




# Application of Artificial Intelligence in Security-Oriented Criminal Policy: Opportunities and Challenges

1. Seyedeh Monira Hejazi : Department of Criminal Law and Criminology, Ta.c., Islamic Azad University, Tabriz, Iran

2. Baharak Shahed \*: Department of Criminal Law and Criminology, Ur.c., Islamic Azad University, Urumiyeh, Iran

3. Jamal Beigi : Department of Criminal Law and Criminology, Ma.c., Islamic Azad University, Maragheh, Iran

4. Keyvan Heidarnejad : Department of Criminal Law and Criminology, Sha.c., Islamic Azad University, Shabestar, Iran

\*Correspondence: baharakshahed@iau.ac.ir

## Abstract

Artificial intelligence (AI), as one of the outcomes of information and communication technologies, has led to remarkable transformations in all aspects of human life, particularly in public policymaking. Criminal justice institutions have shown a strong interest in using AI capabilities in security-oriented criminal policies, including crime prediction, sentencing, recidivism prevention, and risk management. Accordingly, the present study aims to analyze the opportunities and challenges associated with the application of AI in security-oriented criminal policy. The research follows a qualitative approach, seeking to comprehensively examine the study subject through a descriptive–analytical method and by using library resources relevant to the topic. The findings indicate that although AI can serve as an efficient tool in support of criminal policy, in the absence of clear legal frameworks, human oversight, and mechanisms ensuring justice, there is an increased risk of excessive securitization of criminal policy and the erosion of fundamental citizens' rights. Therefore, achieving legitimate and fair use of AI requires balancing technological efficiency with the principles of criminal justice.

**Keywords:** artificial intelligence, security-oriented criminal policy, crime prediction, proactive prevention

Received: 01 July 2025

Revised: 25 September 2025

Accepted: 02 December 2025

Initial Publish: 04 October 2025

Final Publish: 13 December 2025



**Copyright:** © 2025 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

**Citation:** Hejazi, S. M., Shahed, B., Beigi, J., & Heidarnejad, K. (2025). Application of Artificial Intelligence in Security-Oriented Criminal Policy: Opportunities and Challenges. *Legal Studies in Digital Age*, 4(4), 1-10.

## 1. Introduction

In recent decades, law enforcement agencies worldwide have faced complex challenges, including the exponential growth of data produced by digital devices and online services, the increasingly sophisticated nature of modern criminal activity, the globalization of crime, cyber threats, trafficking, and international terrorism. It is evident that traditional criminal policy methods alone are insufficient to respond effectively. Therefore, advanced and innovative initiatives are needed more than ever before. The global development of information and communication technologies has profoundly transformed the economic,

social, cultural, and political dimensions of human life, with the electronic revolution representing a decisive phenomenon of the contemporary era (Khalilpour, 2020). Artificial intelligence (AI), as one of the products of this technological revolution, has experienced significant progress over the past decade, and its role and importance in society are expected to increase steadily. As one of the most advanced technologies of our time, AI can play a vital role in improving criminal policy and public security. With its unique capabilities in processing and analyzing data, identifying patterns, and predicting future events, AI can help criminal justice agencies respond to threats with greater precision and speed. Studies indicate that by leveraging its broad analytical capacities and rapid information processing, AI can substantially contribute to public security through six key functions: more accurate and faster decision-making, improved monitoring and surveillance, proactive crisis management, more effective communication coordination, better resource allocation, and process automation (Nazemnejad, 2024).

The growing volume and diversity of data collected by law enforcement organizations—such as police contact data, criminal records, surveillance footage, and urban data—alongside the need to control costs, increase efficiency, and better predict crime occurrence, have driven governments toward data-driven solutions. Predictive tools such as crime hot-spot mapping, risk assessment of repeat offenders, and facial recognition algorithms have gained a prominent place in criminal policies (Brayne, 2017; Richardson et al., 2019; Situmeang et al., 2024). Consequently, criminal justice institutions show great interest in adopting AI-based capabilities for security-oriented criminal policy, where the use of these tools is primarily aimed at risk management.

Numerous studies have supported the role of AI in combating and addressing crimes (Chen, 2025; Ehsanpour, 2025; Jalali, 2024; Mohammadinia & Alizadeh, 2023). However, several structural, technical, legal, social, and practical limitations hinder the automatic realization of these benefits. First, the quality and quantity of data are often insufficient, fragmented, and affected by historical and operational biases. Case studies show that data derived from discriminatory policies and practices can easily be fed into predictive models, amplifying bias through feedback loops (Richardson et al., 2019). Second, many AI algorithms and products lack the transparency required for evaluation, auditing, or legal defense; this undermines the right to a fair trial and the accountability of public institutions (Europol, 2023). Third, technical and institutional challenges—such as the absence of standardized data protocols, fragmented infrastructures, high maintenance costs, and the shortage of skilled personnel—limit the effective and sustainable application of these technologies. Finally, legal and social concerns, including privacy violations, the risk of pervasive surveillance, and declining public trust, exert significant pressure on the responsible adoption of AI tools in criminal policy (Takemura, 2021).

Despite these challenges, the opportunities presented by AI cannot be overlooked. Accordingly, the present research aims to identify and analyze the opportunities and challenges of applying AI in security-oriented criminal policy and to propose strategies to balance these two dimensions, ensuring responsible and just implementation. The central question of this study is: What are the opportunities and challenges of using AI in security-oriented criminal policy?

## 2. Research Background

In recent years, with remarkable advances in AI, numerous studies have explored its applications in criminal policy, crime prevention, and the justice system. These studies have largely focused on the opportunities for crime prediction and prevention while simultaneously addressing potential ethical, legal, and bias-related concerns.

Abuzari (2024), in a study titled *Combating Delinquency in the Age of Artificial Intelligence: Prediction as Prevention*, examined the contributions of AI to criminal investigations and its effectiveness in combating delinquency. The research concluded that using AI to fight crime is well-justified within risk management frameworks in both criminal and non-criminal domains, aligning with risk-oriented criminal policy that seeks not to identify “born criminals” but to shape environments and situations that minimize the likelihood of crime (Abuzari, 2024).

Ehsanpour (2025), in the article *The Importance and Position of Artificial Intelligence in Crime Prevention*, emphasizes that preventive policing involves using AI data and algorithms to predict the time, place, and type of potential crimes. Facial recognition technology, combined with AI and data analytics, assists law enforcement and security agencies in quickly identifying crimes and offenders, thus preventing crime or facilitating rapid arrests. In cybersecurity, AI has become indispensable by offering capabilities such as intrusion detection, attack prediction, malware identification, user behavior

analysis, and automatic threat response. However, alongside these undeniable advantages, legal and ethical challenges—such as potential violations of citizens' privacy and system biases—must be properly addressed and managed (Ehsanpour, 2025).

Chen (2025), in the study *Improving the Trial Efficiency of Criminal Cases with the Assistance of Artificial Intelligence*, investigated how AI improves the efficiency of criminal trials. Findings indicated that AI-driven proceedings reduced average trial duration by 40% and errors by 55% compared to traditional methods. While AI can significantly enhance judicial efficiency, challenges related to its implementation, scalability, and bias mitigation remain (Chen, 2025).

Situmeang and colleagues (2024), in *The Role of Artificial Intelligence in Criminal Justice*, explored the transformative impact of AI on the justice system. Key findings show that AI can significantly improve crime prediction and prevention, assist in evidence analysis, and support decision-making processes. Predictive policing models using AI can identify potential crime locations and allocate resources more efficiently, while AI-based tools help analyze large volumes of legal documents and evidence. Nonetheless, concerns regarding bias, fairness, transparency, and ethical implications highlight the urgent need for legal frameworks that ensure transparent, accountable, and ethically aligned use of AI (Situmeang et al., 2024).

Takemura (2021), in the article *AI-Algorithm-Big Data, Predictive Criminal Justice and Hyper Crime/Social Control: Surveillance Capitalism after "Singularity" and Prospects of Informational Civilization*, shows that law enforcement organizations worldwide are exploring and adopting AI and robotics to enhance crime prevention and control, though the level of technological maturity and engagement varies among nations. Takemura warns that the general trend of AI applications is toward strengthening surveillance capacity, which poses a serious threat to fundamental rights and privacy. Without safeguards of justice, accountability, and transparency, unregulated AI deployment risks eroding public trust in law enforcement (Takemura, 2021).

Richardson and colleagues (2019), in *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, reveal that law enforcement agencies increasingly rely on predictive policing systems to forecast criminal activity and allocate resources. However, in many jurisdictions, these systems are built on flawed, racially biased, and sometimes illegal practices. Implementing predictive policing in such environments heightens the risk of perpetuating harm through feedback loops across the justice system. Therefore, predictive policing should be approached with caution, supported by mechanisms to audit, evaluate, and challenge the underlying data (Richardson et al., 2019).

Overall, the research background underscores AI's significant potential in improving prevention, prediction, and the efficiency of the justice system while repeatedly highlighting challenges such as bias, privacy violations, and ethical dilemmas. However, this study goes further by specifically focusing on **security-oriented criminal policy** to examine AI's opportunities and challenges and propose strategies for balancing legal-ethical risks with technological benefits.

### 3. Concepts and Theoretical Foundations

#### 3.1. Artificial Intelligence (AI)

The difficulty in defining artificial intelligence lies not in the concept of "artificial" but in the ambiguity of "intelligence," since humans are the only known beings recognized as possessing intelligence. It is striking that the meaning of intelligence is strongly tied to human characteristics. John McCarthy, a leading pioneer of AI who widely defined the term, believed there is no single, universally accepted definition of artificial intelligence (Salari, 2021). During World War II in the 1940s, the British mathematician Alan Turing built a decoding device called the Bombe to break the Enigma code used by the German army. Following this success, Turing wrote the influential paper *Computing Machinery and Intelligence* in the 1950s, significantly shaping the field of AI (Dashti & Mo'tamadnejad, 2024). AI is broadly understood as the study of how to use computational models resembling the human mind (Ebrahimi, 2022). Practically, it refers to a system's ability to interpret data it receives and use it to achieve specific goals (Soufi & Salehnejad Bahrestaghi, 2023). AI covers areas such as decision-making, learning, reasoning, pattern recognition, natural language processing, and machine vision (Chen, 2025; Soufi & Salehnejad Bahrestaghi, 2023).

AI is generally divided into two main categories: *weak AI*, designed to perform specific tasks, and *strong AI*, aimed at achieving general intelligence comparable to humans. Strong AI itself includes machine learning and deep learning

(Nazemnejad, 2024). Machine learning allows systems to learn from data without explicit programming. These algorithms are trained on large and complex datasets to recognize patterns and detect potential threats, commonly applied in malware detection and anomaly identification (Mahmoudi & Bahr Kazemi, 2024). Deep learning, a subfield of machine learning, uses multi-layered neural networks to learn complex relationships between inputs and outputs. It can process diverse data types—including text, images, video, speech, and audio—with less human-provided preprocessing and often achieves higher accuracy than traditional machine learning approaches (Tarseli, 2023).

### 3.2. Security-Oriented Criminal Policy

Criminal policy is the set of strategies by which a society organizes responses to criminal phenomena. It may be likened to a circle with criminal law at its core, surrounded by other interdisciplinary fields. Its purpose is to guarantee human security, enhance the rights of victims and offenders, and preserve social order. Consequently, it must employ both proactive and reactive measures to address those who violate laws and social norms (Marty, 2019).

The concept of “security” has expanded over time. While historically associated with personal and political safety, it now encompasses economic, social, cultural, occupational, and informational security. With this expansion, a security-centered discourse has emerged in society, and citizens often support governments advocating such strategies to reduce crime and fear (Mir Mohammadsadeghi & Soltani Ranani, 2023). In *maximalist* models of criminal policy, influenced by totalitarian ideologies, the aim is absolute citizen security and political stability. Under such systems, the distinction between crime and deviance blurs, personal freedoms vanish under pervasive state surveillance, and due process rights for suspects and defendants are undermined. Conversely, *minimalist* criminal policy models, inspired by liberty-oriented approaches, safeguard personal freedoms by distinguishing between crime and deviance, limiting state intervention to criminal conduct, and ensuring fair trial principles (Soltani Mofrad, 2021).

With the decline of rehabilitative and corrective approaches, modern criminology has shifted toward protecting potential victims and society by excluding high-risk and dangerous offenders to prevent recidivism. Crime control perspectives now view offenders as active agents making rational choices based on cost-benefit calculations (Mahdavi pour & Shahrani Karani, 2014). This shift, alongside the rise of new forms of criminality such as terrorism, has led criminal policy and criminal law to adopt stricter security-focused frameworks, reduce procedural guarantees, and prioritize public order (Majidi & Tajabadi, 2019). Security-oriented criminal policy aims to suppress and marginalize criminal or deviant acts, imposing maximum control over offenders and dangerous groups. It emphasizes concepts like “dangerous state,” preventive measures, and crime warfare while pushing society toward greater policing (Najafi Abrandabadi, 2012). While such a model protects public order and safety, it also raises concerns regarding human rights and individual liberties.

## 4. Research Method

Given the nature of the topic, this study is based on library research using credible academic and legal sources. The collected information was analyzed through a descriptive–analytical approach to provide an in-depth understanding of the subject.

## 5. Opportunities for Applying Artificial Intelligence in Security-Oriented Criminal Policy

### 5.1. Big-Data Analytics and the Discovery of Hidden Patterns

The rise of security-oriented criminal policy—accompanied by a renewed turn toward retribution in response to new forms of criminality, especially terrorism and organized crime—has driven intensified surveillance and the adoption of security- and suppression-focused measures in modern societies. Surveillance entails the collection, recording, and classification of information about processes and institutions; and, historically, the emergence of surveillance societies is not new, stretching at least to the sixteenth century with the rise of nation-states and continuing through the rationalization of criminology and risk management in the nineteenth and twentieth centuries (Brayne, 2017). Building on criminological perspectives such as social and legal control, AI can function as an intelligent tool for assessing criminal behavior (Ghorbani & Ehteshami, 2025). In

criminal investigations, data mining and intelligent crime analysis typically pivot on three sets of variables: spatio-temporal features (time and place coordinates of the offense), behavioral features (e.g., crime-scene characteristics and offender *modus operandi*), and offender characteristics (e.g., age, race, sex). Geographic investigation systems employ standard crime-mapping techniques and, using past crime locations and complex mathematical algorithms, estimate an offender's probable residence in specific areas; some applications also provide alerting and geo-display systems that notify of incidents, victim locations, and risk statuses (Abuzari, 2021; Mohammadinia & Alizadeh, 2023; Tarseli, 2023). Criminologists note that offenders often adopt temporal-spatial routines that have "worked" for them over time, minimizing risk—thereby creating predictability. Consequently, the focus of criminal justice can shift from what has happened to what will likely happen, enabling more effective deployment of resources against anticipated crime patterns (Jalali, 2024; Situmeang et al., 2024). Recent initiatives—for example in Los Angeles—seek to identify crime locations using big data, a move that prioritizes mass surveillance and forward-looking resource allocation over purely reactive responses (Brayne, 2017; Takemura, 2021). Police agencies such as Vancouver's have experimented with AI approaches including boosted decision-tree regression and k-nearest neighbors to forecast future crime risk; more broadly, AI's capacity to ingest and analyze large, heterogeneous datasets yields pattern discovery and operational insights that can strengthen prevention and response (Jalali, 2024; Situmeang et al., 2024).

### 5.2. *Proactive Policing and Crime Prediction*

In the 1970s, the dominant state model for maintaining order and security relied on patrol-centric, reactive policing (random patrols, rapid response to citizen calls, and post-incident investigations). Researchers gradually recognized that these methods had limited impact on crime reduction, prompting a shift toward preventive, evidence-based strategies. In 1994, New York City implemented the CompStat management system linking crime data with police activity, which quickly spread to other cities, including Los Angeles in 2002. Following the September 11, 2001 attacks in the United States, intelligence-led policing expanded as the federal government funded local police to collect, analyze, and share extensive datasets (Brayne, 2017). Broadly defined, predictive policing encompasses any system that analyzes existing data to forecast where crime is likely to occur within a given time window or to identify who is likely to be a victim or perpetrator. It represents the latest data-driven analytic technique offered to law enforcement agencies (Richardson et al., 2019). Since the mid-twentieth century, responses to crime—first in the Americas and Europe and then globally—have increasingly reflected security-oriented criminology, with concentrated controls focused on groups perceived as crime-prone, repeatedly victimized, or situated in high-risk contexts. Within such frameworks, prediction and prevention pivot on reducing opportunities and situational vectors for offending, with monitoring of behaviors and movements serving as core tools (Mahdavi pour & Shahrani Karani, 2014; Meybodi, 2021).

AI, as a new technology, can accelerate and sharpen data analysis to support evidence-based governance, improve state-citizen communication, and reduce human error in administrative processes. Accordingly, AI's link to security can be seen in resource optimization, evidence-informed policymaking, enhanced communication and coordination, and error reduction (Mahmoudi & Bahr Kazemi, 2024). In predictive policing, AI models can analyze historical crime data to identify at-risk individuals and places, enabling early, data-driven preventive measures; by increasing precision and speed in police operations, these systems can bolster public order while curbing costs (Nazemnejad, 2024). Feature sets often combine place-based variables (e.g., weather, location) with person-based variables (e.g., income, literacy), aiding hazard estimation and decision-making for specific areas. AI-enabled police systems can simulate recurrent crime patterns and forecast where and when certain offenses are likely to occur, helping officers arrive at the right place and time (Jalali, 2024; Situmeang et al., 2024). Illustratively—although implementations vary—the literature documents U.S. initiatives that used algorithmic lists to identify individuals at risk of involvement in gun violence (as victims or offenders) and systems that forecast near-term hot spots to guide patrol deployment (Jalali, 2024; Richardson et al., 2019). Beyond policing, countries such as Indonesia have applied AI-based monitoring within correctional settings to track inmate behavior, rapidly detect potential security threats, and enhance the safety of staff and prisoners (Situmeang et al., 2024). European research has also examined near-repeat modeling for burglary, where algorithms forecast short-horizon, small-radius risks following an initial incident, with reported gains in arrests and reductions in burglary rates in pilot cities (Abuzari, 2022; Jalali, 2024).



That said, algorithmic discrimination and disparate decision-making remain among the most serious legal challenges across intelligent, automated decision systems, particularly AI. For example, analyses of widely used risk-assessment tools have shown that socioeconomic factors can drive classifications and shape assessments of “dangerousness,” potentially resulting in fewer rights or harsher outcomes for socioeconomically disadvantaged individuals; other studies document systemic disparities against Black individuals, with inflated recidivism risk predictions that diverge from observed outcomes (Brayne, 2017; Kord Alivand, 2023; Richardson et al., 2019). These findings underscore the need for rigorous auditing, transparency, and accountability regimes to ensure that security-oriented AI enhances safety without compromising fundamental rights.

### 5.3. *Managing the Risk of Dangerous Offenders and Preventing Recidivism*

The concept of “risk” in the criminal justice system is closely linked to how different actors define and assess it. Thus, for the effective implementation of crime risk management strategies in individual and social domains, a clear and precise definition of risk is essential. Each sector is responsible for identifying its own risk factors, and immediate criminal policy decisions must be grounded in these assessments. In other words, both proactive and reactive responses within criminal justice systems—and the operational strategies of its actors—should be organized based on structured risk evaluations (Ghorbani & Ehteshami, 2025).

Crime risk management theory emerged as criminology shifted away from rehabilitative and causal approaches toward statistical or actuarial justice and situational crime prevention. Originating in the 1990s in Anglo-Saxon countries and inspired by risk theories in insurance, this approach categorizes offenders by their level of danger. The division of offenders into high- and low-risk groups informs strict post-sentence supervision, long-term monitoring, and intensified control for high-risk individuals (Abuzari, 2024; Ghorbani & Ehteshami, 2025). Thus, even after serving their sentences, offenders may remain under supervision for limited or indefinite periods to prevent reoffending (Abuzari, 2024).

Preventing recidivism remains one of the most pressing challenges for criminal justice systems. AI, by analyzing criminological data and using predictive modeling, offers new tools to reduce reoffending rates. Examination of AI software integrated into criminal adjudication shows that the economic and social status of defendants significantly influences risk assessments. This underscores the concerns of bias and uncertainty not only in algorithmic use but also across the justice system as a whole (Ebrahimi, 2022; Kord Alivand, 2023).

In common law systems such as the United States, risk level assessments—low, medium, and high—have long informed judges when determining sentences and correctional measures. Offenders deemed low risk for reoffending may receive short custodial sentences or alternatives to imprisonment, while high-risk individuals are often sentenced to long-term incarceration in closed environments. The introduction of risk assessment algorithms aimed to support judicial discretion in these determinations and has expanded over time (Ebrahimi, 2022). For instance, AI tools help decide whether an offender is eligible for parole and can assist correctional authorities in implementing noncustodial measures. Predictive modeling of offenders’ behavior enhances the use of probation, parole, and bail conditions based on individual dangerousness levels (Abuzari, 2024).

In the United Kingdom, Cambridge University developed the Harm Assessment Risk Tool (HART), tested by police since 2007. HART used archived crime data (2008–2012) to predict the likelihood of suspects reoffending, classifying them as low, medium, or high risk. The system considered about 30 variables, some indirectly related to crime (such as age or address), comparing these with suspect profiles to guide decisions on extending detention or release. However, the technology faced criticism for privileging security over fundamental rights and tending to classify individuals as high risk disproportionately (Ebrahimi, 2022; Kord Alivand, 2023).

### 5.4. *Video Surveillance, Audio Monitoring, and Facial Recognition Systems*

Video surveillance, widely deployed in recent decades, is one of the most prominent methods of monitoring and control in social environments. Today, cameras are installed across public and private spaces, often integrated with alert systems to rapidly identify suspects through facial recognition. These cameras act as proxies for security and order-maintaining authorities and have become an essential preventive technology, though their effectiveness depends on specific conditions (Cousen, 2005).

For example, according to the French Banking Association, 90% of banks have cameras at entry and exit points and both inside and outside their facilities to automatically record and transmit suspicious incidents. Cities worldwide use this technology to enhance neighborhood security and public safety. Some states have integrated video monitoring into crime suppression strategies by installing high-rise surveillance cameras to track suspicious individuals or offenders. China operates more than 172 million surveillance cameras under the “Skynet” system, credited with reducing petty crime in major cities by about 20% (Ehsanpour, 2025). The United Kingdom also employs such technologies to control high-risk areas.

Recently, satellite technology has gained a preventive dimension: global positioning systems originally launched by the United States are now leveraged for detecting and combating crimes such as human trafficking, vehicle theft, and energy smuggling (Ehsanpour, 2025). In the U.S., police agencies film public squares and streets to monitor urban life extensively, while France’s social security protection program since 2007 has required schools to install audio and video equipment to monitor student interactions and identify harmful behaviors early. Such measures reflect a securitized criminal policy, where surveillance becomes deeply embedded in daily life, enabling wide-ranging recording, intervention, and even intrusion into private spheres.

Facial recognition technology—a key AI-based tool—is particularly valuable for identifying and tracking suspects. By analyzing images and videos, AI can match individuals to databases, accelerating arrests and investigations. However, its use raises critical privacy concerns and the risk of false positives. Moreover, lower accuracy across certain demographic groups increases the likelihood of ethnic or racial bias in outcomes (Brayne, 2017; Kord Alivand, 2023; Richardson et al., 2019). These issues highlight the need for clear regulatory frameworks, accuracy benchmarks, and strong oversight to ensure that the pursuit of security does not compromise fundamental rights.

## 6. Challenges of Utilizing Artificial Intelligence in Security-Oriented Criminal Policy

### 6.1. *Data-Related Challenges and the Risk of “Dirty Data”*

“Dirty data” refers to missing, inaccurate, manipulated, or inconsistently represented datasets. In policing, such data often arise from corrupt, biased, or unlawful practices that distort criminal records. Intentional manipulation for political or public relations goals—such as inflating or suppressing crime statistics to influence budgets, policies, or perceptions—is one common example. Additionally, false reports and inaccurate citizen calls can further distort official records and propagate systemic errors (Richardson et al., 2019).

Although intelligent machines are often described as objective and consistent, AI systems can carry unconscious biases inherited from their creators. Bias can occur before data collection, during dataset curation, or throughout the machine learning process, since collected data often reflect societal inequalities and discrimination. Socially, bias means unfair predisposition toward or against individuals or groups, while in criminology, algorithmic bias manifests as unfair or discriminatory outcomes for certain racial, gender, economic, or geographic groups (Seifi & Razmkhah, 2021).

Algorithmic discrimination and biased decision-making are among the most serious legal issues across intelligent, automated systems, particularly AI-driven justice applications. Systems trained on flawed data struggle to identify and filter out “bad data,” especially when the data-generation processes themselves are suspect (Richardson et al., 2019). For example, the COMPAS risk assessment tool has been shown to assign higher danger scores to Black defendants than to white defendants with similar records. Likewise, economic bias appears when algorithms label impoverished neighborhoods as high-crime areas; gender bias occurs when systems assume women are less likely to reoffend; and geographic bias emerges when algorithms monitor only certain zones of a city (Kord Alivand, 2023).

Such algorithmic inequities can be especially impactful in security-driven criminal policies, potentially transforming societies into highly disciplinary and controlled environments. In contexts like the United States and the United Kingdom, existing crime-control mechanisms have historically led to disproportionate contact between police and marginalized youth or minority communities, regardless of actual dangerousness. When AI is built on these same biased records, it can amplify and automate injustice (Abuzari, 2021). After legislation such as the U.S. Patriot Act, intensified monitoring of migrants—including phone tapping and facial registration—illustrated how biased enforcement can expand under security rationales.

Introducing AI trained on these skewed patterns risks classifying some groups as highly dangerous and others as almost harmless, regardless of reality (Abuzari, 2021).

## 6.2. *Infringement on Individual and Public Freedoms*

Humans are inherently free, and no limitation is permissible except where one's freedom infringes on others' rights. Any unlawful interference with personal liberty is legally actionable, as recognized in Islamic Penal Code provisions protecting against unauthorized restriction (Hakim & Ebrahimian, 2023). AI, however, enables unprecedented behavioral prediction and control, potentially allowing authorities to monitor, anticipate, and shape individual actions without transparent legal safeguards.

One of the greatest concerns for citizens is preserving privacy and autonomy. AI systems often require extensive personal data and can reconstruct behavioral profiles beyond human comprehension. The tension between privacy and AI is profound: while individuals expect their personal information to be shielded from unauthorized government or private access, AI-driven systems collect, aggregate, and interpret these data. In criminal justice, this may empower fully automated decision-making where algorithms—rather than human judges—determine levels of risk and intervention (Takemura, 2021).

Predictive policing can classify individuals as high-risk offenders or potential victims, placing them under intensive security measures, even without confirmed criminal involvement. Without strict oversight, data-quality standards, and transparency protocols, non-offenders risk being misclassified and subjected to surveillance and control (Europol, 2023).

Moreover, governments equipped with AI-based crime control systems may access personal and financial transactions or monitor social media activity in the name of prevention and security. In authoritarian contexts, such capabilities can become widespread and deeply invasive (Mahmoudi & Bahr Kazemi, 2024). Mass camera networks and facial recognition tools already push societies toward disciplinary models where abnormal or suspicious behaviors—online and offline—are flagged and acted upon. While these measures can strengthen safety, they also risk eroding fundamental human rights and freedoms if unchecked.

In short, the tension between technological efficiency and civil liberties becomes acute when security imperatives dominate criminal policy. AI-driven surveillance can deter crime but also threaten privacy, autonomy, and equality, underscoring the urgent need for legal frameworks ensuring accountability, proportionality, and human rights protection.

## 7. Conclusion

This study provided a comparative and analytical examination of the role of artificial intelligence in security-oriented criminal policy. It shows that this advanced and powerful technology has created significant transformations in recent decades, including in the identification of offenders, crime prediction, crime control, and sentencing. By employing complex algorithms and analyzing big data, artificial intelligence enables the detection of criminal patterns and supports risk-based crime management.

However, the use of this technology within criminal law is not free of threats. New forms of crime may emerge within the very environment created by artificial intelligence, and cyberattacks can target infrastructures and sensitive information. In some instances, governments, depending on their adopted criminal policies, may impose restrictions that risk becoming discriminatory or disproportionately severe against certain social groups under security-driven approaches.

Therefore, applying artificial intelligence in security-oriented criminal policy must be done with caution and supported by clear legal frameworks and human oversight. Without these safeguards, an excessive focus on security can lead to over-securitization of criminal policy and the weakening of justice. Achieving legitimate and fair use of artificial intelligence requires a careful balance between technological innovation and the fundamental principles of criminal justice.

## 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

- Abuzari, M. (2021). Academic Chair on the Application of Artificial Intelligence in Crime Prevention. Danesh Shahr Legal Research Institute
- Abuzari, M. (2022). The Impact of Artificial Intelligence on the Quality of Criminal Investigations. *Journal of New Technology Law*, 6(3), 2-13.
- Abuzari, M. (2024). Combating Delinquency in the Age of Artificial Intelligence: Prediction as Prevention. *Bi-quarterly Journal of Research and Development in Criminal Law and Criminology*, 1(2), 37-67.
- Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, 82(5), 977-1008. <https://doi.org/10.1177/0003122417725865>
- Chen, Q. (2025). Improving the trial efficiency of criminal cases with the assistance of artificial intelligence. *Discov Artif Intell*, 5(110), 1-14. <https://doi.org/10.1007/s44163-025-00353-2>
- Cousen, M. (2005). *Video Surveillance: The Reasons for Success and Failure*.
- Dashti, T. S., & Mo'tamadnejad, R. (2024). The Position of Artificial Intelligence in European Union Legislation. *Journal of News Sciences*, 5-18.
- Ebrahimi, S. (2022). Preventing Recidivism through Artificial Intelligence: Requirements and Limitations. *Quarterly Journal of Criminal Law Teachings*, 19(23), 33-54.
- Ehsanpour, S. R. (2025). The Importance and Position of Artificial Intelligence in Crime Prevention. *Applied Criminology Research*, 3(4), 59-80.
- Europol. (2023). *The Second Quantum Revolution - The impact of quantum computing and quantum technologies on law enforcement*.
- Ghorbani, E., & Ehteshami, A. (2025). A Model for the Application of Artificial Intelligence in Developing Information Dominance to Counter New Psychoactive Substances in Cyberspace. *Quarterly Journal of NAJA Strategic Studies*, 10(1), 193-228.
- Hakim, S. M., & Ebrahimi, S. H. (2023). A Jurisprudential and Legal Study of the Deprivation of Citizen Security by Artificial Intelligence. *Quarterly Journal of Islamic Jurisprudence and Law Research*, 19(72), 74-101.
- Jalali, S. (2024). A Systematic Review of Applied Artificial Intelligence Techniques in Crime Prediction Using a Meta-Synthesis Method. *Quarterly Journal of Law Enforcement Order and Security*, 17(4), 127-164.
- Khalilpour, S. A. (2020). The Legislative Policy of Iranian Criminal Law with an Approach to Securing Cybersecurity for Children. *International Quarterly Journal of Qanoun Yar*, 325-338.
- Kord Alivand, R. (2023). A Comparative Study of the Application of Artificial Intelligence in Criminal Prosecution: Capacities and Challenges. *Quarterly Journal of Comparative Law Research*, 27(1), 81-104.
- Mahdavi, A., & Shahrani Karani, N. (2014). The Securitization of Criminology: Strategies and Its Effects on Criminal Law. *Journal of Criminal Law Research*, 5(1), 159-188.
- Mahmoudi, A. R., & Bahr Kazemi, M. (2024). Artificial Intelligence and its Impact on Cybersecurity and the Right to Privacy. *Quarterly Journal of Comparative Law Research*(3), 88-105.
- Majidi, S. M., & Tajabadi, F. (2019). Security-Oriented Criminalization Techniques in Iranian Criminal Law. *Journal of Islamic Jurisprudence and Law Studies*, 11(21), 289-316.
- Marty, D. (2019). *Great Criminal Policies*. Mizan Publishing.
- Meybodi, M. (2021). A Shift in the Orientation of Prevention based on Hardline Policies and Restrictive Human Rights Mechanisms in Security Criminology. *Journal of Medical Law, Special Issue on Legal Innovations*, 322-340.
- Mir Mohammadsadeghi, H., & Soltani Ranani, A. H. (2023). The Security-Oriented Approach of Iran's Criminal Policy towards Economic Crimes: Foundations and Instances. *Quarterly Journal of Economic and Commercial Law Research*(4), 11-41.
- Mohammadinia, O., & Alizadeh, A. (2023). The Role and Impact of Artificial Intelligence in the Process of Crime Detection. *Scientific Quarterly of the Detective*, 17(63), 85-104.
- Najafi Abrandabadi, A. M. (2012). From Critical Criminology to Security Criminology. (pp. 1-50)
- Nazemnejad, A. (2024). Smart Management and Oversight Using Artificial Intelligence: New Solutions for the Law Enforcement Force. *Quarterly Journal of Semnan Police Knowledge*, 14(51), 115-127.
- Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review*, 94(1), 192-233.
- Salari, S. (2021). *The Approach of Iranian and English Criminal Law to Liability Arising from Artificial Intelligence* Shahid Beheshti University].
- Seifi, A., & Razmkhah, N. (2021). Artificial Intelligence and the Challenges Ahead in the Realm of International Human Rights Law with an Approach to the Right to Work. *Bi-quarterly Journal of Human Rights*, 17(22), 55-74.
- Situmeang, S. M. T., Harliyanto, R., Zulkarnain, P. D., Nahdi, U., & Nugroho, T. (2024). The Role of Artificial Intelligence in Criminal Justice. *Global International Journal of Innovative Research*, 2(8). <https://doi.org/10.59613/global.v2i8.264>

- Soltani Mofrad, S. (2021). Criminal Justice in the Model of Comprehensive Authoritarian Formal Criminal Policy with an Emphasis on the Rights of the Accused in Preliminary Investigations. *Quarterly Journal of Iranian Sociology*, 4(2), 403-420.
- Soufi, S., & Salehnejad Bahrestaghi, S. (2023). The Impact of Artificial Intelligence on the Commission of Cybercrimes. *Journal of Legal Studies*, 11(51), 1-18.
- Takemura, N. (2021). AI-Algorithm-Big Data, Predictive Criminal Justice and Hyper Crime/Social Control: Surveillance Capitalism after 'Singularity' and Prospects of Informational Civilization. *International Journal for Crime, Justice and Social Democracy*, 10(3), 1-16.
- Tarseli, A. (2023). The Application of Artificial Intelligence in Improving Information Gathering and Analysis. *Scientific Quarterly of Interdisciplinary Strategic Knowledge Studies*, 14(56), 277-303.