Interdisciplinary Studies in Society, Law, and Politics 2027; 6(1): 1-18

ISSLP

Original Research

Opportunities of Artificial Intelligence in Scientific Crime Detection: A Review of Global Experiences and Localization Capacities in Iran

Alireza. Gholamhoseini[1], Ali. Najafi Tavana[2*], Atefe. Aminia[2]

[1] Department of Law, UAE.C., Islamic Azad University, Dubai, United Arab Emirates
[2] Department of Law, CT.C., Islamic Azad University, Tehran, Iran

*** Corresponding author email address**: 5809885586@iau.ir

Received: 2026-05-04 **Revised:** 2026-10-01 **Accepted:** 2026-10-07 **Initial Publish:** 2026-11-03 **Final Publish:** 2027-01-01

The increasing complexity of contemporary crime, the expansion of cybercrime and organized criminal activity, and the growing volume of digital and forensic data have exposed significant limitations in traditional methods of crime detection. Artificial intelligence has created new opportunities for scientific crime detection by enabling rapid processing of large datasets, identification of hidden criminal patterns, intelligent analysis of audiovisual and textual evidence, detection of suspicious financial transactions, reconstruction of criminal networks, and enhancement of digital forensic investigations. This study examines the principal opportunities of artificial intelligence in scientific crime detection, reviews selected international experiences, and evaluates the capacities and requirements for localizing these technologies in Iran. Using a descriptive-analytical and comparative approach, the study focuses on the technical, procedural, legal, and institutional dimensions of AI-assisted criminal investigation. The findings indicate that machine learning, deep learning, computer vision, natural language processing, biometric analysis, graph-based analytics, and intelligent anomaly detection can significantly improve the speed, accuracy, and analytical depth of crime detection. International experience also demonstrates, however, that the effectiveness of these technologies depends on data quality, transparency, explainability, human oversight, independent validation, and appropriate legal safeguards. In Iran, existing judicial, police, financial, identity, cybercrime, and administrative data infrastructures provide an important foundation for the development of AI-assisted scientific crime detection. Nevertheless, fragmented databases, limited interoperability, insufficient regulation of algorithmic evidence, risks of bias and unlawful profiling, inadequate explainability, cybersecurity concerns, and shortages of specialized human resources remain substantial obstacles. The study concludes that responsible localization requires secure inter-agency data integration, indigenous Persian-language AI models, explainable and auditable algorithms, clear rules governing the admissibility and use of AI-assisted evidence, specialized professional training, and continuous human control. Artificial intelligence should therefore function as an investigative decision-support instrument rather than an autonomous substitute for investigators, forensic experts, prosecutors, or judges.

Keywords: *Artificial Intelligence; Scientific Crime Detection; Criminal Investigation; Digital Forensics; Predictive Policing; Algorithmic Evidence; Explainable Artificial Intelligence; Iran.*

How to cite this article:
Gholamhoseini, A., Najafi Tavana, A., & Aminia, A. (2027). Opportunities of Artificial Intelligence in Scientific Crime Detection: A Review of Global Experiences and Localization Capacities in Iran. *Interdisciplinary Studies in Society, Law, and Politics, 6*(1), 1-18. https://doi.org/10.61838/kman.isslp.595

© 2027 The authors. Published by KMAN Publication Inc. (KMANPUB). This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

1. Introduction

The transformation of contemporary criminality has created profound challenges for conventional systems of crime detection. Criminal investigations were historically organized around a relatively limited universe of evidence, including witness statements, confessions, physical traces, fingerprints, documentary evidence, and the results of conventional forensic examinations. Although these methods remain fundamental to criminal justice, the environment in which crimes are committed and investigated has changed considerably. Contemporary offenses increasingly involve digital communications, online transactions, interconnected financial systems, large-scale databases, encrypted devices, social networks, intelligent platforms, and transnational information flows. Cybercrime, organized economic crime, identity fraud, sophisticated financial offenses, technology-assisted deception, and crimes committed through online infrastructures generate quantities and varieties of information that are difficult to examine through traditional investigative techniques alone. Artificial intelligence has consequently emerged as a significant technological instrument through which investigative authorities can process complex information, identify hidden relationships, detect patterns that may escape ordinary human observation, and improve the speed with which evidentiary materials are examined. Iranian scholarship has similarly emphasized that artificial intelligence can alter the process of crime detection by enabling investigators to move beyond exclusively manual and reactive forms of analysis toward computationally assisted investigation (Mohammadinia & Alizadeh, 2023). Earlier research on computer-based crime analysis also demonstrated the importance of artificial intelligence methods in extracting meaningful patterns from criminal data and supporting investigative analysis (Keyvanpour et al., 2021).

Scientific crime detection may be understood as the systematic application of scientific knowledge, technologies, analytical techniques, and validated methods to determine whether a crime has occurred, reconstruct relevant events, identify potential perpetrators, analyze evidentiary traces, and provide information capable of assisting criminal proceedings. Its defining characteristic is not merely the use of technological instruments but the effort to increase objectivity, reproducibility, traceability, and reliability in criminal investigation. Artificial intelligence expands this scientific orientation because it introduces computational capacities capable of handling forms of evidence that are too voluminous, complex, or interconnected for conventional manual examination. Machine learning can identify recurring relationships in historical crime data; deep learning can classify images, videos, audio, and complex digital traces; natural language processing can examine large volumes of written material; graph-based methods can uncover relationships among persons, transactions, devices, locations, and organizations; and intelligent anomaly detection can identify unusual patterns that merit further investigation. The growing importance of these tools is reflected in broader scholarship on AI-enabled crime detection and prevention, which emphasizes the capacity of intelligent systems to strengthen pattern recognition, information processing, and analytical support in policing and criminal investigation (Kahla, 2024). Systematic studies of artificial intelligence in criminal justice management likewise indicate that AI is increasingly relevant not only to isolated technical tasks but also to broader investigative and organizational processes (Talukder & Shompa, 2024).

The significance of this transformation is particularly visible in cybercrime investigations. Digital offenses may involve enormous volumes of logs, messages, metadata, network records, device artifacts, financial information, and online behavioral indicators. Traditional investigative review becomes increasingly difficult when relevant evidence is dispersed across multiple platforms or mixed with very large quantities of irrelevant information. Research on the application of artificial intelligence to cybercrime detection has therefore emphasized the role of intelligent tools in identifying suspicious activity, recognizing recurring attack patterns, classifying malicious behavior, and accelerating the analysis of complex digital evidence (Habibi & Rezaei, 2022). Recent systematic research concerning cybercrime intention recognition has further demonstrated that computational analysis may assist in identifying behavioral and linguistic indicators associated with malicious intent, although the reliability of such inferences depends heavily on data quality, contextual interpretation, and appropriate

methodological controls (Kassa et al., 2024). This becomes still more important as AI itself is increasingly used by offenders. AI-powered social engineering can increase the sophistication, scalability, personalization, and plausibility of deceptive communications, creating new investigative problems for law-enforcement institutions (Gonzaga et al., 2026). The technological development of criminal behavior therefore generates a dual imperative: investigative institutions must understand AI both as an instrument that can be exploited by offenders and as an analytical technology that may strengthen the detection of such offenses.

The relevance of artificial intelligence extends equally to economic and financial crime. Banking offenses, tax fraud, money laundering, procurement fraud, and complex schemes involving numerous transactions frequently produce data structures whose evidentiary value becomes visible only when relationships among multiple transactions are examined simultaneously. Research concerning the prevention and detection of banking and tax crimes has emphasized both the advantages and challenges associated with using artificial intelligence for identifying suspicious financial patterns (Haghi & Raisi, 2023). AI-enabled financial crime detection can improve the identification of abnormal transactions, relational patterns, and behavioral anomalies that would be difficult to discover through isolated examination of individual records (Rouhollahi, 2021). Similar approaches can be employed in procurement environments, where artificial intelligence can support the detection of irregular bidding behavior, unusual relationships among participants, and transactional structures that may indicate fraud (Ezeji, 2024). These capacities do not transform an algorithmic signal into proof of criminal responsibility; rather, they create investigative leads that can guide human investigators toward information requiring closer legal and evidentiary scrutiny.

Artificial intelligence also changes the relationship between criminal investigation and surveillance technologies. The rapid development of biometric systems, intelligent video analytics, facial recognition, object recognition, license-plate recognition, movement analysis, and automated image classification has created new possibilities for identifying suspects, locating missing persons, reconstructing events, and searching extensive audiovisual archives. Research on biometric surveillance highlights the potential of these technologies to assist authorities in apprehending offenders while simultaneously demonstrating the need to protect innocent persons from excessive or inaccurate identification practices (Haley, 2025). This dual character is central to any assessment of artificial intelligence in scientific crime detection. A system capable of rapidly identifying a person of interest can significantly accelerate an urgent investigation, but the same system can generate serious legal consequences if it relies on inaccurate biometric matches, incomplete datasets, or discriminatory identification patterns. Artificial intelligence therefore cannot be evaluated solely by reference to its technical capabilities. Its legitimate use in criminal justice also depends on reliability, accountability, explainability, necessity, proportionality, and respect for procedural rights.

Predictive applications make this tension even more pronounced. By analyzing historical crime records, geographical information, temporal patterns, and other variables, AI systems may estimate where certain forms of crime are more likely to occur or identify configurations that warrant preventive attention. Such techniques potentially enable more efficient allocation of investigative and policing resources. At the same time, predictive systems may reproduce historical patterns of enforcement contained within their training data. If earlier policing concentrated disproportionately on particular neighborhoods or social groups, the resulting datasets may lead an algorithm to designate the same locations or populations as high-risk, producing a feedback cycle in which past enforcement patterns are converted into future computational recommendations. The concern that predictive systems may perpetuate rather than merely identify existing bias has consequently become a central issue in contemporary debates about artificial intelligence and crime control (Joseph, 2024). The emergence of machine-centered forms of criminological analysis has also prompted broader questions concerning how algorithmic systems reshape the production of knowledge about crime, risk, offenders, and intervention (Campedelli, 2025). Scientific crime detection therefore requires a distinction between using algorithms to discover relevant patterns and allowing statistical patterns to become substitutes for individualized evidence.

A further transformation concerns criminal profiling. Conventional profiling traditionally depended on behavioral interpretation, investigative experience, psychological inference, and the comparison of crime-scene features with prior cases. Cognitive artificial intelligence now creates the possibility of integrating behavioral, contextual, relational, and historical data to generate more structured investigative hypotheses. Contemporary work on cognitive AI and criminal profiling suggests that computational models can contribute to the organization and evaluation of complex information relevant to offender characteristics and behavioral patterns (Buele et al., 2026). Nevertheless, such systems should not be understood as mechanisms capable of determining guilt or reliably reconstructing subjective criminal intent independently of human judgment. Profiling remains probabilistic and must be distinguished from evidentiary proof. The same caution applies to emerging attempts to connect artificial intelligence with neurological or behavioral prediction, where the prospect of predicting criminal conduct raises particularly serious questions about determinism, autonomy, evidentiary validity, and the presumption of innocence (Deb, 2024).

These developments are directly relevant to Iran. Iranian criminal justice institutions possess expanding digital infrastructures, extensive administrative and judicial datasets, developing cybercrime capabilities, automated identification systems, financial monitoring structures, and an increasingly explicit policy interest in artificial intelligence. These resources create genuine opportunities for the gradual introduction of AI-assisted scientific crime detection. At the same time, localization cannot be understood as the simple importation of foreign software or investigative models. The effectiveness and legality of AI depend on the characteristics of domestic data, the structure of national institutions, Persian-language processing capabilities, rules governing criminal evidence, judicial supervision, privacy protections, cybersecurity requirements, available computational infrastructure, and professional capacity within police, prosecution, forensic, and judicial institutions. A model trained on foreign criminal datasets or linguistic patterns may perform inadequately when transferred directly to Iranian data, while a system developed in a legal environment with different standards of evidence and surveillance may be incompatible with Iranian criminal procedure. Localization must therefore involve technical adaptation, legal regulation, institutional restructuring, and the creation of mechanisms capable of ensuring that artificial intelligence remains subordinate to lawful criminal investigation.

The objective of the present study is to analyze the principal opportunities created by artificial intelligence for scientific crime detection, examine significant lessons derived from international experience, and assess the capacities and requirements for responsible localization in Iran. The central question is how artificial intelligence can enhance the accuracy, speed, analytical depth, and organizational efficiency of scientific crime detection while remaining compatible with evidentiary reliability, fair criminal procedure, privacy, human oversight, and institutional accountability. The study adopts a descriptive-analytical and comparative approach based on the examination of relevant scholarship and the analytical reconstruction of technical, procedural, legal, and institutional dimensions of AI-assisted crime detection. Its emphasis is deliberately narrower than a general examination of artificial intelligence in criminal justice. Sentencing automation, autonomous adjudication, generalized legal prediction, and unrelated applications of AI fall outside the principal scope unless they directly illuminate questions of crime detection, investigative evidence, or institutional design. The analysis proceeds from the proposition that artificial intelligence is most defensible in this field when treated as an advanced instrument of scientific investigation and decision support rather than an autonomous source of criminal suspicion, factual determination, or legal judgment.

2. Artificial Intelligence and the Transformation of Scientific Crime Detection

The most immediate contribution of artificial intelligence to scientific crime detection lies in its capacity to process evidence at a scale that exceeds ordinary human analytical ability. Criminal investigations increasingly generate heterogeneous datasets composed of text, images, video, audio, location data, transaction records, device information, communication metadata, network relationships, and traces obtained from digital platforms. The investigative challenge is therefore no longer confined to obtaining

information; it increasingly concerns identifying which elements within a massive informational environment are legally and factually relevant. Artificial intelligence can assist this process by classifying large datasets, recognizing recurring patterns, identifying anomalies, connecting apparently unrelated records, and prioritizing materials for human examination. Computer-based crime analysis already demonstrated the value of AI techniques for identifying patterns in criminal information and supporting investigative reasoning (Keyvanpour et al., 2021). More recent literature has expanded this perspective by emphasizing that AI can operate across multiple stages of crime detection, from initial data screening to pattern identification and investigative decision support (Kahla, 2024). The transformation is therefore not simply one of automation; it involves a shift from isolated evidence examination toward relational and data-intensive forms of investigation.

Machine learning occupies a central position in this transformation. Instead of relying exclusively on predetermined rules, machine-learning systems can identify statistical relationships within existing datasets and use those relationships to classify new information or generate predictions. In crime detection, such systems may be employed to distinguish normal from suspicious transactions, classify types of cyber activity, identify similarities among incidents, prioritize cases, or recognize recurring behavioral features. Their utility is particularly apparent where the number of variables is too large for conventional manual analysis. Financial crime is an illustrative example because suspicious behavior may be visible not in any individual transaction but in the relationship among sequences of transfers, identities, accounts, timing patterns, and transaction values. AI-enabled financial crime analysis can identify such structures and direct investigators toward potentially significant anomalies (Rouhollahi, 2021). Studies addressing banking and tax crime similarly recognize that intelligent analytical systems can strengthen the detection of complex irregularities, although their effectiveness depends on reliable data and suitable institutional implementation (Haghi & Raisi, 2023). In procurement fraud, artificial intelligence may assist by detecting patterns involving repeated bidders, irregular pricing relationships, abnormal award structures, or suspicious transactional connections (Ezeji, 2024).

Deep learning extends these capacities to forms of evidence such as images, video, speech, and other high-dimensional data. Intelligent video analysis is particularly relevant because modern cities, transportation systems, commercial centers, public institutions, and private facilities produce enormous amounts of surveillance footage. Human operators cannot continuously examine all available recordings with equal attention, and retrospective manual review can consume substantial investigative resources. Computer-vision systems can assist by identifying objects, tracking movement, detecting specified visual characteristics, locating relevant sequences, or flagging events that differ from expected patterns. Biometric surveillance technologies add the possibility of comparing facial or other biometric characteristics against reference databases. Research concerning biometric surveillance emphasizes that such tools may contribute to the identification and apprehension of offenders, but their deployment must be carefully structured to avoid unjustified interference with innocent individuals (Haley, 2025). Accuracy should therefore be treated as an evidentiary and rights-based issue rather than merely a technical performance metric. A false positive in a commercial recommendation system may be inconvenient; a false biometric match in a criminal investigation may lead to detention, intrusive searches, reputational harm, or distorted investigative attention.

Artificial intelligence also offers important possibilities in digital forensic science. Conventional digital forensic practice frequently requires investigators to recover, preserve, classify, and interpret enormous quantities of data from computers, mobile devices, cloud environments, communication applications, and network systems. AI can assist in filtering irrelevant material, identifying potentially significant files, detecting malicious software patterns, reconstructing communication sequences, and recognizing recurring digital signatures. Cybercrime detection is particularly dependent on such capabilities because the relevant evidence may be distributed across multiple devices, platforms, jurisdictions, and technical layers (Habibi & Rezaei, 2022). Research on cybercrime intention recognition further indicates that machine-learning and

language-processing methods may contribute to the identification of linguistic and behavioral indicators associated with malicious conduct (Kassa et al., 2024). These approaches can be useful in distinguishing ordinary communications from phishing attempts, fraudulent solicitations, coercive messages, coordinated deception, or other suspicious digital behavior. However, inference about intention is inherently more difficult than the classification of observable technical events. Systems can identify patterns associated with prior malicious conduct, but legal conclusions regarding intent must still be derived from the totality of evidence and evaluated by human decision-makers.

Natural language processing constitutes another important frontier. Police reports, witness statements, suspect interviews, judicial files, expert opinions, complaint narratives, intercepted communications, and online messages collectively produce vast quantities of textual evidence. Traditional investigation requires human readers to identify names, places, dates, events, relationships, inconsistencies, and recurring patterns across these materials. Natural language processing can accelerate this process by extracting entities, grouping semantically related documents, identifying recurring phrases, comparing accounts, and establishing links among separate cases. Large language models add more flexible forms of semantic search, summarization, information extraction, and question answering. Emerging research has demonstrated the potential of LLM-based systems for detecting complex social engineering scams by reconstructing crime scripts and evaluating the cognitive structure of deceptive interactions (Kim et al., 2026). This is especially relevant as social engineering increasingly exploits psychologically sophisticated and AI-generated communication. The capacity of generative AI to support more personalized and adaptive attacks has expanded the threat environment confronting investigators (Gonzaga et al., 2026). Accordingly, language models may become important both as defensive analytical systems and as objects of forensic scrutiny.

Nevertheless, generative artificial intelligence introduces evidentiary problems different from those associated with deterministic forensic tools. A conventional forensic instrument is generally expected to produce reproducible results when the same validated procedure is applied under the same conditions. Generative systems may produce variable outputs depending on model version, prompt design, parameter settings, contextual input, and probabilistic generation. This raises questions about reproducibility, traceability, and evidentiary confidence. Research examining confidence in AI-generated evidence in cybercrime investigations reflects growing concern about how investigators and other criminal justice professionals evaluate the reliability of outputs generated or interpreted through artificial intelligence (Vaidyan, 2025). An AI-generated summary of a digital record cannot safely substitute for the underlying record, and a model's inferred relationship between two pieces of evidence cannot become self-validating simply because it is computationally produced. Scientific crime detection requires preservation of source data, documentation of processing steps, validation of models, and the possibility of independent examination.

Graph analysis and relationship mapping constitute another major opportunity. Many contemporary crimes are organized through networks rather than isolated acts. Money laundering may involve chains of accounts, companies, intermediaries, and transactions; organized cybercrime may connect devices, digital identities, servers, communication channels, and cryptocurrency wallets; procurement fraud may involve relationships among contractors, officials, intermediaries, and financial beneficiaries. Artificial intelligence can organize such information into network structures and identify central nodes, unusual clusters, recurring associations, or hidden pathways. Community-level fraud and economic crime are strongly shaped by social networks and behavioral relationships, making relational analysis especially valuable in identifying how illicit activity is organized and sustained (Kolhe, 2024). Cognitive AI approaches to criminal profiling likewise demonstrate the potential value of integrating behavioral and relational information instead of examining evidentiary elements in isolation (Buele et al., 2026). Such systems can therefore assist investigators in developing hypotheses about organizational structure, but network centrality or statistical association must not be confused with legal participation in a criminal enterprise.

The procedural implications of these technologies are equally important. Artificial intelligence can shift crime detection from a predominantly reactive model toward a

more proactive analytical model. Traditional policing frequently begins after a complaint, discovery of an offense, or identification of a specific suspect. AI systems can continuously analyze permitted datasets for anomalies or patterns associated with ongoing criminal behavior. Financial systems can flag suspicious transactions as they occur; cyber monitoring can identify unusual network activity; intelligent video systems can detect specified events in real time; and analytical systems can reveal connections between a newly reported incident and earlier unsolved cases. The result is not necessarily prediction in the strong sense of knowing that a crime will occur, but earlier recognition of patterns that may justify lawful investigative attention. Literature concerning AI in criminal justice management illustrates how data-driven technologies are increasingly incorporated into management, investigation, and risk-oriented practices across criminal justice institutions (Talukder & Shompa, 2024). Such systems can reduce the amount of time investigators spend on repetitive data-processing tasks and allow greater attention to interpretation, interviewing, evidentiary evaluation, and investigative strategy.

Predictive policing represents the most controversial extension of this logic. Algorithms can analyze historical information to estimate areas, time periods, situations, or patterns associated with increased crime risk. Properly constrained, such analysis may assist in resource allocation by helping police determine where preventive presence or investigative capacity is most needed. Yet historical crime data are not neutral representations of actual criminality. They are partly records of previous policing choices, reporting practices, detection patterns, institutional priorities, and social inequalities. If an area was subjected to intensive policing in the past, it may contain more recorded offenses even where actual offending rates are not proportionately higher. An algorithm trained on those records may recommend further concentration of policing in the same area. The concern that AI systems may perpetuate bias is therefore not external to scientific crime detection; it concerns the validity of the data from which investigative conclusions are derived (Joseph, 2024). A scientifically responsible system must distinguish between the incidence of recorded crime and the broader phenomenon it claims to predict.

Artificial intelligence can also strengthen institutional coordination by enabling structured analysis across previously separated datasets. A criminal case may involve information held by police, prosecution authorities, forensic institutions, financial regulators, customs agencies, identity registries, telecommunications entities, and other organizations. Fragmented information can prevent investigators from recognizing relationships that become apparent only when datasets are legally and technically interoperable. AI-assisted entity resolution can help determine whether slightly different names, addresses, accounts, devices, or records may refer to the same person or event. Such integration, however, creates substantial privacy and security risks because centralized or interoperable criminal intelligence environments may contain highly sensitive personal information. Scientific efficiency cannot justify unrestricted institutional access. Access controls, legal authorization, logging, purpose limitation, data minimization, security safeguards, and accountability mechanisms must form part of the architecture itself.

The greatest conceptual mistake would therefore be to treat artificial intelligence as an autonomous investigator. AI does not possess legal responsibility, contextual understanding equivalent to experienced human investigation, moral judgment, or independent authority to determine whether coercive measures are justified. It can process evidence, classify information, identify patterns, estimate probabilities, and generate investigative suggestions. The decision to treat a person as a suspect, request a search, restrict liberty, initiate prosecution, or attribute criminal responsibility must remain governed by law and human judgment. The risks become more serious as AI systems grow more autonomous or are attributed capabilities that exceed their validated function. Scholarship concerning the criminal-law implications of advanced artificial intelligence emphasizes the need to anticipate risks associated with increasingly capable systems rather than assuming that technological sophistication automatically generates legal legitimacy (Mamak, 2024). Scientific crime detection is strengthened when AI extends human analytical capacity while remaining subject to evidentiary verification and institutional accountability.

3. Global Experiences in AI-Assisted Crime Detection

International experience demonstrates that artificial intelligence is not being introduced into criminal investigation according to a single institutional model. Different jurisdictions emphasize different combinations of technological innovation, surveillance capacity, data integration, procedural safeguards, regulatory control, and public accountability. These variations are important because the success of AI-assisted crime detection depends not merely on acquiring sophisticated algorithms but on embedding them within institutional arrangements capable of ensuring reliable data, professional competence, lawful access, technical security, and appropriate human supervision. Comparative experience also demonstrates that the same technological function may have substantially different legal implications depending on the surrounding regulatory environment. Facial recognition, predictive analytics, large-scale data integration, automated fraud detection, or AI-assisted profiling can serve legitimate investigative objectives, but the acceptable scope of their use depends upon the relationship between public security and individual rights established within each legal system.

European approaches are particularly significant because they tend to combine technological experimentation with relatively strong requirements concerning privacy, proportionality, transparency, and risk regulation. Police and security organizations in several European jurisdictions have explored artificial intelligence for analyzing CCTV footage, identifying persons or objects, processing digital evidence, detecting patterns across cases, and supporting resource allocation. Yet European policy increasingly treats many criminal justice applications of artificial intelligence as high-risk because they may affect liberty, privacy, equality, and procedural rights. This orientation illustrates an important lesson: legal regulation need not be treated as an obstacle that begins only after a technology has been deployed. Regulation can be incorporated into system design by requiring documentation, validation, human oversight, data-quality controls, traceability, and mechanisms for challenging automated outcomes. The broader literature on AI in criminal justice management supports this risk-sensitive approach by demonstrating that artificial intelligence affects not only operational efficiency but also institutional accountability and justice administration (Talukder & Shompa, 2024).

Biometric surveillance provides a clear example of the balance required in European and other rights-oriented systems. Intelligent facial or biometric recognition may help investigators search large volumes of visual data or identify persons sought in connection with serious offenses. Such systems can be particularly valuable where rapid identification is necessary or where manual examination of extensive surveillance archives would impose substantial delay. However, biometric identification operates on probabilistic similarity rather than infallible recognition. Its risks include false matches, unequal performance across demographic groups, function creep, and the transformation of targeted investigation into generalized surveillance. Research examining biometric surveillance and violent crime reduction emphasizes the potential utility of these technologies while simultaneously stressing the importance of protecting innocent persons (Haley, 2025). The comparative lesson is therefore not simply that biometric AI should or should not be used; it is that the legal conditions governing data collection, matching thresholds, confirmation procedures, retention, audit, and human verification materially determine whether the technology supports or undermines scientific investigation.

The United States provides a different model characterized by extensive technological experimentation combined with a more fragmented regulatory environment. American policing agencies and criminal justice institutions have been among the most visible users of predictive analytics, risk assessment, facial recognition, automated data analysis, and commercial investigative technologies. This environment has encouraged rapid innovation, but it has also generated some of the most prominent controversies regarding algorithmic bias and the opacity of proprietary systems. Predictive tools may appear objective because they express results numerically, but their outputs depend on training data, variable selection, model design, and institutional choices. The concern that crime prediction can reproduce entrenched social bias has become central to contemporary analysis of AI in criminal justice (Joseph, 2024). This experience demonstrates that mathematical formalization should

not be mistaken for neutrality. A model may consistently reproduce patterns contained in historical data while still producing unfair or epistemically misleading consequences.

American experience also shows why independent validation is essential. Criminal justice institutions may purchase systems developed by private technology providers whose internal methodologies are protected as commercial intellectual property. When such systems influence investigative attention or risk classification, secrecy can prevent defense lawyers, judges, researchers, and even police users from understanding why a particular output was generated. This creates a fundamental tension between commercial opacity and criminal procedural transparency. Scientific evidence ordinarily gains credibility from the possibility of testing, replication, methodological criticism, and peer evaluation. An algorithmic system that cannot be meaningfully examined because its design is inaccessible may therefore create difficulties when its output becomes relevant to evidentiary decisions. The emerging literature on confidence in AI-generated evidence reflects precisely this concern with whether criminal investigators can appropriately evaluate the reliability and limitations of computational outputs (Vaidyan, 2025). Comparative experience suggests that institutions should distinguish operational intelligence from evidence intended for courtroom use and subject the latter to substantially stronger validation and disclosure standards.

Predictive systems further reveal the problem of feedback loops. If police deployment is intensified in an area because historical records show higher crime levels, increased police presence may generate additional recorded offenses, arrests, and observations, which then reinforce the dataset used by the predictive system. An algorithm may consequently produce an internally coherent prediction while remaining partly dependent on the earlier enforcement patterns it is supposed to analyze objectively. Machine-oriented criminology increasingly recognizes that technologies do not merely observe crime but can influence how crime is categorized, measured, and institutionally produced as data (Campedelli, 2025). This insight is particularly important for countries considering the importation of predictive policing tools. Their validity cannot be assessed only through accuracy measures calculated against historically recorded outcomes. Policymakers must examine what those outcomes represent, how they were produced, and whether the system intensifies existing distortions.

Experience with economic crime demonstrates a more immediately transferable application of artificial intelligence. Financial institutions and regulatory systems generate structured data that are often more suitable for algorithmic anomaly detection than broad social prediction. AI-enabled financial crime detection can identify suspicious transactional patterns, relationships among accounts, unusual payment sequences, or deviations from established behavior (Rouhollahi, 2021). Banking and tax enforcement similarly benefit from the capacity to analyze high-volume records that would be impractical to inspect manually (Haghi & Raisi, 2023). Procurement fraud detection offers another example in which AI can identify irregular patterns across contracts, suppliers, transactions, pricing structures, and institutional relationships (Ezeji, 2024). These applications illustrate a broader principle for responsible adoption: artificial intelligence is often most defensible where it analyzes clearly defined data for specific anomalies and produces reviewable investigative leads, rather than where it assigns generalized criminal risk to individuals or communities.

Cybercrime has likewise become a major area of international AI deployment because the offense environment itself is digital. Artificial intelligence can support malware classification, intrusion detection, phishing analysis, behavioral anomaly detection, malicious communication identification, and large-scale processing of digital forensic evidence. Existing scholarship on AI-based cybercrime detection confirms the growing relevance of intelligent analytical systems for identifying complex cyber threats (Habibi & Rezaei, 2022). The development of cybercrime intention recognition demonstrates the increasing sophistication of this field, particularly where linguistic and behavioral evidence is used to infer malicious objectives (Kassa et al., 2024). At the same time, criminal actors can use generative artificial intelligence to produce convincing phishing messages, impersonation content, synthetic identities, and automated social engineering at greater scale (Gonzaga et al., 2026). Emerging LLM-based detection frameworks seek to respond by reconstructing

the sequence and cognitive logic of social engineering scams rather than merely searching for isolated suspicious words (Kim et al., 2026). This interaction between offensive and defensive AI indicates that criminal investigation must develop continuously rather than treating AI adoption as a one-time modernization project.

Deepfake-related offenses provide a further illustration of the rapidly changing evidentiary environment. Synthetic audio, images, and video can be used for fraud, harassment, impersonation, disinformation, extortion, or fabrication of apparent evidence. Criminal justice systems must therefore develop technical capacities not only to generate or analyze digital content but also to determine authenticity and preserve evidentiary integrity. Legal scholarship concerning criminal responsibility for AI-enabled deepfake crimes illustrates the difficulty of applying conventional responsibility structures to offenses facilitated by increasingly autonomous or generative systems (Hailtik & Afifah, 2024). The investigative consequence is equally important: visual or audio material can no longer be treated as inherently trustworthy merely because it appears realistic. Scientific crime detection increasingly requires authentication methods capable of identifying manipulation, tracing provenance, examining metadata, and evaluating whether content has been synthetically generated or altered.

Middle Eastern experience is relevant to Iran because several regional states have invested heavily in smart policing, integrated surveillance, digital public services, biometric identification, and centralized data infrastructures. The principal comparative value of these experiences lies less in copying particular systems than in recognizing the importance of infrastructure, centralized strategic planning, and specialized human capital. Artificial intelligence cannot function effectively where datasets are incompatible, records are incomplete, agencies cannot exchange authorized information securely, or users lack the expertise required to interpret model outputs. The adoption of AI in criminal justice therefore requires an institutional ecosystem rather than isolated software procurement. Literature emphasizing the broader social consequences of AI in criminology reinforces the point that technological transformation affects organizational practices, social relationships, and perceptions of legitimacy alongside technical efficiency (Teresia, 2024). A technologically advanced investigative system can lose public legitimacy if citizens perceive it as unaccountable or indiscriminately intrusive.

East Asian experiences, particularly highly integrated surveillance environments, demonstrate the technical possibilities created by combining dense sensor networks, biometric identification, extensive data integration, and computational analytics. From an investigative perspective, such systems can drastically reduce the time required to search for persons, trace movements, link events across locations, or detect patterns across extensive information networks. Yet these same capacities illustrate why localization must be constrained by the legal and constitutional characteristics of the receiving country. The fact that a technology is operationally effective in one institutional environment does not establish that the same intensity of surveillance is legally or socially acceptable elsewhere. Criminal justice technology embodies normative choices regarding privacy, suspicion, state authority, and acceptable risk. Comparative learning should therefore focus on technical architecture and regulatory lessons while avoiding the assumption that foreign institutional models can simply be transferred intact.

Cognitive artificial intelligence for criminal profiling represents another emerging international development. These systems attempt to synthesize behavioral, situational, psychological, and relational information in ways that support investigative reasoning. Recent scholarship on cognitive AI and criminal profiling suggests that such technologies can potentially improve the structured evaluation of complex behavioral evidence (Buele et al., 2026). Their legitimate value lies in hypothesis generation, case linkage, and analytical support rather than automated attribution of guilt. This distinction is especially important because profiling techniques may encourage confirmation bias if investigators treat algorithmically generated profiles as authoritative descriptions of offenders. The problem becomes even more serious when predictive systems attempt to infer future criminality from neurological, behavioral, or psychological characteristics. Theoretical research on AI and neuroprediction highlights the fundamental legal and ethical difficulties associated with using predictive claims about human behavior within criminal justice

(Deb, 2024). International experience therefore supports a general boundary: AI may strengthen the organization and interpretation of evidence, but predictions about persons must remain subject to strict scrutiny and cannot replace individualized proof.

The global experience also demonstrates that legal frameworks often develop more slowly than technological capability. New forms of AI-enabled offending, autonomous systems, synthetic media, and generative technologies challenge conventional definitions of authorship, causation, responsibility, and evidentiary authenticity. Research concerning legislative challenges in confronting crimes associated with artificial intelligence illustrates the difficulty of maintaining legal clarity in a rapidly changing technological environment (El-Mahrouki, 2024). Broader work on criminal risks in the age of artificial intelligence similarly emphasizes that AI can transform both offending opportunities and the mechanisms used to detect and respond to crime (Shen, 2024). The policy lesson is that regulation should be technologically informed but functionally defined. Legislatures should avoid rules tied so narrowly to a specific model or software architecture that they rapidly become obsolete. Instead, legal standards should focus on matters such as reliability, explainability, authorized use, data governance, human responsibility, evidentiary traceability, and independent oversight.

The comparative experience ultimately reveals several principles relevant to Iran. AI adoption should be gradual rather than indiscriminate; priority should be given to clearly defined use cases in which the benefits can be objectively evaluated; investigative outputs should remain reviewable by qualified humans; systems affecting individual rights require stronger safeguards than purely administrative tools; data quality must be treated as a legal as well as technical issue; models should undergo validation before operational use; procurement contracts should preserve sufficient transparency for audit and legal review; and algorithms should not acquire authority simply because they produce numerical or apparently scientific outputs. The strongest international lesson is that successful AI-assisted crime detection depends on institutional trustworthiness. Technical sophistication without governance can magnify investigative error, whereas careful integration can convert artificial intelligence into a valuable extension of scientific forensic practice.

4. Localization of AI-Assisted Scientific Crime Detection in Iran

Localization in Iran should begin from the recognition that the country already possesses important components of the institutional and informational environment required for AI-assisted crime detection. Police organizations increasingly operate digital systems for cybercrime investigation, electronic identification, traffic monitoring, and information management. Judicial institutions have developed electronic case-management and digital service infrastructures, while financial, identity, customs, taxation, banking, and administrative systems generate large quantities of structured data potentially relevant to the investigation of economic and organized crime. Iranian research has already identified the potential role of artificial intelligence in improving the process of crime detection (Mohammadinia & Alizadeh, 2023), and domestic work on computer-based crime analysis has highlighted the relevance of AI methods for analyzing criminal information (Keyvanpour et al., 2021). Research concerning banking and tax crimes also demonstrates domestic awareness of both the opportunities and the practical difficulties associated with AI-assisted detection (Haghi & Raisi, 2023). The principal challenge is therefore not the absence of technological potential but the need to transform fragmented capacities into a coherent, lawful, and scientifically validated investigative ecosystem.

The first localization requirement concerns data architecture. Artificial intelligence depends fundamentally on data quality, completeness, interoperability, and lawful accessibility. Criminal investigations may require information originating from police files, judicial records, forensic examinations, banking systems, identity databases, communications evidence, customs records, property information, tax records, or other administrative sources. If these systems remain technologically isolated, investigators cannot fully exploit relational analysis. Yet complete centralization of sensitive data would create severe security and privacy risks. Iran should therefore prioritize secure interoperability rather than indiscriminate accumulation. Authorized institutions

should be capable of querying relevant datasets through controlled technical gateways in which access is based on legal authority, institutional role, investigative purpose, and judicial permission where required. Every access request should be logged, attributable, and auditable. AI should operate within this controlled environment rather than becoming a justification for unrestricted cross-agency surveillance.

Financial and economic crime should be among the first priority areas for localization because these investigations involve structured and relatively well-defined datasets. Artificial intelligence can assist in identifying abnormal transaction sequences, unusual account relationships, repeated behavioral patterns, suspicious concentrations of payments, or networks of apparently separate entities. International research on AI-enabled financial crime detection provides a strong conceptual foundation for this use (Rouhollahi, 2021). Iranian research specifically concerning banking and tax crime likewise demonstrates the potential relevance of AI to these areas (Haghi & Raisi, 2023). Procurement fraud analysis may provide another suitable field because public procurement generates contractual, financial, organizational, and temporal data that can be examined for irregular relationships (Ezeji, 2024). Such systems should not automatically classify persons as criminals; their function should be to identify anomalies requiring professional investigation. This distinction can make AI both more effective and more legally defensible.

Cybercrime constitutes another major area for indigenous development. Iran possesses specialized cyber-policing capabilities and a substantial Persian-language digital environment that cannot be analyzed optimally through systems designed primarily for English-language content. Domestic development of Persian-language models for cybercrime detection could support phishing analysis, scam identification, classification of malicious communications, extraction of indicators from complaint narratives, and examination of large quantities of seized digital material. Iranian scholarship has already recognized AI's significance for detecting cybercrimes (Habibi & Rezaei, 2022). International research concerning cybercrime intention recognition demonstrates how computational models may assist in identifying malicious patterns within digital behavior and communication (Kassa et al., 2024). Emerging social-engineering detection models based on large language models show additional potential for reconstructing the stages and cognitive structure of scams (Kim et al., 2026). Such capabilities are particularly relevant in Persian because imported systems may fail to recognize culturally specific linguistic forms, colloquial expressions, deception strategies, or semantic patterns.

Localization must also address the growing challenge created by generative artificial intelligence. Social engineering, phishing, impersonation, synthetic identities, deepfakes, and automated fraud can increasingly be produced at scale and adapted to individual victims. AI-powered social engineering has created new attack vectors that combine technological automation with psychological manipulation (Gonzaga et al., 2026). Deepfake-enabled offending similarly complicates questions of authenticity and criminal responsibility (Hailtik & Afifah, 2024). Iranian investigative institutions therefore need domestic capabilities for synthetic-media detection, provenance analysis, linguistic assessment, metadata examination, and forensic verification of potentially manipulated content. This is not simply a cybersecurity issue. Deepfake material may enter ordinary criminal cases as purported evidence, and an inability to authenticate digital media can directly affect the reliability of fact-finding.

Biometric identification constitutes another field with substantial potential but equally substantial legal sensitivity. Existing camera networks and identification infrastructures can potentially support rapid searches for suspects, missing persons, stolen vehicles, or persons connected to serious offenses. International research suggests that biometric surveillance can contribute to crime reduction and offender apprehension when deployed under appropriate safeguards (Haley, 2025). In Iran, however, any expansion of biometric AI should be governed by clearly defined legal purposes, judicial authorization requirements where necessary, retention limits, accuracy thresholds, and procedures for human confirmation. A biometric match should function as an investigative lead rather than conclusive proof of identity. The distinction is essential because the consequences of a false match can be severe, particularly where automated outputs trigger coercive measures.

Explainability is perhaps the most important legal-technological requirement for Iranian localization.

Criminal investigation differs from many commercial applications of artificial intelligence because its outputs may contribute to searches, arrests, restrictions of liberty, prosecution decisions, or evidentiary arguments. A system that produces a risk score or identifies a suspect without providing a comprehensible basis may conflict with the requirement that criminal decisions remain reasoned and reviewable. The difficulty is particularly acute where complex deep-learning systems operate as black boxes. The problem of algorithmic bias further demonstrates why reviewability matters. Predictive systems may reproduce historical distortions within the data on which they are trained (Joseph, 2024). Scientific validity therefore requires more than predictive performance; investigators and courts must understand the variables influencing an output, the conditions under which the model was validated, its known error rates, and the limitations of the dataset used.

Iran should consequently prioritize explainable artificial intelligence for criminal justice rather than assume that the most technically complex model is necessarily the most appropriate. In many investigative contexts, a somewhat less accurate but interpretable model may be preferable to a highly complex system whose reasoning cannot be meaningfully reconstructed. Hybrid systems can combine statistical prediction with rule-based explanation, while model documentation can identify relevant variables, confidence levels, known limitations, and the basis for particular classifications. When AI is used to establish connections among cases, the system should be capable of identifying which data points generated the connection. When it flags a suspicious transaction, investigators should be able to determine which patterns made the transaction anomalous. When it identifies a visual match, users should receive a confidence measure and sufficient information to conduct independent verification. The objective is not to require algorithms to reason like judges but to ensure that human decision-makers remain capable of evaluating computational assistance.

Evidentiary admissibility must be addressed at the same time as technical development. AI-assisted evidence can take several different forms, and each requires different legal treatment. An algorithm may merely help an investigator locate an existing document, in which case the document itself remains the primary evidence. It may enhance an image, classify a fingerprint, compare biometric characteristics, identify a network connection, generate a transcription, or estimate the probability of a match. It may also generate new text or summaries through a language model. The further the system moves from locating existing evidence toward generating interpretative conclusions, the greater the need for methodological scrutiny. Research on confidence in AI-generated evidence illustrates the uncertainty that can arise when computational outputs enter cybercrime investigation (Vaidyan, 2025). Iranian criminal procedure therefore requires a clear distinction between AI-assisted discovery, AI-assisted forensic interpretation, and AI-generated analytical output.

A reliable evidentiary framework should require preservation of the original evidence, documentation of each automated processing stage, identification of the model and version used, recording of relevant parameters, preservation of system logs, and disclosure sufficient to permit meaningful challenge. Courts should be able to request expert evaluation of the system where an algorithmic output materially affects the prosecution case. Defense lawyers should have a meaningful opportunity to challenge reliability, data quality, error rates, or inappropriate model use. A claim that a system constitutes proprietary technology should not automatically prevent scrutiny where its output materially affects criminal liability or investigative coercion. The principle of equality of arms becomes difficult to maintain if the prosecution can rely upon an algorithmic system whose functioning the defense cannot examine.

Algorithmic auditing should therefore become a central institutional component of Iranian localization. Before an AI system is used operationally in police or prosecutorial investigations, it should undergo independent technical and legal evaluation. Audit should address accuracy, false-positive and false-negative rates, dataset representativeness, cybersecurity, robustness, explainability, discriminatory impact, model drift, and the compatibility of the intended use with criminal procedural law. The concern with bias is particularly significant in predictive systems because historical criminal justice datasets may reflect previous enforcement practices rather than neutral distributions of offending (Joseph, 2024). Cognitive AI systems used in profiling likewise require careful validation because

their apparent analytical sophistication may encourage users to attribute excessive authority to probabilistic assessments (Buele et al., 2026). A specialized criminal algorithm auditing body could establish minimum standards, approve specific use cases, maintain a registry of authorized systems, require periodic revalidation, and suspend models that demonstrate unacceptable error or bias.

Human oversight should be built into every consequential application. Artificial intelligence is most valuable as a decision-support system for investigators, forensic experts, prosecutors, and judges, not as an autonomous substitute for them. The system may identify a suspicious pattern, but a trained investigator must determine whether the pattern has an innocent explanation. It may find similarities between two offenses, but human analysis must establish whether the similarities are legally and factually meaningful. It may generate a suspect profile, but investigators must avoid confirmation bias and test alternative hypotheses. It may identify a potential biometric match, but identity must be independently verified. This is particularly important because advanced AI may encourage automation bias, in which users assume that a computational output is more reliable than their own professional judgment. Scholarship concerning artificial general intelligence and criminal law demonstrates why systems of increasing capability require correspondingly serious consideration of responsibility and control (Mamak, 2024). The allocation of legal responsibility must therefore remain unequivocally human and institutional.

Professional training is equally important. Judges, prosecutors, investigators, and forensic experts do not need to become machine-learning engineers, but they do need sufficient AI literacy to evaluate outputs critically. They should understand the difference between correlation and causation, classification and proof, prediction and certainty, training data and real-world populations, model confidence and evidentiary reliability, as well as false-positive and false-negative errors. Without such knowledge, even technically well-designed systems may be misused. Training should therefore combine legal education, forensic methodology, data literacy, privacy and cybersecurity, algorithmic bias, and practical exercises involving AI-assisted investigation. Specialized technical experts should also be trained to communicate computational findings in language comprehensible to legal professionals.

Localization also requires investment in secure computational infrastructure. Sensitive criminal data should not be routinely transmitted to external platforms or foreign cloud services whose data-retention, access, and security conditions cannot be adequately controlled. Iran therefore needs secure institutional computing environments capable of running forensic and analytical models internally. Offline or controlled models may be particularly important for confidential case information. Technical sovereignty in this context does not mean isolation from international scientific development; rather, it means maintaining effective control over sensitive criminal data while benefiting from global knowledge and validated open methodologies. Systems should be designed so that model updates, access permissions, data transfers, and user activity can be independently audited.

Legislative reform should accompany institutional development. The rapid expansion of artificial intelligence has created new challenges for criminal legislation worldwide (El-Mahrouki, 2024). Emerging AI-related risks also show that criminal justice rules must evolve alongside technological change (Shen, 2024). Iran requires clearer regulation concerning criminal data processing, algorithmic investigation, biometric analysis, automated profiling, AI-assisted digital evidence, and the limits of predictive policing. Legislation should be technologically neutral enough to remain applicable as models evolve while being specific about procedural safeguards. It should define permissible purposes, authorization requirements, oversight structures, documentation obligations, rights of challenge, and consequences for unlawful use.

A realistic Iranian strategy should therefore proceed incrementally. Initial deployment should prioritize applications with relatively clear benefits and manageable rights implications, such as digital forensic triage, financial anomaly detection, document classification, case linkage, cybercrime analysis, and administrative information extraction. More intrusive applications, including broad biometric surveillance, individualized crime prediction, and automated behavioral profiling, should face much stricter thresholds. Pilot programs should be independently evaluated before national deployment, and effectiveness

should be measured not only by the number of algorithmic alerts generated but by validated investigative outcomes, false-positive rates, resource savings, procedural fairness, and effects on citizens' rights. Localization will be successful only when technical effectiveness and legal legitimacy develop together.

5. Conclusion

Artificial intelligence is reshaping the conceptual and operational foundations of scientific crime detection. The principal change is not the replacement of conventional forensic science but its extension into an environment characterized by large-scale digital evidence, interconnected databases, complex financial relationships, continuous communications, extensive audiovisual records, and increasingly sophisticated technology-enabled offending. Conventional investigative techniques remain indispensable, but they are increasingly insufficient when investigators must examine millions of records, reconstruct relationships across multiple systems, identify subtle patterns within heterogeneous data, or respond rapidly to offenses occurring in digital environments. Artificial intelligence provides a means of expanding analytical capacity while preserving the scientific objective of reconstructing criminal events through evidence.

The most significant opportunities arise from the combination of several technological capabilities. Machine learning can classify large datasets and identify anomalous patterns. Computer vision can accelerate the examination of video and photographic evidence. Natural language processing can extract relationships, entities, inconsistencies, and recurring patterns from extensive textual records. Graph analysis can reveal hidden connections among persons, transactions, organizations, devices, and events. Digital forensic tools can prioritize large volumes of seized data and assist investigators in locating materials relevant to a case. AI-assisted financial analysis can reveal patterns that become visible only when transactions are evaluated collectively. These technologies can therefore reduce investigative delay, improve information organization, and enable the discovery of relationships that conventional methods might overlook.

The procedural contribution of artificial intelligence is equally important. AI can transform investigation from a sequence of isolated manual tasks into a more integrated analytical process. Different forms of evidence can be examined simultaneously, new incidents can be compared with historical cases, suspicious activities can be identified more rapidly, and investigative resources can be directed toward areas requiring greater attention. This can be particularly valuable in organized crime, cybercrime, money laundering, banking fraud, procurement fraud, serial offending, and other offenses characterized by complex networks or extensive records. Nevertheless, the value of AI lies in its capacity to assist the investigative process, not in its ability to replace the legal and professional judgment on which criminal justice depends.

The international experience demonstrates that technological sophistication alone does not guarantee legitimate or effective crime detection. Artificial intelligence can amplify the weaknesses of the institutions in which it is deployed. Poor-quality data produce unreliable outputs. Historically biased data can reproduce unequal enforcement patterns. Opaque systems can prevent meaningful scrutiny. Excessively broad surveillance can transform targeted investigation into generalized monitoring. Proprietary algorithms can obstruct the ability of defendants and courts to examine the basis of important conclusions. Generative systems can produce outputs that are difficult to reproduce or authenticate. Predictive technologies can create feedback loops in which earlier enforcement decisions become the basis for future intervention. These problems do not negate the value of artificial intelligence, but they show why scientific crime detection requires legal, methodological, and institutional safeguards.

The international comparison also demonstrates that different applications should not be treated as if they carry the same level of risk. AI used to sort large volumes of digital files, detect duplicate records, or identify abnormal financial transactions raises different concerns from AI used to classify individuals according to future criminal risk. A system assisting investigators in locating evidence is different from a system whose output becomes evidence. A facial-recognition search generating an investigative lead is different from treating the automated match as proof of identity. A language model summarizing existing records is different from a system generating interpretative allegations. Regulatory

design must reflect these distinctions rather than attempting to govern every form of artificial intelligence through a single undifferentiated rule.

For Iran, the opportunity is substantial. The country possesses extensive public-sector data, developing judicial digital infrastructure, specialized cybercrime institutions, financial monitoring systems, identification databases, surveillance technologies, and a growing domestic technological capacity. These resources provide the foundation for the gradual development of AI-assisted scientific crime detection. Yet they remain dispersed across institutions and governed by rules that were not designed for contemporary algorithmic analysis. Successful localization therefore requires more than the acquisition of software. It requires the construction of a national framework in which data, technology, law, institutional authority, and professional competence are coordinated.

The first priority should be secure and lawful data interoperability. Artificial intelligence cannot discover meaningful relationships across fragmented information if relevant institutions cannot exchange data when legally authorized. At the same time, the solution should not be unrestricted centralization. Sensitive criminal, financial, biometric, identity, and communications data require strict access controls. Iran should develop secure inter-agency gateways through which authorized queries can be conducted while preserving institutional responsibility, judicial supervision, purpose limitation, and complete access logs. Every use of sensitive data should remain traceable to an identified user, institutional authority, and legitimate investigative purpose.

The second priority should be the development of indigenous and explainable models. Iranian investigations operate within a Persian-language legal, cultural, and social environment that cannot be fully represented by models trained primarily on foreign datasets. Domestic language technologies should therefore be trained and evaluated using appropriate Persian legal texts, crime reports, cybercrime data, and other lawfully obtained materials. Localization should also extend to technical performance. Facial recognition, text analysis, fraud detection, and behavioral models should be validated against relevant domestic populations and conditions rather than assumed to function equally well after importation.

Explainability should become a foundational requirement wherever artificial intelligence materially affects investigative decisions. Investigators should know why a transaction has been classified as suspicious, why two cases have been linked, why a biometric match has been suggested, or which variables contributed to a risk classification. Courts and defense lawyers should have sufficient access to the methodology to examine its reliability when algorithmic outputs influence the evidentiary record. Scientific investigation is strengthened by transparency because transparency enables verification, criticism, correction, and accountability.

The third priority should be the establishment of a clear legal framework for AI-assisted evidence. Criminal procedure should distinguish between systems that merely help locate existing evidence and systems that produce new analytical conclusions. The original evidence must always remain preserved wherever technically possible. Processing steps should be documented. The version of the model, relevant parameters, date of analysis, user identity, input data, and resulting output should be recorded. Where an algorithmic analysis becomes materially relevant to criminal responsibility, independent expert examination should be possible. The use of artificial intelligence must never deprive defendants of the practical ability to challenge evidence used against them.

The fourth priority should be independent algorithmic auditing. A specialized national mechanism should evaluate AI systems before they are introduced into police, forensic, prosecutorial, or judicial practice. Validation should include accuracy, error rates, cybersecurity, data representativeness, explainability, robustness, discriminatory effects, and compliance with criminal procedural requirements. Approval should be limited to defined use cases, because a model validated for one purpose may not be reliable for another. Periodic reassessment should also be mandatory because algorithmic performance can change as data distributions, criminal behavior, institutional practices, and software versions evolve.

The fifth priority concerns human responsibility. Artificial intelligence should remain a decision-support mechanism throughout the cycle of scientific crime detection. No person should become a suspect solely because an algorithm has assigned a risk score. No

intrusive investigative measure should be justified solely by an uninterpretable automated output. No biometric match should be treated as conclusive without independent verification. No generated summary should replace examination of the underlying evidence. No predictive model should substitute statistical association for individualized suspicion. Investigators, prosecutors, forensic experts, and judges must retain both authority and responsibility for decisions affecting fundamental rights.

The sixth priority should be professional capacity building. Technical systems are only as reliable as the institutions and users surrounding them. Police investigators need to understand the limitations of algorithmic leads. Prosecutors need to evaluate whether AI-assisted evidence satisfies requirements of reliability and lawful acquisition. Judges need sufficient technological literacy to assess challenges to computational evidence. Forensic experts must be able to document and explain automated analytical processes. Defense lawyers require meaningful opportunities to question technical methodologies. Interdisciplinary training should therefore become a permanent element of professional development rather than a temporary response to technological modernization.

Iran should initially prioritize applications in which artificial intelligence can generate substantial investigative benefits without transferring excessive authority to automated systems. Financial anomaly detection, cybercrime analysis, digital forensic triage, document processing, case linkage, identification of repeated patterns, and controlled search of large evidentiary databases provide appropriate starting points. More intrusive technologies, including generalized biometric monitoring, predictive profiling of individuals, and automated assessments of criminal propensity, require substantially stronger justification and safeguards. The principle should be proportionality between the technological power of the system, the sensitivity of the data involved, and the legal consequences that may follow from its output.

Ultimately, the future of scientific crime detection should not be conceptualized as a competition between human investigators and artificial intelligence. The more appropriate model is one of structured cooperation in which machines perform tasks suited to large-scale computation while humans retain responsibility for interpretation, contextual understanding, evidentiary judgment, legal reasoning, ethical evaluation, and coercive decision-making. Artificial intelligence can identify patterns, but it cannot independently determine their legal meaning. It can calculate probabilities, but it cannot transform probability into guilt. It can connect information, but it cannot decide whether a citizen's rights should be restricted. It can assist in reconstructing events, but responsibility for the legitimacy of criminal investigation must remain with accountable human institutions.

The central opportunity for Iran is therefore not simply to introduce artificial intelligence into existing investigative structures, but to use the emergence of AI as an opportunity to modernize the broader architecture of scientific crime detection. Secure data integration, indigenous technological development, explainable models, robust evidentiary rules, independent auditing, professional training, cybersecurity, and human oversight should form parts of a single national strategy. If these elements develop together, artificial intelligence can increase the accuracy, speed, and analytical capacity of criminal investigation without displacing the principles of lawful evidence and fair procedure. If technological adoption proceeds without these safeguards, the same systems may magnify error, opacity, discriminatory patterns, and unjustified surveillance. Responsible localization therefore requires neither rejection of artificial intelligence nor uncritical technological enthusiasm. It requires a model in which AI is deliberately confined to the role for which it is most defensible: a powerful scientific and analytical instrument placed at the service of human investigators and judicial authorities, operating within clearly defined legal limits and subject to continuous verification, oversight, and accountability.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

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

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Buele, J., Miranda-Toapanta, D., & Rojas-Cañizares, D. (2026). Rethinking Criminal Profiling Through Cognitive Artificial Intelligence. *Frontiers in Artificial Intelligence*, *9*. https://doi.org/10.3389/frai.2026.1824060

Campedelli, G. M. (2025). A Criminology of Machines. https://doi.org/10.48550/arxiv.2511.02895

Deb, E. (2024). Exploring the Nuptial Bond Between Neuroprediction and AI in Criminal Justice: A Theoretical Review. https://doi.org/10.20944/preprints202405.0409.v2

El-Mahrouki, M. M. (2024). Legislative Industry Challenges in Confronting Artificial Intelligence Crimes. *Journal of Law and Sustainable Development*, *12*(4), e3566. https://doi.org/10.55908/sdgs.v12i4.3566

Ezeji, C. L. (2024). Artificial Intelligence for Detecting and Preventing Procurement Fraud. *International Journal of Business Ecosystem and Strategy (2687-2293)*, *6*(1), 63-73. https://doi.org/10.36096/ijbes.v6i1.477

Gonzaga, K., Serra, S., Gomes, M., & Malta, S. (2026). AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies. *Computers*, *15*(2), 128. https://doi.org/10.3390/computers15020128

Habibi, M. S., & Rezaei, Y. (2022). Application of Artificial Intelligence in Detecting Cybercrimes. *Criminological Legal Studies*, *3*(8).

Haghi, M., & Raisi, M. (2023). Examining the Challenges and Benefits of Using Artificial Intelligence in the Prevention and Detection of Banking and Tax Crimes. Brussels.

Hailtik, A. G. E., & Afifah, W. (2024). Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia. *Asian Journal of Social and Humanities*, *2*(4), 776-795. https://doi.org/10.59888/ajosh.v2i4.222

Haley, P. (2025). The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent. *Sensors*, *25*(10), 3160. https://doi.org/10.3390/s25103160

Joseph, J. (2024). Predicting Crime or Perpetuating Bias? The AI Dilemma. *Ai & Society*, *40*(4), 2319-2321. https://doi.org/10.1007/s00146-024-02032-9

Kahla, L. Z. (2024). Leveraging Artificial Intelligence for Crime Detection and Prevention. *International Journal of Scientific Research in Engineering and Management*, *08*(05), 1-5. https://doi.org/10.55041/ijsrem34207

Kassa, Y. W., James, J. I., & Belay, E. G. (2024). Cybercrime Intention Recognition: A Systematic Literature Review. *Information*, *15*(5), 263. https://doi.org/10.3390/info15050263

Keyvanpour, M., Javideh, M., & Ebrahimi, M. (2021). Computer-Based Crime Analysis Using Artificial Intelligence Methods. *Detective*, *4*(3).

Kim, H. S., Kim, C., Shin, S., & Kang, J. (2026). SCRIPTMIND: Crime Script Inference and Cognitive Evaluation for LLM-based Social Engineering Scam Detection System. https://doi.org/10.48550/arxiv.2601.13581

Kolhe, D. (2024). Crime and Fraud at the Community Level: Social Networking Understanding Into Economic Crimes and Psychology Motivations. *Journal of Social Sciences and Economics*, *3*(2), 109-128. https://doi.org/10.61363/g0kb2s44

Mamak, K. (2024). AGI Crimes? The Role of Criminal Law in Mitigating Existential Risks Posed by Artificial General Intelligence. *Ai & Society*, *40*(4), 2691-2701. https://doi.org/10.1007/s00146-024-02036-5

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.

Rouhollahi, Z. (2021). Towards Artificial Intelligence Enabled Financial Crime Detection. https://doi.org/10.48550/arxiv.2105.10866

Shen, Y. (2024). Research on Criminal Risks in the Age of Artificial Intelligence. *Journal of Artificial Intelligence Practice*, *7*(2). https://doi.org/10.23977/jaip.2024.070208

Talukder, K. A., & Shompa, T. F. (2024). Artificial Intelligence in Criminal Justice Management: A Systematic Literature Review. *Non Human Journal*, *1*(01), 63-82. https://doi.org/10.70008/jmldeds.v1i01.42

Teresia, J. N. W. (2024). Criminology and Social Impact in the Age of Artificial Intelligence [AI]. *East African Journal of Information Technology*, *7*(1), 221-239. https://doi.org/10.37284/eajit.7.1.2141

Vaidyan, V. M. (2025). Confidence Levels of Artificial Intelligence Generated Evidence in Cybercrime Investigations - A Survey. https://doi.org/10.21203/rs.3.rs-7401864/v1