How to cite this article:
Kamali, A., Ashrafy, M., & Saeedi, Y. (2027). The Role of Artificial Intelligence in Situational Crime Prevention with an Emphasis on Privacy Challenges. *Journal of Historical Research, Law and Policy, 5*(2), 1-16. https://doi.org/10.61838/jhrlp.351

Article history:
Original Research

Dates:
Submission Date: 10 February 2026
Revision Date: 24 May 2026
Acceptance Date: 31 May 2026
First Pubication Date: 01 June 2026
Final Pubication Date: 01 March 2027

The Role of Artificial Intelligence in Situational Crime Prevention with an Emphasis on Privacy Challenges

1. Alireza. Kamali [1] : Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran
2. Mahmoud. Ashrafy [2*]: Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran
3. Yasin. Saeedi [3]: Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran

*corresponding author's email: mahmood.ashrafy@iau.ac.ir

ABSTRACT

This article examines the role of artificial intelligence in situational crime prevention with particular emphasis on privacy challenges. Situational crime prevention focuses on reducing criminal opportunities by modifying environmental, technological, and organizational conditions that facilitate crime. Artificial intelligence has expanded this preventive model through predictive analytics, smart surveillance, biometric identification, cyber threat detection, automated risk assessment, and data-driven criminal justice management. These technologies can improve the speed, accuracy, and efficiency of preventive interventions by identifying crime patterns, detecting suspicious behavior, supporting resource allocation, and strengthening responses to both physical and cybercrime. However, the use of artificial intelligence in crime prevention also creates serious legal and ethical concerns. Because AI systems depend on extensive data collection and algorithmic processing, they may threaten informational privacy, increase mass surveillance, enable discriminatory profiling, reduce transparency, and weaken accountability. The article argues that the preventive benefits of AI cannot justify unrestricted monitoring or automated suspicion. Instead, AI-based situational prevention must be governed by legality, necessity, proportionality, transparency, explainability, human oversight, data minimization, purpose limitation, independent auditing, and effective remedies. The study concludes that artificial intelligence should function as a supportive tool for human decision-making rather than a substitute for legal judgment. A legitimate model of AI-based crime prevention must reduce criminal opportunities while preserving privacy, dignity, equality, and the rule of law.

Keywords: *Artificial intelligence; situational crime prevention; privacy; predictive policing; criminal justice; algorithmic surveillance; data protection; accountability.*

Introduction

The rapid development of artificial intelligence has transformed the contemporary landscape of criminal justice, security governance, and crime prevention. In traditional criminal justice systems, the response to crime was primarily retrospective: the state intervened after the commission of an offense, identified the offender, gathered evidence, prosecuted the accused, and imposed punishment when liability was established. However, the expansion of preventive criminology has shifted part of the criminal justice agenda from reaction to anticipation, from punishment to risk management, and from offender-centered intervention to the modification of environments in which crime becomes possible. In this context, situational crime prevention has emerged as a practical and policy-

oriented approach that seeks to reduce criminal opportunities by changing the immediate conditions that facilitate crime. The importance of artificial intelligence in crime prevention has been emphasized in recent criminological studies because AI systems can process large volumes of data, detect hidden patterns, and support preventive decision-making before crime occurs (1). This technological capacity gives AI a particular relevance for situational crime prevention because both AI-based prevention and situational prevention are concerned with prediction, opportunity reduction, risk detection, and timely intervention.

Situational crime prevention is based on the assumption that many criminal acts are not only the result of individual motivation but also the product of accessible opportunities, weak guardianship, vulnerable targets, and environments that make illegal conduct easier or less risky. Therefore, instead of focusing exclusively on moral reform, rehabilitation, or post-crime punishment, situational prevention attempts to alter the practical conditions under which crime occurs. AI expands this preventive logic by allowing security institutions to monitor environments more intelligently, identify risk indicators more quickly, and intervene more precisely. Contemporary discussions of AI in crime prevention point to its capacity to support risk mapping, automated surveillance, predictive analytics, and the identification of recurring patterns in criminal behavior (2). These developments indicate that artificial intelligence is not merely an auxiliary technical instrument; it is increasingly becoming part of the architecture of criminal policy itself.

The significance of AI in crime prevention is especially visible in the transition from traditional surveillance to algorithmic surveillance. Conventional surveillance depended on human observation, physical patrols, manual reports, and relatively limited databases. AI-enabled surveillance, by contrast, can integrate video feeds, biometric information, digital traces, geolocation data, social media activity, cyber activity, and historical crime records. Such systems may detect suspicious behavior, forecast crime-prone locations, identify abnormal digital transactions, or support rapid responses to emergencies. In cybersecurity, AI has been used to combat computer crimes by detecting intrusion patterns, malware behavior, phishing attempts, and anomalous network activity (3). In urban security, AI may strengthen monitoring of public spaces and support the allocation of police resources to areas where crime opportunities are more concentrated. In judicial and procedural contexts, AI has also been discussed as a tool for improving efficiency, case processing, and criminal justice decision-making (4). These applications reveal that AI affects not only crime prevention in the narrow sense but also broader institutional processes within criminal justice.

At the same time, the integration of AI into crime prevention creates a complex legal and ethical dilemma. The same technologies that make prevention more effective may also increase the capacity of the state and private actors to collect, analyze, and retain personal information. AI systems require data, and the more predictive and adaptive they become, the more they tend to rely on extensive datasets. This creates serious concerns about privacy, informational self-determination, autonomy, due process, fairness, and democratic accountability. Studies on algorithmic discrimination have shown that AI systems may reproduce or intensify social bias when they are trained on unequal, incomplete, or historically biased data (5). In crime prevention, this problem becomes particularly serious because biased predictions may lead to disproportionate surveillance of certain communities, repeated targeting of specific groups, and the transformation of statistical suspicion into institutional practice.

Privacy is not a secondary issue in AI-based crime prevention; it is one of the central conditions for the legitimacy of preventive security policy. When AI systems monitor individuals, classify risk levels, identify behavioral patterns, or infer future threats, they do not merely observe reality. They participate in shaping how institutions understand

suspicion, danger, and security. This is why fair-trial guarantees and procedural safeguards become relevant even before formal prosecution begins. Research on the right to a fair trial in the context of AI-based criminal justice warns that algorithmic tools can affect procedural justice when their operation is opaque, when affected persons cannot challenge their conclusions, or when decision-makers over-rely on automated outputs (6). Although situational crime prevention is primarily preventive, its effects may extend into policing, investigation, prosecution, and judicial assessment; therefore, privacy and due process must be considered together.

The problem is intensified by the fact that AI systems often operate through probabilistic reasoning rather than direct proof. They may identify correlations, predict risks, or classify individuals and places according to statistical models. While such outputs may be useful for preventing crime, they can also blur the distinction between evidence and prediction, between risk and guilt, and between preventive attention and punitive suspicion. The use of AI in criminal policy and criminal procedure has therefore raised important questions about the limits of prediction in criminal justice and the degree to which algorithmic assessments should influence institutional behavior (7). If AI-based situational prevention is not carefully regulated, it may produce a preventive model in which individuals are treated as potential offenders not because of what they have done, but because of what an algorithm predicts they might do.

Another reason this topic is important is that AI changes the distribution of responsibility in criminal justice systems. When a human officer makes a preventive decision, responsibility can usually be attributed through ordinary legal and administrative mechanisms. When an AI system recommends an intervention, triggers an alert, misidentifies a person, or produces a discriminatory risk score, responsibility becomes more difficult to assign. Legal studies on criminal liability arising from AI errors emphasize the need to determine whether liability should attach to developers, operators, users, institutions, or autonomous systems themselves (8). Similar challenges appear in discussions of AI criminal liability in the digital era, where the increasing autonomy of AI systems complicates traditional frameworks of fault, causation, and accountability (9). In the field of situational crime prevention, these debates are highly relevant because preventive AI tools may cause harm even when no crime has occurred: they may falsely identify a person, unjustifiably expose private information, or trigger intrusive monitoring.

The Iranian criminal legal context also gives this issue particular importance. Recent studies have examined the challenges of assigning criminal liability to autonomous AI systems in the Iranian criminal legal system and have emphasized the need for legislative clarification (10). Other research has explored the feasibility of criminal liability for AI based on philosophical foundations, suggesting that legal systems must address whether autonomous systems can meaningfully be treated as responsible agents or whether responsibility must remain attached to human and institutional actors (11). These debates are closely connected to AI-based crime prevention because preventive systems may operate autonomously or semi-autonomously in ways that influence security decisions, data collection, and individual rights. When such systems violate privacy or produce harmful outcomes, legal systems need clear rules for responsibility, redress, and institutional control.

The social impact of AI also requires attention. AI does not enter a neutral social environment; it interacts with existing inequalities, institutional practices, public expectations, and cultural understandings of security. Criminological analysis of the social impact of AI has shown that AI affects not only technical processes but also social relations, trust in institutions, and public perceptions of criminal justice (12). Similarly, studies on criminal psychology and AI indicate that algorithmic systems may influence how risk factors are interpreted and how criminal behavior is predicted (13). These insights suggest that AI-based situational prevention must be examined not only

as a technical innovation but also as a social and legal phenomenon that reshapes the relationship between citizens, public spaces, digital infrastructures, and state power.

The central problem of this article is therefore the tension between the preventive benefits of AI and the privacy challenges created by its use in situational crime prevention. On the one hand, AI may strengthen crime prevention by improving accuracy, speed, resource allocation, and pattern recognition. On the other hand, it may expand surveillance, weaken privacy, reproduce discrimination, reduce transparency, and create new forms of legal uncertainty. The objective of this study is to analyze the role of artificial intelligence in situational crime prevention while critically examining the privacy challenges and legal safeguards necessary for its legitimate use.

Artificial Intelligence and the Transformation of Situational Crime Prevention

Artificial intelligence transforms situational crime prevention by changing the way crime opportunities are identified, evaluated, and controlled. Traditional situational prevention relied on physical and organizational techniques such as improving lighting, increasing guardianship, controlling access, hardening targets, installing cameras, redesigning vulnerable spaces, and increasing the perceived risk of detection. These methods remain important, but AI adds a new layer of preventive capacity by converting raw data into actionable intelligence. Studies on the role of AI in crime prevention emphasize that artificial intelligence can support decision-making by recognizing patterns that may be invisible to human observers and by helping institutions move from general prevention to more targeted intervention (1). This means that AI can make situational prevention more dynamic, because preventive measures no longer depend only on static environmental design but also on continuous data analysis.

The most visible transformation appears in predictive policing and risk forecasting. Predictive policing systems use historical crime records, spatial information, temporal patterns, demographic variables, and sometimes broader datasets to estimate where certain crimes may occur or which situations may require preventive attention. A reflection on the trend of AI in crime prevention shows that AI is increasingly used to identify risk-prone environments and to support preventive policing strategies (2). In situational terms, this allows institutions to anticipate opportunity structures before they produce criminal incidents. For example, if an algorithm detects that thefts frequently occur in certain commercial areas at particular times under particular environmental conditions, law enforcement agencies may increase patrols, improve surveillance, or advise businesses to modify access control. The preventive logic is not necessarily to identify a future offender but to reduce the conditions under which offending becomes easier.

AI also transforms surveillance by making it more automated, integrated, and analytical. A conventional camera records images, but an AI-enabled camera may detect unusual movement, identify objects, recognize faces, count crowds, classify behavior, or alert authorities to potential threats. In cybersecurity, AI systems can monitor digital environments in ways that resemble situational prevention in physical spaces: they detect vulnerabilities, identify suspicious access attempts, and respond to threats before damage occurs. Research on using AI to combat computer crimes and improve cybersecurity performance demonstrates that AI can strengthen preventive mechanisms by identifying abnormal cyber behavior and supporting rapid technical responses (3). This shows that situational prevention is no longer limited to streets, buildings, and public spaces; it also extends to digital environments where criminal opportunities are created by weak passwords, insecure networks, software vulnerabilities, and delayed detection.

Another important transformation concerns the speed of preventive response. Human institutions often suffer from delay: reports must be received, analyzed, transmitted, and acted upon. AI can reduce this delay by automatically detecting risk signals and generating alerts. In criminal justice administration, AI has been discussed as a means of improving the efficiency of criminal case processing and assisting institutional decision-making (4). Although trial efficiency is not identical to situational prevention, the same logic of technological acceleration applies. AI systems can process information faster than human officers, enabling earlier recognition of patterns and quicker preventive intervention. In contexts such as fraud detection, online abuse, cybercrime, or public-space monitoring, speed can be decisive because delayed detection may allow harm to spread.

AI also supports the personalization and localization of preventive strategies. Traditional prevention often applies uniform measures across broad environments. AI can help tailor preventive interventions to specific places, times, behaviors, and risk profiles. For instance, an algorithm may suggest different prevention strategies for cyber fraud, urban theft, domestic violence risk, or organized digital scams. Studies on AI in criminal justice management describe AI as a tool that can assist institutions in organizing information, managing criminal justice processes, and improving operational effectiveness (14). This managerial capacity is important for situational crime prevention because prevention requires not only theoretical knowledge but also institutional coordination, resource allocation, and practical decision-making. AI can help determine where preventive resources are most urgently needed.

However, the transformation of situational prevention through AI is not simply a story of improvement. AI systems may produce false positives, false negatives, biased classifications, and misleading risk assessments. A false positive may cause innocent individuals or harmless situations to be treated as suspicious, while a false negative may fail to detect genuine threats. In criminal psychology, AI-based risk assessment raises questions about the interpretation of risk factors and the possibility that complex human behavior may be reduced to algorithmic categories (13). Situational prevention must therefore avoid treating AI outputs as objective truth. AI can assist human judgment, but it should not replace the legal, ethical, and contextual reasoning necessary in criminal justice.

The relationship between AI and criminal policy is also significant. Criminal policy determines how societies define threats, allocate enforcement resources, and balance prevention with rights protection. AI increasingly participates in this process by influencing what institutions see, prioritize, and classify as risky. Research on AI and criminal justice policymaking in contemporary Iran emphasizes both the opportunities and challenges that AI creates for judicial officers and criminal policy actors (15). This is particularly relevant to situational crime prevention because preventive choices are never purely technical. Deciding which spaces to monitor, which data to collect, which risks to prioritize, and which interventions to authorize reflects legal and political judgments. AI may inform these judgments, but it cannot determine their legitimacy on its own.

The expansion of AI also changes the concept of guardianship in situational crime prevention. In classical situational theory, guardianship often referred to the presence of police officers, security personnel, neighbors, employees, or other capable observers who could prevent crime by increasing the likelihood of detection. AI creates algorithmic guardianship: digital systems that observe, analyze, and alert. This can be beneficial in environments where human monitoring is impossible or insufficient. In cybercrime, for example, human observation alone cannot detect every intrusion attempt or malicious pattern. AI-based cybersecurity tools can operate continuously and identify threats across large networks (3). Yet algorithmic guardianship also raises the question of who guards the guardians. If AI systems monitor citizens, institutions must ensure that these systems are themselves subject to oversight, auditing, and legal constraints.

AI also affects target hardening. Traditional target hardening involves strengthening locks, barriers, authentication systems, and access controls. AI enables adaptive target hardening, where systems learn from attacks and modify defenses accordingly. In financial crime prevention, identity verification, and cyber fraud detection, AI can recognize unusual transactions or suspicious login behavior and impose additional verification steps. This reflects the situational principle of increasing the effort required to commit crime. But if AI-based access control relies on biometric data, behavioral profiling, or continuous identity tracking, it may create privacy risks. Research on algorithmic discrimination demonstrates that AI-based classifications can produce unequal outcomes when systems are trained on biased data or when regulatory safeguards are insufficient (5). Thus, even a preventive tool designed to protect targets may become problematic if it unfairly excludes, misclassifies, or monitors individuals.

AI may also reduce rewards and disrupt criminal opportunities by detecting and blocking illegal gains. In cyber environments, automated fraud detection can identify suspicious transactions before completion. In physical environments, intelligent surveillance can deter theft by increasing the perceived likelihood of detection. In administrative contexts, AI can identify irregularities that suggest corruption, document fraud, or identity misuse. The preventive value of AI lies partly in making criminal opportunities less attractive. Nevertheless, if preventive systems become too intrusive, they may impose generalized suspicion on ordinary activity. Studies on the broader social impact of AI in criminology warn that AI can reshape social life by normalizing surveillance and changing how individuals behave in monitored environments (12). Situational prevention should therefore be designed in a way that deters crime without turning everyday life into a permanent object of suspicion.

The use of AI in situational prevention also has implications for criminal liability when harm occurs. If an AI-based monitoring system misidentifies a person as a suspect and causes wrongful intervention, legal systems must determine who is responsible. Studies on liability arising from AI errors highlight the difficulty of assigning responsibility when errors result from complex interactions between developers, data providers, users, and autonomous system behavior (8). In cybercrime contexts, the problem becomes even more complex when AI systems are used both by offenders and by prevention authorities. Research on attributing liability to AI with emphasis on causal relationships in cybercrimes indicates that causation becomes difficult to establish when autonomous systems contribute to harmful outcomes (16). This is highly relevant to AI-based prevention because preventive systems can themselves become sources of legal harm.

The transformation of situational prevention through AI also forces a reconsideration of the boundary between public and private security. Many AI systems used for prevention are developed by private companies, deployed by private platforms, or operated through public-private partnerships. Digital platforms use AI to detect fraud, hate speech, child exploitation, cyber abuse, and suspicious transactions. Private security companies use AI for surveillance, access control, and biometric identification. State institutions may rely on privately developed algorithms whose internal logic is not fully transparent. This creates legal and ethical challenges because preventive power may be exercised through technological infrastructures that are not fully accountable to public law. In this environment, the use of AI in criminal policy and criminal procedure requires clear standards for transparency, accountability, and institutional responsibility (7).

AI therefore transforms situational crime prevention in three interconnected ways. First, it increases preventive capacity by improving prediction, detection, monitoring, and response. Second, it expands the scope of prevention from physical environments to digital and hybrid spaces. Third, it introduces new legal, ethical, and social risks that must be addressed if AI-based prevention is to remain legitimate. The central challenge is not whether AI can

contribute to situational crime prevention; the evidence and literature suggest that it can. The more important question is how AI can be used in a way that preserves privacy, prevents discrimination, maintains human oversight, and respects the rule of law.

Privacy Challenges and Legal-Ethical Risks of AI-Based Crime Prevention

The main privacy challenge in AI-based situational crime prevention arises from the fact that artificial intelligence depends on data-intensive operations. AI systems do not prevent crime through intuition; they rely on collection, classification, comparison, prediction, and continuous learning. This means that preventive AI often requires access to personal information, behavioral data, biometric identifiers, digital traces, and environmental records. While these data can improve preventive accuracy, they can also expose individuals to extensive monitoring. Research on the importance of AI in crime prevention recognizes the preventive value of such systems but also implies the need to examine the legal limits of their use (1). Privacy becomes vulnerable when prevention is treated as a justification for unlimited data collection.

The first major risk is mass surveillance. AI makes surveillance more scalable because it can analyze large amounts of information faster and more consistently than human observers. Cameras, sensors, smartphones, online platforms, financial systems, and administrative databases can all become sources of preventive intelligence. In traditional surveillance, the practical limits of human attention created natural constraints. AI reduces those constraints by allowing automated monitoring across time and space. Criminological work on the social impact of AI warns that the age of artificial intelligence can reshape social behavior by increasing the presence of automated observation in everyday life (12). In situational crime prevention, this creates the danger that public safety policies may normalize permanent monitoring as an ordinary condition of citizenship.

The second risk concerns informational privacy. AI-based prevention does not only observe visible behavior; it may infer hidden characteristics, predict future conduct, or create risk profiles. A person may be classified as high-risk based on location history, social connections, online activity, purchasing patterns, or association with certain environments. These classifications may occur without the person's knowledge and without meaningful opportunity to challenge the result. Research on algorithmic discrimination shows that algorithmic systems may generate harmful classifications when they rely on biased or incomplete data (5). In preventive criminal justice, such classifications are particularly dangerous because they may produce suspicion without individualized evidence. A person may become visible to law enforcement not because of a concrete act but because of statistical resemblance to a risk category.

Biometric surveillance creates a particularly serious privacy concern. Facial recognition, voice identification, gait analysis, fingerprint databases, iris recognition, and other biometric tools can support situational prevention by identifying suspects, controlling access, or detecting unauthorized presence. However, biometric data are deeply personal because they are attached to the body and cannot easily be changed when compromised. If biometric systems are inaccurate, biased, or insecure, the consequences may be severe. Studies on AI-related criminal liability in the digital era suggest that legal frameworks must adapt to harms created by AI systems, including errors and violations arising from automated technologies (9). In the context of biometric crime prevention, such adaptation is essential because wrongful identification can lead to intrusive police intervention, reputational harm, and deprivation of liberty.

The third risk is algorithmic opacity. Many AI systems, especially those based on complex machine learning models, operate in ways that are difficult for ordinary users, affected individuals, and even institutional decision-makers to understand. This “black box” problem undermines transparency and accountability. If an AI system recommends increased surveillance of a neighborhood, flags a person as suspicious, or predicts a high probability of criminal activity, affected individuals may not know the basis of that decision. Research on fair-trial rights in AI-based criminal justice emphasizes that transparency and contestability are necessary when AI tools influence criminal justice outcomes (6). Although situational prevention may occur before trial, opacity remains problematic because preventive decisions can affect liberty, privacy, mobility, and access to public spaces.

The fourth risk is discrimination. AI systems learn from data, and data often reflect existing social inequalities. If historical policing practices disproportionately targeted certain neighborhoods, an algorithm trained on those records may predict higher risk in the same neighborhoods, leading to more policing, more recorded incidents, and further reinforcement of the original pattern. This feedback loop can make discrimination appear objective because it is expressed through data rather than explicit prejudice. Research on algorithmic discrimination and regulatory measures shows that legal systems must address multiple forms of algorithmic bias, including discriminatory outcomes caused by data, design, and deployment choices (5). In situational crime prevention, discrimination may appear as unequal surveillance, unequal suspicion, or unequal exposure to preventive control.

The fifth risk concerns the erosion of the presumption of innocence. Situational crime prevention is not supposed to punish individuals; it is designed to reduce opportunities for crime. However, AI-based prediction may blur the line between prevention and suspicion. If someone is treated as a potential offender because of algorithmic risk scoring, the system may impose a practical burden on that individual even without formal accusation. Studies on AI in criminal policy and procedure highlight the importance of examining how AI affects procedural rights and criminal justice decision-making (7). Preventive systems must therefore be carefully limited so that they do not become informal mechanisms of punishment without trial.

The sixth risk involves data security. AI-based prevention systems store and process sensitive information. If these systems are hacked, misused, or inadequately protected, the data collected for security purposes may itself become a source of harm. In cybercrime prevention, AI can improve cybersecurity performance by detecting threats and strengthening defenses (3). Yet the same systems may become attractive targets for criminals because they contain valuable personal and institutional data. This creates a paradox: technologies designed to prevent crime may generate new criminal opportunities if their data infrastructures are insecure. Situational prevention must therefore include not only the prevention of external crime but also the prevention of misuse within preventive systems.

The seventh risk is function creep. Data collected for one preventive purpose may later be used for another purpose. For example, information gathered to prevent terrorism may be used for ordinary policing; data collected for traffic safety may be used for criminal investigations; biometric databases created for identity verification may become tools of generalized surveillance. The risk of function creep is particularly high in AI systems because integrated databases increase the value of data reuse. Research on criminal justice management and AI shows that AI can improve institutional efficiency by organizing and processing information (14). However, efficiency must not become a justification for unrestricted secondary use of personal data. Legal systems must define purpose limitations and prevent the gradual expansion of surveillance beyond its original justification.

The eighth risk concerns responsibility for harm. If an AI system violates privacy, produces discriminatory outputs, or causes wrongful intervention, it may be unclear who should be held responsible. Developers may claim that users deployed the system improperly; users may claim that they relied on technical expertise; institutions may claim that the system only supported human decision-making; and vendors may protect their algorithms as trade secrets. Studies on legal frameworks of criminal liability for AI systems emphasize the need to clarify responsibility in the digital era (17). Similarly, research on autonomous AI in the Iranian criminal legal system argues that legislative necessities arise when existing doctrines cannot adequately address harms caused by autonomous systems (10). In AI-based situational prevention, accountability cannot remain vague because privacy violations require remedies.

The ninth risk relates to causation. AI systems often operate as part of complex networks involving data providers, software developers, institutional users, human supervisors, and automated feedback mechanisms. When harm occurs, identifying the causal chain can be difficult. Research on attributing liability to AI with emphasis on causal relationships in cybercrimes highlights the difficulty of determining responsibility when autonomous or semi-autonomous systems contribute to unlawful outcomes (16). In privacy-related harms, causation may be even more complicated because damage may result from data collection, later inference, unauthorized sharing, algorithmic classification, or institutional action based on automated output. A clear legal framework must therefore address both direct and indirect harms.

The tenth risk concerns public trust. Crime prevention depends on cooperation between citizens and institutions. If people believe that AI-based prevention is intrusive, discriminatory, secretive, or unaccountable, trust in criminal justice institutions may decline. Studies on AI and criminal justice policymaking in Iran emphasize that AI creates opportunities for judicial officers but also introduces challenges that must be managed through appropriate policy design (15). Trust is especially important because situational prevention often operates in public spaces and everyday environments. Citizens may accept reasonable security measures when they are transparent, lawful, and proportionate, but they may resist systems that treat ordinary life as a continuous source of suspicion.

The ethical risks of AI-based prevention also include dehumanization of criminal justice. When decisions are mediated by algorithms, individuals may be reduced to risk scores, behavioral categories, or data points. Criminal psychology research on AI and risk factors indicates that artificial intelligence can influence how human behavior is understood and classified (13). This may be useful for identifying risk, but it can also oversimplify complex social, psychological, and environmental realities. Situational prevention must avoid reducing people to predictive profiles. Ethical prevention should focus on reducing opportunities for harm while preserving human dignity and avoiding unnecessary intrusion.

Another legal-ethical problem is the possible privatization of preventive power. Many AI tools are created by private companies and deployed through contractual arrangements with public institutions. If proprietary algorithms influence public security decisions, democratic oversight may be weakened. Private actors may control technical knowledge, data architecture, and system design while public institutions remain formally responsible for outcomes. Studies on criminal liability arising from AI errors emphasize that responsibility must be addressed in relation to the actors who design, deploy, and benefit from AI systems (8). This issue is especially important in privacy protection because private vendors may process sensitive data while affected individuals have limited visibility into how their information is used.

Finally, AI-based situational crime prevention creates a normative challenge: how much privacy should society sacrifice for security? This question cannot be answered by technology alone. Some uses of AI may be justified when they are necessary, proportionate, transparent, and subject to oversight. Other uses may be illegitimate because they create excessive surveillance or unjustified data collection. Research on special features of criminal liability concerning AI demonstrates that AI requires legal analysis adapted to its unique characteristics (18). The same is true of privacy. Traditional privacy rules may be insufficient when AI systems can infer sensitive information from ordinary data. Therefore, privacy protection must evolve from a narrow focus on secrecy toward a broader model of data governance, algorithmic accountability, and rights-based prevention.

Regulatory Frameworks and Strategies for Balancing AI-Based Prevention and Privacy Protection

The legitimate use of artificial intelligence in situational crime prevention requires a regulatory framework capable of balancing security needs with privacy protection. Such a framework must begin with the principle of legality. AI-based preventive measures should not operate in a legal vacuum, especially when they involve surveillance, biometric identification, predictive profiling, or automated decision-making. Research on legal frameworks of criminal liability for AI systems emphasizes the need for clear rules that define responsibility, institutional duties, and the legal consequences of AI-related harms (17). In the field of situational crime prevention, legality means that authorities must have a defined legal basis for collecting data, deploying AI tools, retaining information, sharing outputs, and intervening based on algorithmic assessments.

The second principle is necessity. AI should be used in crime prevention only when it addresses a genuine preventive need that cannot be achieved through less intrusive means. Not every security problem requires algorithmic surveillance. Some risks may be managed through environmental design, community engagement, ordinary policing, or non-invasive technologies. Studies on AI in crime prevention emphasize its importance and potential, but this potential should be understood as conditional rather than unlimited (1). Necessity requires institutions to justify why AI is appropriate for a specific preventive purpose. For example, AI-based anomaly detection may be necessary in cybersecurity environments where threats occur rapidly and at large scale, while continuous facial recognition in ordinary public spaces may require a much stronger justification.

The third principle is proportionality. Even when AI use is lawful and necessary, it must not impose excessive burdens on privacy and liberty. Proportionality requires a careful comparison between the preventive benefit and the rights-related cost. If a system collects extensive biometric data to prevent minor offenses, the intrusion may be disproportionate. If a predictive tool subjects an entire neighborhood to increased surveillance based on weak statistical correlations, the measure may also be disproportionate. Research on algorithmic discrimination demonstrates that regulatory systems must evaluate not only the formal design of AI but also its actual social effects (5). Proportionality therefore requires impact assessment before deployment and continuous evaluation after implementation.

Transparency is another essential requirement. Individuals and communities should know when AI is being used in crime prevention, what type of data it processes, what purpose it serves, and what safeguards exist. Transparency does not necessarily require disclosure of every technical detail, especially where security concerns are legitimate, but it does require meaningful public information and institutional explainability. Research on fair-trial rights and AI in criminal justice shows that the use of AI becomes problematic when affected persons cannot understand or challenge algorithmic influence (6). In situational prevention, transparency is necessary even before

trial because preventive AI may shape policing patterns, surveillance intensity, and individual exposure to state power.

Human oversight must also be central. AI should support human decision-making rather than replace legal judgment. This is especially important when preventive measures affect privacy, liberty, or equality. Human oversight means that trained officials must evaluate AI outputs, consider context, identify possible errors, and remain responsible for final decisions. Research on improving criminal case efficiency through AI suggests that AI can assist criminal justice processes, but assistance should not become uncontrolled automation (4). In situational crime prevention, human oversight is needed to prevent mechanical reliance on risk scores and to ensure that preventive action remains legally and ethically justified.

Accountability is closely connected to oversight. A regulatory framework must identify who is responsible for AI system design, data quality, deployment, monitoring, error correction, and rights violations. Studies on criminal liability arising from AI errors argue that legal systems must determine how responsibility should be assigned when AI produces harmful outcomes (8). Similarly, research on autonomous AI in the Iranian criminal legal system emphasizes legislative necessities regarding liability and accountability (10). In AI-based prevention, accountability should include developers, public institutions, operators, supervisors, and decision-makers. It should also include mechanisms for complaint, review, compensation, and correction.

Data minimization is another core strategy. AI systems should collect only the data necessary for a defined preventive purpose. Excessive data collection increases the risk of misuse, breach, discrimination, and function creep. In cybersecurity, AI may require large-scale data analysis to detect threats, but even in this field, data governance must distinguish between necessary technical information and unnecessary personal exposure (3). In physical surveillance, data minimization may require limiting retention periods, restricting access, anonymizing information where possible, and avoiding unnecessary biometric collection. Preventive effectiveness must be pursued through precise data use rather than indiscriminate accumulation.

Purpose limitation must accompany data minimization. Data collected for one purpose should not be reused for unrelated purposes without legal authorization and rights-based assessment. AI systems become more powerful when databases are integrated, but integration can undermine privacy if it allows continuous expansion of surveillance. Research on AI in criminal justice management emphasizes the institutional value of organized information and efficient processing (14). However, institutional efficiency must be limited by legal purpose. A system designed to prevent cyber intrusions should not become a general tool for monitoring employee behavior unless a separate lawful basis exists. A database created for access control should not automatically become an investigative database.

Algorithmic auditing is also necessary. AI systems should be tested for accuracy, bias, security, and proportionality before and after deployment. Audits should examine training data, error rates, demographic disparities, false positives, false negatives, and real-world consequences. Research on algorithmic discrimination highlights the importance of regulatory measures capable of detecting and correcting discriminatory outcomes (5). In situational prevention, auditing should be independent where possible because institutions that benefit from AI deployment may have incentives to underestimate its risks. Independent audits can help ensure that preventive technologies remain aligned with legal and ethical standards.

Privacy-by-design should be incorporated into AI systems from the beginning. This means privacy safeguards should not be added only after harm occurs. Instead, systems should be designed to minimize data exposure,

protect anonymity where possible, secure databases, limit access, and provide explainable outputs. Studies on AI-related legal frameworks show that criminal liability and regulatory structures must respond to the distinctive features of AI systems (9). Privacy-by-design is one way to operationalize this response because it translates legal values into technical architecture. For example, a surveillance system may be designed to detect abandoned objects without identifying every person in a public space. A cyber prevention tool may analyze suspicious traffic patterns without exposing unnecessary personal content.

Another strategy is the creation of clear standards for explainability. AI systems used in crime prevention should be explainable enough for institutional users, oversight bodies, and affected individuals to understand the basis of significant decisions. Explainability is especially important when AI outputs lead to intervention, increased surveillance, or restriction of access. Research on the application of AI in criminal policy and criminal procedure shows that AI can influence legal processes and therefore requires careful procedural safeguards (7). Explainability does not require every algorithm to be simple, but it does require that decisions based on AI are not treated as unquestionable. Institutions must be able to explain why a preventive action was taken and what role AI played in it.

The right to challenge AI-based decisions should also be recognized. If a person is misidentified by facial recognition, wrongly classified as suspicious, or subjected to repeated preventive intervention due to algorithmic error, there must be a meaningful pathway for correction. Fair-trial research in AI-based criminal justice emphasizes the importance of procedural rights when AI affects legal outcomes (6). In situational prevention, similar logic applies even if the person has not been formally charged. Preventive measures can still affect rights. Therefore, complaint procedures, review mechanisms, and access to remedies are necessary components of legitimate AI governance.

Regulation must also address the procurement and deployment of AI by public institutions. Governments should not adopt AI tools simply because they are technologically advanced or commercially attractive. They should require evidence of accuracy, rights compliance, security, and suitability for the intended preventive purpose. Research on AI and criminal justice policymaking in Iran highlights the importance of managing both opportunities and challenges for judicial officers (15). This implies that public institutions need technical literacy, legal awareness, and ethical capacity before adopting AI. Procurement contracts should include audit rights, data protection obligations, transparency requirements, and liability clauses.

In addition, regulatory frameworks must consider the role of private actors. Many AI crime prevention tools are developed, owned, or operated by private companies. This creates risks related to trade secrecy, profit incentives, data commercialization, and limited public accountability. Research on special features of criminal liability concerning AI indicates that AI requires legal treatment attentive to its distinctive operational structure (18). In preventive contexts, this means that private vendors should not be allowed to evade responsibility by presenting themselves as neutral technology providers. If their systems process personal data or influence security decisions, they must be subject to legal obligations and oversight.

Education and professional training are also necessary. Law enforcement officers, judges, prosecutors, policymakers, and administrators must understand both the capabilities and limitations of AI. Overconfidence in AI may lead to automation bias, where human decision-makers accept algorithmic outputs without sufficient scrutiny. Underconfidence may lead to rejection of useful tools that could prevent harm. Studies on criminal psychology and AI show that risk factors and implications must be carefully interpreted rather than mechanically applied (13).

Training should therefore emphasize critical use, legal standards, bias detection, privacy protection, and human responsibility.

A balanced model of AI-based situational crime prevention should also distinguish between different levels of risk. Low-risk AI tools, such as systems that detect technical anomalies without identifying individuals, may require lighter regulation. High-risk tools, such as biometric identification, predictive policing, automated suspicion scoring, or systems that trigger police intervention, require stricter controls. Research on criminal liability and AI errors shows that risk increases when AI outputs can cause serious legal or personal harm (8). A risk-based approach allows regulation to be flexible without being permissive. It encourages innovation where risks are manageable while imposing strict safeguards where rights are vulnerable.

Finally, AI governance in situational crime prevention should be grounded in a rights-based understanding of security. Security is not the opposite of privacy; both are conditions of human dignity and social order. Crime prevention loses legitimacy if it destroys the rights it claims to protect. Studies on the feasibility of criminal liability for AI based on philosophical foundations suggest that law must confront deeper questions about agency, responsibility, and the moral status of AI-related actions (11). In a similar way, privacy regulation must confront deeper questions about the kind of society created by preventive technologies. The proper goal is not to reject AI but to embed it within legal structures that preserve liberty, equality, accountability, and public trust.

Conclusion

Artificial intelligence has become one of the most important technological developments affecting contemporary crime prevention. Its relevance to situational crime prevention is especially strong because both AI and situational prevention are oriented toward anticipation, risk reduction, opportunity control, and practical intervention. AI can strengthen situational prevention by identifying crime patterns, supporting predictive analysis, improving surveillance capacity, detecting cyber threats, assisting resource allocation, and accelerating institutional response. These capacities make AI a powerful tool for modern security governance, especially in environments where crime is complex, data-intensive, rapidly changing, and difficult to prevent through traditional methods alone.

However, the preventive value of artificial intelligence cannot be evaluated only in terms of efficiency. A crime prevention system may be technically effective but legally and ethically unacceptable if it violates privacy, normalizes excessive surveillance, reproduces discrimination, or weakens accountability. The central challenge is therefore not whether AI can assist situational crime prevention, but under what conditions its use can be considered legitimate. AI-based prevention becomes problematic when it treats individuals as permanent objects of suspicion, collects excessive personal data, relies on opaque algorithms, or allows automated predictions to replace human judgment.

Privacy is the most important limiting principle in this field because AI-based crime prevention depends heavily on data. The more extensive the data collection, the greater the risk of intrusion into private life. Preventive systems may collect biometric information, location data, behavioral patterns, online activity, financial records, and environmental surveillance footage. Even when these systems are introduced for legitimate security purposes, they may create risks of function creep, unauthorized reuse, data breaches, wrongful identification, and discriminatory classification. Therefore, privacy protection must not be treated as an obstacle to prevention; it must be treated as a condition for legitimate prevention.

The use of AI in situational crime prevention also requires careful attention to responsibility. When AI systems produce errors, cause harm, or contribute to rights violations, legal systems must be able to identify responsible actors and provide effective remedies. Responsibility cannot disappear simply because a decision was technologically mediated. Developers, operators, public institutions, private vendors, and human decision-makers must all remain within a clear framework of accountability. Without such accountability, AI-based prevention may create a dangerous gap between technological power and legal responsibility.

A balanced approach requires legality, necessity, proportionality, transparency, explainability, human oversight, data minimization, purpose limitation, independent auditing, and meaningful remedies. These principles should not remain abstract. They must be translated into institutional procedures, technical design requirements, procurement standards, professional training, and enforceable legal duties. AI systems used in crime prevention should be evaluated before deployment, monitored during use, and corrected or withdrawn when they produce unjustified harms. High-risk applications such as facial recognition, biometric databases, predictive policing, and automated suspicion scoring require particularly strict safeguards.

The future of AI in situational crime prevention depends on whether societies can develop a model of technological governance that protects both security and liberty. If AI is used responsibly, it can help prevent crime, reduce harm, improve institutional effectiveness, and support more informed decision-making. If it is used without sufficient safeguards, it may expand surveillance, intensify inequality, and undermine public trust in criminal justice institutions. The proper path is neither unconditional acceptance nor total rejection of AI, but critical, rights-based, and accountable integration.

In conclusion, artificial intelligence should be understood as a supportive instrument for situational crime prevention, not as an autonomous substitute for legal judgment, ethical reasoning, or human responsibility. Its preventive power must be limited by privacy, dignity, equality, and the rule of law. A legitimate AI-based prevention system is one that reduces criminal opportunities while also preserving the fundamental rights of the individuals and communities it is designed to protect.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Ehsanpour SR. The Importance and Position of Artificial Intelligence in Crime Prevention. Applied Criminology Research. 2025;3(4):59-80.
2. Najafi, Mousavifar. A Reflection on the Trend of Artificial Intelligence in Crime Prevention. Quarterly Journal of Legal Civilization. 2025;8(23):e218735.
3. Kaveh MH, Barani M. Using Artificial Intelligence to Combat Computer Crimes and Improve Cybersecurity Performance. Comparative Criminal Jurisprudence Quarterly. 2025;5(1).
4. Chen Q. Improving the trial efficiency of criminal cases with the assistance of artificial intelligence. Discov Artif Intell. 2025;5(110):1-14. doi: 10.1007/s44163-025-00353-2.
5. Wang X, Wu YC, Ji X, Fu H. Algorithmic Discrimination: Examining Its Types and Regulatory Measures With Emphasis on US Legal Practices. Frontiers in Artificial Intelligence. 2024;7. doi: 10.3389/frai.2024.1320277.
6. Trang NTT, Linh NH, Hoang NTC, Kiet PVT, Loan LTN, Phuc NTH. Right to a Fair-Trial When Applying Artificial Intelligence in Criminal Justice - Lessons and Experiences for Vietnam. Journal of Law and Sustainable Development. 2024;12(3):e601. doi: 10.55908/sdgs.v12i3.601.
7. Miri S. Application of Artificial Intelligence in Criminal Policy and Criminal Procedure. Tehran: Manzoumeh Kherad Pajouhan; 2025.
8. Al-Jamili OHJ. Criminal Liability Arising from Artificial Intelligence Errors. Egypt: Dar Misr for Printing and Publishing; 2025.
9. Al-Halahlah AKF. Artificial intelligence and crime: Legal frameworks of criminal liability in the digital era. 2025.
10. Rostami Zabol B, editor Criminal liability arising from the actions of autonomous Artificial Intelligence in the Iranian criminal legal system: Challenges and legislative necessities. 14th International and National Conference on Management, Accounting, and Law Studies; 2025; Tehran.
11. Zandi M, Rafiei Alavi SE. Feasibility of criminal liability in Artificial Intelligence based on its philosophical foundations. Philosophy of Law. 2024;3(1).
12. Teresia JNW. Criminology and Social Impact in the Age of Artificial Intelligence [AI]. East African Journal of Information Technology. 2024;7(1):221-39. doi: 10.37284/eajit.7.1.2141.
13. Sung Y-E. Criminal Psychology and Artificial Intelligence (AI): Risk Factors and Implications. Korea Assoc Crim Psychol. 2024;20(4):105-30. doi: 10.25277/kcpr.2024.20.4.105.
14. Talukder KA, Shompa TF. Artificial Intelligence in Criminal Justice Management: A Systematic Literature Review. NHJ. 2024;1(01):63-82. doi: 10.70008/jmldeds.v1i01.42.
15. Amirian Farsani A. Artificial Intelligence and Criminal Justice Policymaking in Contemporary Iran: New Opportunities and Challenges for Judicial Officers. Quarterly Journal of Contemporary Political and Social Changes of Iran. 2025. doi: 10.30510/pscci.2025.450070.1037.
16. Mirshekarloo K, Yasin, Ghiyasi J. Attributing liability to Artificial Intelligence with emphasis on the causal relationship in cybercrimes. Judicial Precedent. 2025;1(1).
17. Ghavamipour Sereshkeh M, Mahmoudi A. An Introduction to the Legal Frameworks of Criminal Liability for Artificial Intelligence Systems. Modern Technologies Law. 2025;6(11):209-32. doi: 10.22133/mtlj.2024.449703.1314.
18. Younes YZK. Special features of criminal liability concerning artificial intelligence. Iraqi Journal. 2024;68.