacks prior to the occurrence of damage.

From a legal standpoint, a key issue concerns the evidentiary value of data generated through artificial intelligence processing—particularly given that existing legislation primarily addresses data retention rather than the authenticity and reliability of algorithmically processed outputs (Mousavi, 2022).

c) Deep Learning-Based Intrusion Detection Systems

Intrusion detection systems represent another significant tool of situational prevention. By utilizing deep learning algorithms such as artificial neural networks, these systems are capable of recognizing complex cyberattack patterns (Amiri, 2023).

However, from a legal perspective, such systems generate challenges related to data privacy and civil liability in cases of system error. Monitoring network traffic may entail the analysis of users' personal information without explicit consent, potentially conflicting with privacy protection principles within Iranian legal doctrine (Hosseini, 2021; Kazemi, 2023).

Accordingly, the deployment of AI-based intrusion detection systems must be accompanied by transparent regulatory frameworks and comprehensive personal data protection mechanisms.

d) Social Network Analysis for Identifying Cyber Offenders

Social network analysis constitutes another method for identifying relationships among individuals, groups, and criminal activities within cyberspace. Artificial intelligence systems are capable of analyzing user data to detect suspicious groups, phishing pages, and organized cybercriminal networks (Mohammadi, 2020).

Nevertheless, this method poses heightened risks of privacy infringement and erroneous labeling of innocent individuals. In the Iranian legal system, the absence of a comprehensive data protection law has resulted in insufficient regulatory oversight of such analytical practices, thereby increasing the risk of misuse of user data (Ghasemi, 2023; Zamani, 2022).

In sum, AI-based situational prevention methods have demonstrated considerable effectiveness in mitigating cyber threats. However, within the Iranian legal system, the absence of explicit standards concerning the evidentiary validity of intelligent data, the allocation of liability for inaccurate predictions, and comprehensive privacy regulations constitute the principal challenges to lawful implementation. The formulation of a structured legal charter governing artificial intelligence and cybersecurity could represent a significant step toward addressing these regulatory deficiencies.

5. Relevant Legal Foundations within the Iranian Legal System

a) Criminal Laws and Procedural Regulations

Within the Iranian legal system, the primary statutory framework governing cybercrimes is the Computer Crimes Act of 2009, recognized as the first comprehensive legislative instrument addressing offenses related to information technology (Rahimi, 2020). This law encompasses provisions relating to criminal offenses, procedural mechanisms, and supplementary regulations. Among its key provisions are those addressing unauthorized access, unlawful interception, and interference with computer data and systems.

The procedural section of the Act introduces mechanisms such as digital data analysis, electronic interception, and traffic data examination to facilitate the detection and prosecution of cybercrimes. Nevertheless, the integration of artificial intelligence technologies into investigative processes remains legally ambiguous, as the legislator primarily contemplated conventional technological tools without defining the role of algorithms and machine learning models in crime detection (Mousavi, 2021).

Furthermore, the Criminal Procedure Code of 2014 contains provisions recognizing the legitimacy of electronic evidence and digital data. However, the collection and analysis of such data through AI-based systems necessitate supplementary regulations clarifying issues of privacy protection and the legality of automated data processing (Hashemi, 2022).

b) Cyberspace Regulations, User Protection, and Data Governance Initiatives

In addition to the Computer Crimes Act, several legislative proposals and policy initiatives have been introduced in recent years to regulate relationships among users, service providers, and the state in cyberspace. Notably, draft legislation concerning

user rights and foundational online services emphasizes data sovereignty, user privacy protection, and platform accountability for unlawful content (Khosravi, 2022).

Although such initiatives do not explicitly reference artificial intelligence, certain provisions mandate domestic data storage and governmental oversight of data-processing algorithms, potentially creating legal and technical challenges for the development of machine learning and big data technologies (Ghasemi, 2023). The absence of comprehensive legislation governing data ownership, user consent, and personal data exploitation remains a substantial obstacle to the lawful application of artificial intelligence in cybercrime prevention.

c) National Strategies on Artificial Intelligence and Data Governance

At the macro-policy level, national strategic documents concerning artificial intelligence emphasize the balanced and ethical development of intelligent technologies and acknowledge their application in security and governance domains (Mirzayi, 2023). These policy frameworks highlight the necessity of establishing legal, ethical, and security standards for deploying artificial intelligence within the criminal justice system.

However, such strategic documents often lack enforceable mechanisms and institutional integration with existing criminal legislation. The absence of coordination between technological policymaking, criminal law legislation, and executive institutions has limited the practical implementation of artificial intelligence and big data tools in cybercrime prevention. Consequently, the establishment of a comprehensive legal framework aligned with the Computer Crimes Act and national data policies is indispensable for the future development of Iranian cybercriminal law.

6. Fundamental Legal and Ethical Challenges in the Use of AI and Big Data for Situational Prevention of Cybercrimes

a) Fundamental Rights and Protection of Privacy

One of the most fundamental challenges in employing artificial intelligence for cybercrime prevention concerns the threat to citizens' privacy. Crime prediction algorithms and behavioral analytics typically rely on large-scale datasets, including locational, communicational, and even psychological information. Because many of these datasets are indirectly identifiable, their collection and processing may result in violations of provisions concerning unauthorized access under Iranian cybercrime legislation (Hosseini, 2021; Rahimi, 2020).

Within the Iranian legal system, there is still no comprehensive statute governing personal data protection; only scattered provisions in ministerial regulations and draft legislation address aspects of privacy. Consequently, the deployment of AI systems for analyzing sensitive data—such as ethnicity, religion, political affiliation, or criminal records—without explicit consent may generate serious conflicts with constitutional principles protecting dignity and individual rights, as well as broader human rights standards (Kazemi, 2023; Nemati, 2023).

b) Data Processing Consent, Legal Basis, and Transparency

Another major issue concerns consent and the legal basis for data processing. In Iranian law, the legitimacy of information processing is generally grounded in informed consent or statutory necessity. However, in AI-based situational prevention systems, data are often automatically extracted from public sources or digital platforms without users being fully aware of the manner or scope of data collection and analysis (Sharifi, 2022).

The absence of binding regulations concerning algorithmic transparency prevents citizens from understanding the extent to which their data are used and the consequences such processing may have for security or judicial decision-making. This situation stands in tension with principles of transparency and the right to information reflected in national AI policy discussions, which emphasize the obligation to clarify the logic of algorithmic decision-making in sensitive domains (Mirzayi, 2023).

c) Error, Algorithmic Bias, and Reliability

Machine learning-based crime prediction systems are inherently exposed to data bias because they are trained on historical datasets. Empirical studies have demonstrated that such systems may disproportionately concentrate surveillance on lower-income regions or specific social groups, thereby increasing the risk of discriminatory monitoring and prosecution (Akbari, 2021).

If similar predictive models are implemented by Iranian cybercrime enforcement agencies without effective legal and ethical oversight, there exists a tangible risk of analytical error and misuse of data. The absence of technical and legal standards for evaluating algorithmic accuracy may undermine the reliability of outcomes and weaken the legitimacy of preventive interventions (Taheri, 2023).

d) Criminal and Civil Liability Arising from Erroneous Decisions

A further complex issue involves the attribution of liability for algorithmic errors. If an intelligent system's decision results in reputational harm or wrongful arrest, the central question becomes whether liability rests with the software developer, the human operator, or the governmental authority deploying the system (Kazemi, 2022).

At present, neither the Computer Crimes Act nor the Criminal Procedure Code explicitly addresses shared human–machine responsibility. Therefore, liability must be inferred from general civil law doctrines concerning causation and fault in supervision. In the absence of specific implementing regulations, however, establishing a causal link between system error and damage remains highly challenging (Azizi, 2023; Rahimi, 2023).

e) Transparency, Explainability, and the Right to Know

In technology law, the principle of explainability constitutes a core element of AI ethics. According to this principle, individuals must be informed of the rationale underlying algorithmic decisions affecting them. Without such transparency, effective objection and remedy mechanisms become illusory (Razavi, 2023).

In Iran, there is currently no explicit obligation to disclose the logic of automated decisions, a gap that may lead to violations of the right to defense and fair trial principles. It is therefore advisable that the legislator draw inspiration from European regulatory models, which recognize the right to obtain meaningful information about automated decision-making processes (European Union, 2024; Hashemi, 2024).

7. Legal Conflicts with International Instruments and Comparative Experiences

a) The Budapest Convention and International Standards on Cybercrime

The Convention on Cybercrime (2001), adopted by the Council of Europe, represents the first binding international instrument addressing computer-related offenses (Council of Europe, 2001). It establishes four principal pillars: criminalization of unauthorized access and computer fraud, protection of data integrity, procedural tools for investigation, and international cooperation.

Article 15 of the Convention emphasizes respect for fundamental human rights, including privacy and freedom of expression, when employing technological surveillance measures. In contrast, Iranian cybercrime legislation tends to prioritize security considerations and lacks an explicit balancing mechanism between surveillance powers and fundamental rights (Rahimi, 2020). Moreover, Iran's non-membership in the Budapest Convention limits the scope of judicial cooperation in cross-border data exchange and prosecution (Hashemi, 2022).

Regarding the use of artificial intelligence in cybercrime prevention, the Budapest standards stress proportionality and necessity in electronic interventions. In Iran, however, no specific directive regulates the scope and duration of large-scale data analysis conducted by security institutions, creating a significant gap between domestic practice and international standards (Mousavi, 2023).

b) European Union Regulatory Models

The European Union Artificial Intelligence Act (2024) constitutes the first comprehensive global legal framework regulating AI applications (European Union, 2024). This regulation adopts a risk-based approach, classifying AI systems into four categories: unacceptable, high-risk, limited-risk, and minimal-risk applications.

Crime prediction systems are categorized as high-risk because of their potential to generate discrimination or infringe upon individual freedoms. Under the Act, developers must conduct fundamental rights impact assessments, ensure algorithmic transparency, and document training data before deployment (Smith, 2024).

For Iran, the EU model offers several key lessons: the necessity of differentiating risk levels in security-related AI applications; the obligation to conduct human rights impact assessments prior to deployment; and the importance of establishing

an independent supervisory authority over predictive systems. At present, no such independent oversight body or structured risk assessment mechanism exists within Iran's legal framework (Ghasemi, 2024).

c) International Risk Management Frameworks

International organizations have also developed influential, though non-binding, frameworks for AI governance. The NIST Artificial Intelligence Risk Management Framework (2023) emphasizes four core pillars: governance, mapping, measurement, and risk management, underscoring the continuous evaluation of ethical, technical, and legal risks associated with AI systems (Nist, 2023).

Similarly, the OECD AI Principles (2019) articulate five key dimensions: inclusive and sustainable growth through AI; respect for human rights; transparency and explainability; developer accountability; and security and system robustness (Oecd, 2019).

These principles may serve as an appropriate model for Iran to integrate ethical considerations with criminal regulatory mechanisms in developing a localized framework for AI-based situational prevention of cybercrimes. The absence of a structured risk management approach in domestic law has resulted in AI deployment being treated predominantly as a technical matter rather than as an issue intertwined with human rights and data governance concerns (Nemati, 2024).

8. Conclusion

The rapid evolution of emerging technologies, particularly artificial intelligence and big data processing, has profoundly transformed the concept of security and crime prevention. In the field of situational prevention of cybercrimes, these technologies provide unprecedented capabilities in analyzing behavioral patterns, detecting threats proactively, and identifying criminal activities in cyberspace. Nevertheless, the analysis conducted in this study demonstrates that within the Iranian legal system, the application of these technologies remains at an early stage and lacks a clear legal, ethical, and institutional foundation.

From a legal perspective, the most significant challenge stems from the absence of a comprehensive statute governing personal data protection and privacy. Although the Computer Crimes Act of 2009 represented an initial step toward criminalizing digital misconduct, its primary focus on punitive measures has left preventive, data-driven, and algorithmic dimensions largely unaddressed. Furthermore, the lack of explicit provisions concerning transparency, informed consent, and the civil liability of developers has resulted in ambiguity regarding the legitimacy and accountability of predictive systems and data analytics employed by security institutions.

From an ethical and social standpoint, the use of artificial intelligence in crime prevention requires adherence to principles such as algorithmic fairness, non-discrimination, explainability, and respect for human dignity. Machine learning systems may suffer from data bias or analytical error, potentially leading to the unjust investigation or prosecution of innocent individuals. Such consequences can undermine public trust in the criminal justice system unless effective oversight mechanisms are established to ensure the accuracy and fairness of algorithmic processes.

Comparative analysis indicates that leading jurisdictions have moved toward risk-based regulatory models, treating technology not merely as a threat but as a tool for intelligent prevention—provided that it operates within a framework of data governance, transparency, and multilayered oversight. In Iran, however, a coherent linkage between national data policies, criminal legislation, and technological institutions has yet to be effectively established.

Legislative and Policy Recommendations

First, it is necessary to enact a comprehensive personal data protection law grounded in principles such as informed consent, purpose limitation, data minimization, storage limitation, and citizens' right of access to their personal information. Such legislation should complement the Computer Crimes Act and explicitly address emerging technologies, including artificial intelligence and big data analytics.

Second, the Computer Crimes Act of 2009 should be amended to include a dedicated chapter on intelligent prevention of cybercrimes, with explicit provisions governing the civil and criminal liability of developers, operators, and public authorities deploying AI-based systems.

Third, interdisciplinary educational capacities must be strengthened for judges, law enforcement officers, and cybercrime specialists in the areas of data analytics and algorithmic literacy, ensuring that preventive decision-making is grounded in a proper understanding of intelligent system functionality.

Ultimately, the principal challenge facing Iranian law in its encounter with artificial intelligence is not technological deficiency but the absence of a coherent legal and ethical infrastructure. If the legislator succeeds in establishing a balanced framework reconciling security interests with fundamental rights, artificial intelligence and big data may become effective instruments for the prevention of cybercrimes. Achieving this objective requires a multidimensional approach integrating law, technology, ethics, and public policy within a structured data governance model—an approach capable of shifting the use of technology from a purely security-oriented application toward a justice-centered and rule-of-law-based paradigm.

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

Akbari, F. (2021). Evaluating algorithmic bias in predictive policing. *Journal of Behavioral Sciences and Technology*(3), 79-90.
Amiri, A. (2023). Application of deep learning in computer network security and its legal challenges. *Journal of Legal Research and Technology*(5), 75-90.
Azizi, M. R. (2021). Situational prevention of cybercrimes with an artificial intelligence approach. *Cyber Law Journal*, *3*(1), 45.
Azizi, N. (2023). *Artificial Intelligence and Legal Challenges in Iran*. Mizan Publishing.
Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger. https://doi.org/10.5040/9798400636554
Cath, C. (2018). Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A*, *376*(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080
Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies*.
Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, *16*, 41-96.
Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.
Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science advances*, *4*(1), eaao5580. https://doi.org/10.1126/sciadv.aao5580
European Union. (2024). *Artificial Intelligence Act - Final Text*.
Felson, M., & Clarke, R. V. (1998). *Opportunity Makes the Thief: Practical Theory for Crime Prevention*. Home Office Research Study.
Ghadiri, H. (2021). Cybersecurity management through log data analysis using AI methods. *Journal of Information Technology and Law*(1), 51.
Ghasemi, N. (2023). Data sovereignty and the legal challenges of Big Data in Iran. *Public Law and Technology Quarterly*(1), 57-70.
Ghasemi, N. (2024). The EU Artificial Intelligence Act and its implications for non-European legal systems. *Iranian IT Law Quarterly*(1), 45-60.
Goodman, M. (2015). *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. Doubleday.
Hashemi, A. A. (2022). *Criminal Procedure for Cybercrimes*. SAMT Publications.
Hashemi, A. A. (2024). *A Comparative Analysis of Algorithmic Proceedings in Iranian and European Law*. Jangal Publications.
Hosseini, L. (2021). *Privacy and Personal Data in Iran's Cyberspace*. Mizan Publishing.
Kazemi, M. (2022). Civil liability of smart system developers. *Journal of Comparative Technology Law*(1), 65-80.
Kazemi, M. A. (2023). Privacy and cyber surveillance in the Iranian legal system. *Public Law Research Journal*, *6*(1), 56.
Khosravi, M. (2022). Challenges of the bill for the protection of user rights in cyberspace. *Iranian IT Law Journal*(3), 117-135.
Maleki, P. (2022). Predictive policing and technological crime prevention in cyberspace. *Journal of Police Science*(75), 68.
Marr, B. (2018). *Data-Driven HR: How to Use Analytics and Metrics to Drive Performance*. Kogan Page.

Mirzayi, S. (2023). A comparative analysis of Iran's national policies in the field of AI and data. *Journal of Law and New Technologies*(4), 38-52.
Mohammadi, F. (2020). Big Data analysis in identifying cybercrimes and its legal challenges. *IT Law Quarterly*, *4*(2), 98-115.
Mousavi, E. (2022). A legal analysis of digital data in the Computer Crimes Law of Iran. *Modern Law Journal*(4), 127.
Mousavi, F. (2021). A comparative study of electronic evidence in the Iranian judicial system. *Journal of Modern Criminal Law Studies*(2), 65-85.
Mousavi, F. (2023). Legal challenges of international cooperation in cybercrimes. *Journal of Comparative Iranian and European Law*(3), 41-58.
Najafi Abrandabadi, A. H. (2011). *Crime Prevention in Iranian Criminal Policy*. Mizan Publishing.
Nemati, S. (2023). Fundamental rights challenges in the application of AI in the criminal justice system. *Iranian Criminal Law Research*(2), 89-105.
Nemati, S. (2024). AI risk management and international models. *Research in Technology Law and Smart Ethics*(2), 43-57.
Nist. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1.jpn
Oecd. (2019). *Recommendation of the Council on Artificial Intelligence*. OECD Publishing.
Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation.
Rahimi, M. (2020). *Criminal Law of Information Technology*. Mizan Publishing.
Rahimi, S. (2023). Civil liability arising from AI error prediction in the crime prevention process. *Journal of Comparative Law Studies*(2), 93.
Razavi, H. (2023). Explainability of algorithmic decisions and citizenship rights. *Journal of Law and Ethics of Technology*(2), 29-44.
Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
Safayi, N. (2020). Artificial Intelligence and the transformation in the criminal prevention system. *Criminal Law Research Quarterly*(2), 112.
Sharifi, N. (2022). Legal foundations of consent in data processing. *IT Law Journal*(4), 54-68.
Smith, A. (2024). Regulating High-Risk AI under the EU AI Act. *European law review*, *39*, 210-225.
Taheri, M. (2023). *Legal Standards in Machine Learning and Data Liability*. University of Tehran Press.
Wall, D. S. (2011). *Cybercrime: The Transformation of Crime in the Information Age* (2nd ed.). Polity Press.
Zamani, Y. (2022). Legal challenges of user data analysis in social networks. *Quarterly of Communication and Media Law*(3), 149.