


Artificial Intelligence and crime detection: A critical review

Karim Salehi¹, Simin Habib Zadeh Khiyaban^{2*}, Shoaib Sabbar³

1. Department of Law, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran.
2. Department of Public Administration, Faculty of Accounting and Management, Allameh Tabataba'i University, Tehran, Iran. (*Corresponding author: simin.habibzadeh1969@gmail.com,  <https://orcid.org/0009-0007-1707-8014>)
3. Department of International Commercial Law, Faculty of Law, Azad University, Tehran. Iran.

Article Info	Abstract
Original article	Background: Since the advent of modern policing, technological innovations in communication and information management have significantly shaped investigative practices and crime detection strategies.
Main Object: Law	Aims: The current research study explores the transformative role of Artificial Intelligence in modern crime detection and prevention across diverse domains including cybercrime, environmental crime, financial fraud, and urban surveillance.
Received: 13 September 2025	Methodology: Employing a qualitative meta-synthesis methodology, the research critically examines peer-reviewed literature published between the years 2015 and 2025 to identify emerging trends, technological innovations, and socio-legal implications associated with AI-driven policing.
Revised: 16 September 2025	Findings: The key findings highlight the integration of machine learning, computer vision, and natural language processing techniques into the predictive and real-time law enforcement systems. These technologies have demonstrably enhanced the accuracy, efficiency, and responsiveness of crime prevention strategies. However, the current study also reveals significant challenges, including algorithmic bias, lack of transparency, and inadequate regulatory oversight, particularly in socially stratified or underregulated contexts.
Accepted: 18 September 2025	Conclusion: The current article underscores the necessity of embedding explainability, accountability, and human oversight into Artificial Intelligence systems to ensure the ethical and equitable implementation of AI-driven policing systems.
Published online: 21 September 2025	
Keywords: algorithmic accountability, artificial intelligence, crime prevention, predictive policing, surveillance ethics.	

Cite this article: Salehi K, Habib Zadeh Khiyaban S, Sabbar S. (2026). "Artificial Intelligence and crime detection: A critical review". *Cyberspace Studies*. 10(1): 181-197. doi: <https://doi.org/10.22059/jcss.2025.402206.1179>.



Creative Commons Attribution-NonCommercial 4.0 International License
 Website: <https://jcss.ut.ac.ir/> | Email: jcss@ut.ac.ir |
 EISSN: 2588-5502
 Publisher: University of Tehran

1. Introduction

Since the advent of modern policing, technological innovations in communication and information management have significantly shaped investigative practices and crime detection strategies. The incorporation of the telegraph in the 19th century revolutionized inter-jurisdictional communication, enabling faster transmission of criminal intelligence and suspect descriptions. By the early 20th century, the adoption of two-way radios allowed real-time coordination between officers and dispatch centers, fundamentally altering the temporal dynamics of police response (Manning, 2008). These innovations laid the groundwork for the eventual digitization of law enforcement operations, including the implementation of databases for criminal records, forensic evidence management systems, and Geographic Information Systems (GIS) for spatial crime analysis. As policing institutions adapted to the increasing complexity of urban life and organized crime, digital communication tools became essential for evidence sharing, case management, and interagency collaboration. However, the rapid digitalization of society in the 21st century, coupled with the exponential growth of data generation, has far outpaced the capacity of conventional policing technologies to manage and interpret relevant information effectively.

This technological gap has become particularly salient in the context of new forms of crime that exploit the affordances of digital infrastructure. Cybercrime, financial fraud, environmental crime, and terrorism often operate through transnational networks that utilize encryption, anonymity tools, and digital currencies, thereby evading traditional investigative reach (Leukfeldt & Holt, 2020). Moreover, the increasing reliance on surveillance systems, body-worn cameras, and social media analysis has generated vast amounts of unstructured data that require rapid interpretation (Rahmatian & Sharajsharifi, 2022). Conventional investigative models—based on linear workflows, manual data analysis, and human pattern recognition—are insufficient in processing the velocity, volume, and variety of modern crime data. The reactive nature of many existing crime detection methods limits their utility in preemptive policing or in responding to rapidly evolving threats. As crime becomes more decentralized, adaptive, and technologically mediated, the necessity for advanced, automated, and intelligent systems to assist in crime detection becomes undeniable (Brantingham et al., 2018).

Artificial intelligence has emerged as a transformative force in this domain, offering new modes of automating and augmenting investigative processes. AI applications in policing include, but are not limited to, predictive analytics for identifying crime hotspots, facial and license plate recognition for suspect tracking, natural language processing for threat assessment on social media, and anomaly detection in surveillance video feeds (McCue, 2020). Through machine

learning algorithms trained on large-scale datasets, AI can uncover complex patterns and correlations that would be inaccessible to human analysts. These capabilities are particularly valuable in high-density urban areas, where real-time data integration and decision-making can mean the difference between prevention and escalation. Research has shown that AI-enhanced systems can significantly improve both the speed and accuracy of crime detection, contributing to more efficient resource allocation and targeted interventions (Babuta & Oswald, 2020). However, these advances are not without controversy. Concerns surrounding algorithmic opacity, racial and socioeconomic bias, data privacy, and the erosion of civil liberties have provoked debates about the legitimacy and governance of AI in policing. These challenges necessitate a critical examination of both the technological potentials and the socio-legal risks of AI in law enforcement.

This study conducts a qualitative meta-synthesis of scholarly and technical literature published between 2015 and 2025 to investigate the role of AI in contemporary crime detection. The analysis encompasses diverse domains, including urban surveillance, cybercrime mitigation, environmental protection, and financial crime investigation. In doing so, the study identifies key technological trends—such as the use of deep learning for video analytics, spatio-temporal modeling for crime forecasting, and natural language processing for online threat detection. Beyond technical applications, the study critically engages with the ethical, legal, and operational implications of AI integration, paying particular attention to the uneven regulatory landscapes and the potential for disproportionate surveillance of vulnerable populations. The goal is not only to map the current state of AI in policing but also to interrogate its broader societal impact. By synthesizing empirical findings, conceptual models, and critical perspectives, the research provides a foundation for informed policymaking, ethical innovation, and sustainable deployment of AI technologies in public safety infrastructures.

2. Methodology

This study employs a qualitative meta-synthesis methodology to explore the current landscape, technological applications, and socio-legal implications of artificial intelligence in crime detection and prevention. A purposive sampling strategy guided the selection of literature, targeting peer-reviewed academic articles, technical reports, and proceedings published between 2015 and 2025. Sources were identified through systematic searches across major scholarly databases including IEEE Xplore, Scopus, Web of Science, and Google Scholar, using keywords such as “AI in policing”, “crime prediction”, “surveillance”, and “machine learning in law enforcement”. Inclusion criteria emphasized methodological transparency, relevance to AI-based policing practices, and thematic focus on specific domains such

as urban surveillance, cybercrime, environmental crime, and financial fraud. Articles were excluded if they lacked empirical or conceptual rigor or failed to address either technological mechanisms or social consequences. The final corpus consisted of 30 high-quality publications that reflected a diverse range of AI applications, contexts, and critical perspectives. These documents served as the basis for an integrative thematic analysis aimed at synthesizing patterns, identifying key innovations, and critically assessing normative tensions.

Analytical procedures followed a multi-phase coding framework. First, each selected document was reviewed to extract data on its research objectives, AI methods (e.g., deep learning, natural language processing, anomaly detection), crime domains, data sources, and key findings. Second, inductive coding was applied to uncover recurring themes, including technical performance metrics, ethical concerns, legal considerations, and societal impacts. This process was supported by qualitative data analysis software (e.g., NVivo) to ensure systematic categorization and traceability. Thematic clusters were then compared across studies to identify convergences and divergences in technological efficacy, operational scalability, and governance challenges. Special attention was paid to studies that incorporated explainable AI, participatory design, or policy-oriented frameworks. Through this meta-synthesis, the research sought to develop a nuanced understanding of how AI is operationalized in law enforcement, how it reshapes institutional practices, and what safeguards are required for its responsible deployment. This approach enables the generation of evidence-informed insights that are both technologically grounded and normatively critical.

3. Findings

Drawing from a diverse corpus of empirical and conceptual studies published between 2015 and 2025, this section presents thematic insights into how AI technologies are being operationalized across various domains of law enforcement. The selected studies span a range of methodologies, contexts, and crime types— including cybercrime, environmental violations, financial fraud, and urban surveillance— highlighting the breadth of AI integration in public safety infrastructure. Common patterns identified include the use of machine learning for predictive analytics, natural language processing for social media monitoring, and computer vision for real-time surveillance. In addition to technical efficacy, the studies also expose critical issues such as algorithmic bias, data governance challenges, and the lack of standardized ethical frameworks. The paragraphs that follow synthesize these findings across multiple dimensions, focusing on both the functional contributions of AI systems and the socio-legal complexities surrounding their deployment in contemporary policing environments.

Tayal et al. (2015) proposed a modular approach to crime detection

and criminal identification in Indian cities by leveraging data mining techniques on unstructured crime datasets. Their system was designed around six interconnected modules: data extraction, data preprocessing, clustering, Google Map-based visualization, classification, and implementation using the WEKA® software suite. The data extraction module sourced crime data from various online repositories covering the period from 2000 to 2012. This was followed by a preprocessing stage, which standardized and refined the data into a structured dataset comprising 5,038 crime instances characterized by 35 predefined attributes. The crime detection process employed k-means clustering to group similar crimes into two primary clusters, aiding in pattern recognition and trend analysis. To enhance interpretability, results were visually represented using Google Maps. For criminal identification and predictive classification, the study utilized the K-Nearest Neighbors (KNN) algorithm, while validation of the clustering output was conducted through WEKA®, yielding high accuracy rates of 93.62% and 93.99% for the respective clusters. The integration of clustering and classification techniques demonstrated the potential for improving investigative processes and reducing crime rates by enabling more informed and efficient responses from law enforcement agencies. The study thus highlighted the utility of data mining as a practical framework for supporting crime analytics and public safety in the Indian context.

Butt et al. (2021) proposed a spatio-temporal crime prediction framework aimed at enhancing public safety in smart cities through the integration of artificial intelligence and urban surveillance infrastructure. The study focused on identifying high-risk crime zones and forecasting crime incidence using both spatial and temporal data. To detect crime hotspots, the authors applied the Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN) algorithm, which outperformed conventional clustering techniques in managing noisy and non-linear data. For temporal crime forecasting within these identified zones, the Seasonal Auto-Regressive Integrated Moving Average (SARIMA) model was employed. This dual-model approach was tested on a decade's worth of crime data (2008–2017) from New York City. Evaluation was conducted using an 80:20 training-to-testing data split, with performance measured through Mean Absolute Error (MAE). Results showed a substantial improvement in predictive accuracy, with the proposed HDBSCAN-SARIMA model achieving an average MAE of 11.47, significantly outperforming a DBSCAN-based baseline model (MAE 27.03). The study underscored the practical benefits of incorporating spatio-temporal analytics into smart city infrastructures, enabling authorities to anticipate crime patterns and allocate resources proactively. This work contributes to the development of AI-powered predictive policing tools that are both data-efficient and actionable in urban safety planning.

Shoeibi et al. (2021) developed AI-Crime Hunter, a multi-component artificial intelligence platform aimed at detecting and analyzing crime-related content on Twitter. The system was designed to address societal threats such as hate speech and terrorist propaganda by analyzing public tweets through a combination of graph analysis, metadata examination, natural language processing (NLP), and machine learning. The platform begins by extracting and maintaining Twitter data, after which user interactions are examined through graph analysis to map behavioral connections. A time-series analysis of user profiles is then conducted to identify behavioral anomalies. Profiles exhibiting suspicious or abnormal behavior are flagged for further analysis. In the contextual analysis stage, a binary text classification model—combining Support Vector Machine (SVM) with Term Frequency–Inverse Document Frequency (TF-IDF)—is employed to identify tweets related to criminal content, achieving an accuracy of 88.89%. Subsequently, an aspect-based sentiment analysis is applied to crime-related tweets using a DistilBERT model paired with a Feed-Forward Neural Network (FFNN), reaching 80% accuracy. This stage evaluates whether users express dangerous sentiments—such as positive opinions toward criminal acts—which could indicate a potential threat. The platform ultimately generates actionable insights for law enforcement agencies, supporting early detection and intervention strategies in digital crime propagation. The study showcases the value of hybrid AI architectures in mining social media data for public safety and cybercrime control.

Gopichand et al. (2021) proposed an AI-driven framework aimed at detecting and mitigating on-road crimes through the integration of automated surveillance, vehicle identification, and biometric recognition. Responding to the rising incidence of road-related offenses, including kidnapping and vehicular crimes, the study presented a system that leverages traffic cameras and AI models to detect vehicle number plates in real time. Once a number plate is identified, the system queries the Regional Transport Office (RTO) database to retrieve the registered owner's information. In parallel, the system employs face detection and facial recognition techniques to match individuals captured by traffic surveillance with existing biometric records, thereby aiding in suspect identification. This dual-pronged approach enhances real-time situational awareness for law enforcement agencies, facilitating immediate intervention. The proposed solution also supports forensic investigations by providing traceable identity information linked to vehicular activity. The authors emphasized the system's potential to contribute significantly to public safety, particularly in urban areas where road surveillance infrastructure is already in place. This work demonstrated how AI and machine learning technologies can be operationalized for dynamic crime detection and prevention in transit environments.

Meena and Joshi (2023) examined the evolving role of AI in the Indian criminal justice system, focusing on the dual aspects of crime detection and prevention through the lens of "AI policing". The study, rooted in doctrinal analysis, explored the integration of AI technologies such as facial recognition, video and audio analysis, vehicle identification, robotic surveillance, and text-based intelligence processing in policing practices. These tools, supported by predictive policing algorithms, allow law enforcement agencies to analyze vast datasets on criminal activities, thereby enabling proactive crime prevention strategies. The authors acknowledged that such technologies can significantly enhance investigative capabilities and improve crime scene analysis. However, the paper also emphasized the critical challenges surrounding the deployment of AI in the Indian legal context. Key concerns included algorithmic bias, data inaccuracy, lack of human oversight, and the potential infringement on constitutional rights, particularly in a socially stratified society. The study argued that while AI policing holds significant promise, it poses ethical and legal risks if not properly regulated. To address these issues, the authors proposed measures for improving AI accuracy, promoting transparency, and establishing strong legal frameworks to safeguard individual rights. The paper concluded that a balanced approach—one that combines technological innovation with robust legal and ethical oversight—is essential for realizing the benefits of AI policing within a fair and accountable criminal justice system in India.

Apene et al. (2024) examined the transition from traditional crime prevention and detection strategies to advanced AI-driven methodologies. Through a combination of literature review, local observation, and analysis of global news sources, the authors assessed the limitations of conventional methods such as neighborhood watch programs, random stop-and-search tactics, foot patrols, surveillance systems, and crime mapping techniques. These approaches were found to be labor-intensive, reactive, and often inefficient in addressing modern security challenges. The study highlighted how AI technologies, particularly machine learning and computer vision, can enhance the capabilities of law enforcement agencies by enabling predictive and automated responses to crime. Machine learning models were recognized for their capacity to analyze large datasets and identify patterns indicative of potential criminal activity, while computer vision systems could process visual data from surveillance infrastructure to detect and respond to suspicious behavior in real time. The authors advocated for the structured integration of AI into policing practices and recommended the development of a deep learning-based framework to optimize crime detection efforts. They further emphasized the need for ongoing research to refine these technologies and ensure their effective and ethical application in public safety contexts.

Basthikodi et al. (2024) presented an AI-based automated framework designed to improve crime detection and crowd management through intelligent surveillance systems. Recognizing the limitations of manual monitoring—such as time constraints and susceptibility to human error—the study proposed an integration of AI and machine learning (ML) technologies to facilitate real-time, data-driven decision-making. The system centers on AI-enabled CCTV networks capable of processing both static images and live video feeds to detect anomalies, recognize patterns, and deliver timely security threat alerts. Emphasizing both dynamic analysis and operational efficiency, the framework offers enhanced capabilities in monitoring public spaces and detecting potential criminal activity. The research highlights the necessity for substantial investments in technological infrastructure, as well as the establishment of effective data governance practices to support deployment. In addition, ethical considerations surrounding privacy were underscored as essential to the responsible use of such systems. The implementation of this framework aims to provide law enforcement and security agencies with a more modern, accurate, and responsive toolset to manage crowds and preemptively detect crimes. The study contributes to the growing body of literature on AI-driven public safety solutions, demonstrating the potential for intelligent systems to align with contemporary security needs.

Sharma et al. (2024) addressed the complex task of detecting financial crimes, specifically money laundering, by developing an AI-based framework that integrates both supervised and unsupervised machine learning techniques. Presented at the 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), the study focused on minimizing human oversight while improving the precision of suspicious transaction detection. The proposed system features enhanced data preprocessing pipelines and an auto-labeling mechanism to facilitate more efficient training of models using partially labeled or unlabeled financial data. Anomaly detection algorithms were employed to identify atypical transaction patterns that may indicate fraudulent activity. A key emphasis of the research was reducing false positives, a persistent challenge in financial crime detection, in order to ensure more actionable and trustworthy alerts for compliance teams. This dual-method approach enabled the system to not only recognize known patterns of illicit financial behavior but also adaptively discover novel, previously unseen indicators of fraud. The authors demonstrated that AI-powered automation can significantly strengthen FinTech crime surveillance capabilities while reducing manual workload and response times. The work contributes to the growing body of AI applications in cybersecurity and financial regulation, emphasizing the need for intelligent, scalable solutions in high-volume transactional environments.

AlSuwaidi et al. (2024) conducted a survey examining the current landscape and advancements in visual AI applications within smart surveillance systems, with a focus on crime detection and prevention. The review explored the integration of visual AI technologies—particularly in the form of Convolutional Neural Networks (CNNs)—across various surveillance tasks including object detection, facial recognition, anomaly detection, behavior analysis, and scene understanding. These applications collectively contribute to real-time monitoring and threat assessment in urban and critical infrastructure environments. While CNN-based models have become central to image and video analysis in surveillance contexts, the authors identified persistent challenges such as limited access to high-quality, labeled datasets, the computational intensity of deep learning models, and obstacles to scalable deployment. The survey presented a synthesis of state-of-the-art frameworks and innovations, offering a critical evaluation of their effectiveness and limitations. In doing so, the paper highlighted key research gaps and proposed directions for future work aimed at improving system performance, robustness, and operational feasibility. The authors concluded that while visual AI holds significant promise in enhancing security infrastructures, greater attention is needed to address issues related to data efficiency, computational scalability, and context-aware decision-making in crime prevention systems.

Gandal et al. (2024) proposed a deep learning-based system for enhancing crime detection and prediction through the analysis of surveillance video footage. Recognizing the growing need for intelligent monitoring solutions in the face of rising global crime rates, the authors developed a framework that integrates advanced object detection and classification algorithms to identify potentially criminal activities in real time. The system utilizes state-of-the-art deep learning models such as YOLOv5 and Faster R-CNN for precise object detection within video frames. These models are paired with traditional machine learning classifiers—including Support Vector Machines (SVM), Decision Trees, and Random Forests—to categorize the detected objects and predict possible crime-related behaviors. The system was evaluated on a dataset of surveillance videos, and results indicated promising accuracy in both object classification and crime prediction tasks. The proposed solution is intended to assist law enforcement agencies by enabling early detection and intervention, thus contributing to crime prevention efforts. Additionally, the authors suggested that the system's architecture could be adapted to various other contexts, such as traffic monitoring, wildlife tracking, and industrial safety applications. This work demonstrates the utility of combining computer vision and machine learning for proactive public safety surveillance.

Singh (2024) explored the transformative potential of AI in detecting and addressing environmental crimes, an area where conventional law

enforcement methods have historically struggled due to the scale, complexity, and often transboundary nature of such offenses. The study emphasized the limitations of traditional surveillance and legal mechanisms in managing crimes like illegal deforestation, wildlife trafficking, and pollution-related offenses, which are often vast, underreported, and difficult to monitor in real time. In response, the paper proposed AI as a paradigm-shifting solution capable of enhancing environmental law enforcement through technologies such as satellite imagery analysis and machine learning algorithms. These tools can detect anomalous patterns and environmental changes indicative of illegal activities, thereby enabling earlier intervention and more effective regulatory responses. Singh also critically examined the legal challenges associated with adopting AI in this context, including evidentiary standards, accountability for algorithmic errors, and the necessity of building a legal framework that accommodates technologically driven investigations. The study concluded by advocating for a multidisciplinary approach that balances innovation with legal safeguards, ensuring that AI's integration into environmental crime detection enhances both ecological protection and justice system integrity. This work contributes to emerging discourse on the role of digital technologies in environmental governance and criminal law reform.

Iqbal et al. (2025) conducted a systematic literature review to investigate recent advancements in AI, particularly machine learning and deep learning, as applied to crime prediction. Acknowledging that prior reviews had not comprehensively addressed the latest AI techniques, the authors aimed to consolidate state-of-the-art methodologies and highlight current trends and research gaps. Using a rigorous qualitative selection process across multiple digital repositories, they identified and analyzed 55 high-quality research articles. These articles were assessed across several dimensions, including publishing venues, predictive models employed, geographical coverage, data sources, real-time data usage, and temporal scope of crime records. The review found that IEEE Access was the most frequent publishing outlet in this domain. Traditional statistical and machine learning techniques were still prevalent (33%), but there was a clear emergence of sophisticated models such as Convolutional Neural Networks (CNNs), Long Short-Term Memory Networks (LSTMs), Generative Adversarial Networks (GANs), and Graph Neural Networks (GNNs), indicating a shift toward more complex and hybrid approaches. The geographical analysis showed a significant focus on U.S.-based datasets (56%), suggesting a disparity in global research representation. Importantly, the review identified a lack of integration of real-time data into predictive models, representing a major limitation and a priority area for future research. Overall, the study offered critical insights for researchers, practitioners, and

policymakers seeking to develop more robust, context-sensitive, and data-rich AI-driven crime prediction systems.

Kanwal et al. (2025) investigated the role of AI in enhancing crime detection and policing effectiveness, with a particular emphasis on operational efficiency and stakeholder perceptions. The study surveyed 159 police officers acquainted with AI tools and assessed their views across five domains: AI technologies, crime detection and control, policing effectiveness, ethical/ legal/ social implications, and public trust. Statistical analysis using SPSS revealed that AI had a significant positive impact on both crime detection ($\beta = 0.48$, $P < 0.001$) and operational efficiency ($\beta = 0.318$, $P < 0.01$), affirming the first two hypotheses. However, mediation analysis indicated that public trust did not mediate the relationship between ethical concerns and AI's effectiveness in crime detection ($P > 0.95$), and moderation analysis found no significant effect of ethical concerns ($P = 0.437$) or public trust ($P = 0.398$) on the core relationship between AI use and crime detection. These findings underscore that AI technologies contribute independently to improving law enforcement operations but also highlight that current levels of public trust and ethical engagement do not significantly influence this enhancement. The authors emphasized the importance of transparent governance and ethical oversight in the implementation of AI systems to ensure sustainable, responsible integration into policing frameworks. The study contributes to the literature by quantifying perceptions within police departments and outlining the potential and limitations of AI-driven strategies in public safety management.

Bagonza et al. (2024) explored the integration of AI into public safety and emergency management systems in the United States, emphasizing its transformative potential in addressing escalating threats such as violent crime, mass shootings, and climate-related disasters. Drawing on historical data—such as over 630 mass shootings in 2023, 56,580 wildfires, and 387 climate disasters since 1980—the paper outlined the urgent need for real-time, predictive, and proactive public safety infrastructure. The authors proposed a comprehensive AI-driven framework that leverages machine learning models, predictive analytics, and threat detection algorithms to improve situational awareness, decision-making, and resource allocation. The framework processes real-time inputs from diverse sources including crime reports, social media, IoT sensors, and environmental data to detect threats, anticipate crime, and optimize emergency responses. The study included practical case studies demonstrating how law enforcement, disaster response teams, and cybersecurity agencies can use AI technologies to shift from reactive to proactive operations. Beyond technical considerations, the paper also examined critical ethical concerns related to AI deployment, such as privacy, algorithmic bias, and data governance. The authors proposed responsible AI frameworks

to ensure equitable, transparent, and accountable implementation. Ultimately, the study presented a strategic roadmap for integrating AI into U.S. public safety infrastructure, aiming to enhance national preparedness, responsiveness, and community resilience in the face of evolving public safety and emergency challenges.

Bertrand et al. (2024) investigated the challenges posed by AI integration into highly regulated sectors—specifically financial crime detection within anti-money laundering (AML) frameworks—by centering the perspectives of supervisors, i.e., regulatory professionals responsible for auditing AI-driven compliance processes. Despite AI's capacity to enhance fraud detection, its adoption remains limited in fields like banking due to the opacity of model decision-making, which conflicts with strict regulatory standards for explainability and accountability. To address this, the authors conducted scenario-based workshops with 13 supervisors and 6 banking professionals, analyzing their needs in relation to auditing AI systems. The study revealed seven specific requirements that supervisors demand for model justifiability, including traceable logic, consistency with legal obligations, and explanations that qualify as audit-ready evidence. These findings underscore that supervisors are not only concerned with the technical performance of AI models, but also with their ability to produce interpretable, transparent outputs that align with institutional and legal norms. The paper emphasized that existing AI systems often fail to meet these standards, highlighting a gap between technical capabilities and compliance expectations. The study calls for the development of human-centered, regulation-aware explanation systems to ensure the trustworthiness and legal defensibility of AI in financial crime contexts.

Natarajan et al. (2024) investigated the application of artificial intelligence in crime detection, focusing specifically on automated face sketch synthesis to enhance suspect identification. The study addressed the limitations of traditional methods, such as hand-drawn or manually rendered computer sketches, which are often used by law enforcement when photographic evidence is unavailable. To improve the accuracy and utility of suspect identification in large-scale digital forensic contexts, the authors proposed a deep learning-based solution using the Golden Jackal Optimized Artificial Neural Network (GJO-ANN). This model automates the generation of facial sketches based on crime scene inputs such as time, location, and crime type, facilitating comparison with sketches from eyewitnesses or forensic artists. The system supports the classification of potential perpetrators by identifying visual similarities across datasets. Experimental evaluations demonstrated that the GJO-ANN approach yielded superior accuracy and efficiency in producing face sketches compared to conventional techniques, thereby enhancing the investigative capacity of law enforcement. The study contributes to the field by integrating optimized neural network architectures into visual-based criminal profiling and underscores the

potential of deep learning tools to address persistent challenges in forensic sketch analysis and electronic crime scene investigation.

Ersöz et al. (2025) conducted a comprehensive literature review examining the role of AI in crime prediction, with a particular focus on explainability as a critical factor for trust and adoption in law enforcement contexts. The survey synthesized findings from 142 selected studies addressing AI applications in predicting crimes against individuals, property, and society. While the review confirmed the potential of AI to enhance predictive policing through accurate pattern recognition and data-driven decision-making, it also underscored the challenges associated with the opacity of many AI systems. To address concerns over the interpretability and fairness of these models, the authors analyzed the emerging field of Explainable AI (XAI), which aims to make AI decision processes more transparent and understandable to stakeholders. Despite growing interest, the review found that XAI techniques remain insufficiently integrated into existing crime prediction frameworks. The authors emphasized that explainability is vital not only for ethical AI use but also for fostering public trust and institutional accountability. The study's methodological framework involved rigorous criteria for selecting both foundational reviews and original research articles, with a structured assessment of how each incorporated or neglected explainability features. The paper concludes by advocating for increased research and development of XAI tools in crime prediction to ensure these systems are accurate, interpretable, and socially responsible, thereby supporting more effective and equitable crime prevention strategies.

Fernandez-Basso et al. (2025) introduced an AI knowledge-based system designed to assist law enforcement in managing and analyzing large-scale data during criminal investigations, particularly in complex environments such as the dark web. Recognizing the growing challenge posed by data volume and complexity, the authors developed an early warning and early action system that integrates multiple AI tools to streamline data collection, processing, and knowledge extraction. The system supports investigative workflows by identifying relevant patterns, entities, and potential criminal hotspots, thus enhancing the efficiency and direction of police investigations. A key feature of the system is its ability to extract actionable intelligence from unstructured sources, exemplified through case studies involving dark web data, including firearm-related advertisements. This application demonstrates the tool's capacity to surface hidden criminal activity and provide leads for deeper inquiry. While not intended to replace human judgment, the system mitigates the burden of manual data analysis and facilitates more timely and targeted law enforcement responses. The authors emphasized the tool's flexibility in adapting to various investigative scenarios and its potential role in augmenting decision-making during early-stage investigations. Overall, the study contributes

a practical AI-assisted framework aimed at improving the investigative capacity and situational awareness of law enforcement agencies in data-intensive contexts.

Kaushik et al. (2025) proposed the Advanced AI-Based Detection and Tracking System (ADTS), a real-time surveillance framework designed to enhance urban crime prevention and suspect identification through cutting-edge computer vision technologies. The system integrates YOLOv8 for high-performance object detection and Multi-task Cascaded Convolutional Networks (MTCNN) for precise face detection and tracking. By processing unstructured video data from multiple CCTV camera feeds, ADTS identifies suspicious activities and continuously monitors individuals of interest using facial feature matching techniques. This enables persistent tracking of suspects across different locations within a surveillance network. The system's architecture supports scalability and operational efficiency, making it viable for large-scale urban deployments. Experimental evaluation demonstrated high accuracy in object and face detection, consistent tracking performance, and efficient resource utilization, thus addressing key limitations of earlier AI surveillance solutions. The study emphasizes the system's potential to advance situational awareness for law enforcement agencies, enabling faster response times and proactive crime mitigation. Overall, ADTS represents a significant advancement in intelligent surveillance technology, contributing to more effective real-time crime monitoring and identification in high-density urban environments.

4. Conclusion

AI technologies are changing all aspects of human life (Rahmatian & Sharajsharifi, 2021). They have introduced profound shifts in the epistemology and logistics of policing by redefining how knowledge about crime is produced, operationalized, and acted upon. From predictive analytics to computer vision, the tools now available to law enforcement are not simply augmentations of existing practices—they are reshaping the very foundations of investigative reasoning and decision-making. The empirical evidence synthesized in this review suggests that AI systems can outperform traditional methods in speed, scale, and granularity, offering novel capabilities in surveillance, threat detection, and resource optimization. Yet, this apparent technical superiority invites deeper reflection: What kinds of crimes are being detected more efficiently, whose behaviors are being monitored, and what institutional assumptions are embedded in these systems?

Beneath the surface of efficiency gains lie substantial epistemological and ethical challenges. AI systems do not simply process neutral data; they are trained on historically situated, socially patterned information that reflects and reproduces existing biases (Black, 2023). This review reveals a persistent undercurrent of

algorithmic discrimination, particularly against marginalized communities, as well as a systemic opacity that undermines procedural justice. Moreover, the delegation of discretionary judgment to non-transparent machine learning models raises serious concerns about accountability, particularly when these systems make high-stakes determinations such as identifying suspects or flagging behaviors as criminally suspicious. The findings suggest that, despite the promise of AI in augmenting police capabilities, its uncritical deployment risks reinforcing structural inequalities and insulating decision-making from democratic scrutiny.

Furthermore, the global landscape of AI in policing remains uneven, not only in terms of technological infrastructure but also in legal safeguards, cultural norms, and institutional readiness. Many studies originate from technologically advanced contexts with specific normative assumptions—such as the prioritization of security over privacy—which may not translate across jurisdictions. The lack of contextual adaptability in AI models, combined with a scarcity of real-time, high-quality, and representative data in many regions, limits both their effectiveness and ethical defensibility. Equally troubling is the relatively weak integration of interdisciplinary oversight, where critical voices from law, sociology, philosophy, and affected communities are often absent from design and deployment processes. This fragmentation reflects a broader tension between technological determinism and democratic governance—one that must be resolved if AI is to serve as a tool of justice rather than control.

The future of AI in crime detection hinges not on technical sophistication alone, but on the willingness of institutions to embed these systems within transparent, accountable, and normatively guided frameworks. This study emphasizes the need for a paradigm shift: from AI as a tool of unreflective automation to AI as a contested and negotiated socio-technical system. Policymakers must move beyond compliance checklists toward meaningful regulatory architectures that ensure fairness, auditability, and public legitimacy.

Conflict of interest

The authors declared no conflicts of interest.

Ethical considerations

The authors have completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc. This article was not authored by artificial intelligence.

Data availability

The dataset generated and analyzed during the current study is available from the author on reasonable request.

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

References

- AlSuwaidi, H.A.; Harous, S.; Serhani, M.A. (2024). "Review of visual AI applications in smart surveillance for crime detection and prevention: A survey". *4th International Conference on Distributed Sensing and Intelligent Systems (ICDSIS 2023)*. <https://doi.org/10.1049/icp.2024.0502>.
- Apene O.Z.; Blamah, N.V.; & Aimufua, G.I.O. (2024). "Advancements in crime prevention and detection: From traditional approaches to artificial intelligence solutions". *European Journal of Applied Science, Engineering and Technology*. 2(2): 285-297. [https://doi.org/10.59324/ejaset.2024.2\(2\).20](https://doi.org/10.59324/ejaset.2024.2(2).20).
- Babuta, A.; & Oswald, M. (2020). *Data Analytics and Algorithms in Policing in England and Wales*. Royal United Services Institute. https://static.rusi.org/rusi_pub_165_2020_01_algorithmic_policing_babuta_final_web_copy.pdf.
- Bagonza, J.K.; Nakayenga, H.; & Zimbe, I. (2024). "Leveraging AI for real time crime prediction, disaster response optimization and threat detection to improve public safety and emergency management in the US". *World Journal of Advanced Research and Reviews*. 23(3): Article 2835. <https://doi.org/10.30574/WJARR.2024.23.3.2835>.
- Basthikodi, M.; Vidya, B.; Pinto, E.M.; Basith, M.; & Rao, S.A. (2024). "AI based automated framework for crime detection and crowd management". In *2024 Second International Conference on Advances in Information Technology (ICAIT)*. IEEE. <https://doi.org/10.1109/ICAIT61638.2024.10690527>.
- Bertrand, A.; Eagan, J.R.; Maxwell, W.; & Brand, J. (2024). "AI is entering regulated territory: Understanding the supervisors' perspective for model justifiability in financial crime detection". In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. Article 480: 1-21. <https://doi.org/10.1145/3613904.3642326>.
- Black, A. (2023). "AI and democratic equality: how surveillance capitalism and computational propaganda threaten democracy". In *International Conference on Bridging the Gap between AI and Reality* (pp. 333-347). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-73741-1_21.
- Brantingham, P.J.; Valasik, M. & Mohler, G.O. (2018). "Does predictive policing lead to biased arrests? Results from a randomized controlled trial". *Statistics and Public Policy*. 5(1): 1-6. <https://doi.org/10.1080/2330443X.2018.1438940>.
- Butt, U.M.; Letchmunan, S.; Hassan, F.H.; Ali, M.; Baqir, A.; & Koh, T.W. (2021). "Spatio-temporal crime predictions by leveraging artificial intelligence for citizens security in smart cities". *IEEE Access*. 9: 47516-47529. <https://doi.org/10.1109/ACCESS.2021.3068306>.
- Ersöz, F.; Ersöz, T.; Marcelloni, F.; & Ruffini, F. (2025). "Artificial Intelligence in crime prediction: A survey with a focus on explainability". *IEEE Access*. 13: 59646–59674. <https://doi.org/10.1109/ACCESS.2025.3553934>.
- Fernandez-Basso, C.; Gutiérrez-Batista, K.; Gómez-Romero, J.; Ruiz, M.D.; & Martín-Bautista, M.J. (2025). "An AI knowledge-based system for police assistance in crime investigation". *Expert Systems*. 42(1): e13524. <https://doi.org/10.1111/exsy.13524>.
- Gandal, J.R.; Gandal, S.J.; & Suryavanshi, M. (2024). "Analysis of object detection, prediction, and prevention AI and ML algorithms for enhancing crime surveillance videos". In *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*. IEEE. <https://doi.org/10.1109/I2CT61223.2024.10544214>.
- Gopichand, G.; Vijayakumar; & Pasupuleti, N.S. (2021). "On-road crime detection

- using artificial intelligence”. In Favorskaya, M.N.; Mekhilef, S.; Pandey, R.K.; & Singh, N. (Eds.). *Innovations in Electrical and Electronic Engineering* (pp. 423-432). Springer. https://doi.org/10.1007/978-981-15-4692-1_32.
- Iqbal, N.; Hassan, A.; & Waheed, T. (2025). “AI-driven crime prediction: A systematic literature review”. *Journal of Computational Social Science*. 8: 53. <https://doi.org/10.1007/s42001-025-00373-z>.
- Kanwal, S.; Iftikhar, S.; Munir, R.; Ahmad, M.; & Waheed, A. (2025). “Role of artificial intelligence in crime detection and control: Enhancing policing strategies and effectiveness”. *Journal of Social Signs Review*. 3(07): 243-255. <https://www.socialsignsreview.com/index.php/12/article/view/324>.
- Kaushik, A.; Paprunia, D.; Wangde, I.; Jain, S.; Deepak, S.; & Sankhe, M. (2025). “Advanced AI-Based Detection and Tracking System (ADTS) for crime prevention and identification in real-time surveillance”. In *2025 International Conference on Computing Technologies (ICOCT)*. IEEE. <https://doi.org/10.1109/ICOCT64433.2025.11118424>.
- Leukfeldt, R.; & Holt, T.J. (2020). *The Human Factor in Cybercrime*. London, Routledge. <https://doi.org/10.4324/9780429460593>.
- Manning, P.K. (2008). *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. NYU Press. <http://ndl.ethernet.edu.et/bitstream/123456789/14252/1/81.pdf>.
- McCue, C. (2020). *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. 2nd ed. Butterworth-Heinemann. http://repo.darmajaya.ac.id/4009/1/Data%20Mining%20and%20Predictive%20Analysis%2C%20Second%20Edition_%20Intelligence%20Gathering%20and%20Crime%20Analysis%20%28%20PDFDrive%20%29.pdf.
- Meena M.; & Joshi, A. (2023). “AI policing in criminal justice: Methods & concerns in crime detection and prevention in India”. *NFSU Journal of Law and Artificial Intelligence*. 2(1). <https://doi.org/10.62995/jlai1220250812>.
- Natarajan, R.; Mahadev, N.; Gupta, S.K.; & Alfurhood, B.S. (2024). “An investigation of crime detection using Artificial Intelligence and face sketch synthesis”. *Journal of Applied Security Research*. 19(4): 542-559. <https://doi.org/10.1080/19361610.2024.2302237>.
- Rahmatian, F.; & Sharajsharifi, M. (2022). “Reimagining MBA education in the age of artificial intelligence: A meta-synthesis”. *Socio-Spatial Studies*. 6(1). <https://doi.org/10.22034/soc.2022.223610>.
- Rahmatian, F.; & Sharajsharifi, M. (2021). “Artificial intelligence in MBA education: Perceptions, ethics, and readiness among Iranian graduates”. *Socio-Spatial Studies*. 5(1). <https://doi.org/10.22034/soc.2021.223600>.
- Sharma, P.; Prakash, A.S.; & Malhotra, A. (2024). “Application of advanced AI algorithms for fintech crime detection”. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE. <https://doi.org/10.1109/ICCCNT61001.2024.10725857>.
- Shoeibi, N.; Shoeibi, N.; Hernández, G.; Chamoso, P.; & Corchado, J.M. (2021). “AI-crime hunter: An AI mixture of experts for crime discovery on Twitter”. *Electronics*. 10(24): 3081. <https://doi.org/10.3390/electronics10243081>.
- Singh, S. (2024). “AI in environmental crime detection: A paradigm shift in criminal law”. *Conference: Environmental Law: Issues and Emerging Challenges*. SSRN. <https://ssrn.com/abstract=5123120>.
- Tayal, D.K.; Jain, A.; Arora, S.; Agarwal, S.; Gupta, T.; & Tyagi, N. (2015). “Crime detection and criminal identification in India using data mining techniques”. *AI & Society*. 30: 117-127. <https://doi.org/10.1007/s00146-014-0539-6>.