Macrothink Institute™

International Journal of Social Science Research
ISSN 2327-5510
2026, Vol. 14, No. 3

Policy Requirements for Responsible AI Adoption in UAE Forensic Science Institutions

Ebtisam Abdulrahman Saleh Abdulrahman Alabdooli

Faculty of Technology Management and Business Universiti Tun Hussein Onn Malaysia, Malaysia

Sabariah Eni (Corresponding author)

Faculty of Technology Management and Business Universiti Tun Hussein Onn Malaysia, Malaysia

E-mail: saba@uthm.edu.my

Received: July 1, 2026 Accepted: September 4, 2026 Published: September 14, 2026

doi:10.5296/ijssr.v14i3.24036 URL: https://doi.org/10.5296/ijssr.v14i3.24036

Abstract

Artificial intelligence is increasingly relevant to forensic science because modern investigations involve large volumes of digital, biometric, chemical, visual, and documentary evidence. In the United Arab Emirates, AI adoption in forensic science aligns with national priorities for digital transformation, smart governance, public security, and AI-enabled government services. However, forensic science is a high-stakes domain in which technological efficiency must be balanced with legal admissibility, scientific validity, ethical responsibility, professional accountability, and public trust. This paper argues that responsible AI adoption in UAE forensic science institutions requires more than the acquisition of advanced tools. It requires a coherent policy framework that connects governance, validation, legal and ethical compliance, professional capability, stakeholder coordination, transparency, procurement standards, and continuous evaluation. Drawing on forensic AI literature, public-sector AI governance, and the UAE policy context, the paper identifies key policy requirements for responsible AI adoption in forensic institutions. It then organises these requirements into a five-pillar framework: AI governance and accountability, validation and scientific reliability, legal, ethical and evidential compliance, professional capability and human oversight, and stakeholder engagement and institutional coordination. The paper concludes that AI can support forensic capability in the UAE only when it is embedded within institutional systems that promote accuracy, fairness, accountability, transparency, and legally defensible practice.

Keywords: artificial intelligence, forensic science, UAE, AI governance, digital forensics, responsible AI, forensic policy, stakeholder engagement, legal admissibility

1. Introduction

Artificial intelligence has become an important part of contemporary discussions on forensic science, law enforcement, and criminal justice. AI systems can assist forensic professionals in processing complex evidence, identifying patterns, comparing biometric features, analysing digital traces, classifying substances, supporting image and video interpretation, and improving the speed of investigative decision-making (Ball, 2018; Choudhury et al., 2022; Ketsekioulafis et al., 2024). These capabilities are especially relevant in a period when forensic institutions are required to manage increasingly large and diverse forms of evidence, including mobile device data, CCTV footage, cybercrime artefacts, DNA profiles, toxicology results, fingerprints, voice recordings, and digital transaction records (Casey, 2021; Faehndrich et al., 2023).

In the United Arab Emirates, the relevance of AI in forensic science is strengthened by the country's broader national commitment to digital transformation and artificial intelligence. The UAE National Strategy for Artificial Intelligence 2031 aims to improve government performance, support smart digital systems, strengthen AI investment, and position the country as a leader in AI-enabled development (UAE Ministry of Artificial Intelligence, 2020, 2023). These national priorities create an enabling environment for AI adoption in security, policing, justice, and forensic science. Studies on AI readiness and digital transformation in the UAE and GCC context further suggest that institutional readiness, governance capacity, and strategic foresight are important factors shaping AI adoption in the public sector (Alsharqi et al., 2022; Othman & Al Mahaddi, 2023; Raed, 2020).

However, forensic science is not an ordinary technological setting. It is a domain where scientific analysis can influence criminal investigation, prosecution, judicial decision-making, individual rights, and public confidence in justice institutions. For this reason, the central policy question is not simply whether AI should be adopted in forensic science. The more important question is how AI should be adopted responsibly. AI tools may improve speed and efficiency, but they may also introduce new risks if they are poorly validated, legally unclear, biased, opaque, insecure, or misunderstood by users (Mavroeidis et al., 2022; Tian et al., 2022).

In forensic science, an AI-generated output cannot be treated as reliable merely because it is produced by an advanced system. It must be scientifically validated, explainable enough for forensic and legal scrutiny, integrated into chain-of-custody procedures, and subject to professional oversight (Veldhuis et al., 2022; Zhou & Xu, 2024). This paper argues that responsible AI adoption in UAE forensic science institutions requires a comprehensive policy framework. Such a framework should connect national AI ambitions with the operational realities of forensic practice. It should ensure that AI tools support forensic professionals rather than replace expert judgement. It should also ensure that AI adoption strengthens, rather than weakens, evidential reliability, ethical practice, procedural fairness, and institutional accountability.

The purpose of this paper is therefore to identify and explain the main policy requirements for responsible AI adoption in UAE forensic science institutions. The paper focuses on

governance, legal compliance, validation, professional learning, stakeholder engagement, data protection, procurement, transparency, and continuous evaluation. It presents AI adoption as an institutional transformation process rather than a purely technical upgrade.

2. AI and Forensic Science in the UAE Context

Forensic science has traditionally depended on expert examination of physical evidence, including fingerprints, DNA, toxicology, questioned documents, firearms, biological traces, and crime-scene materials. In recent years, forensic science has expanded into more digital and data-intensive areas. Digital forensics, cybercrime investigation, biometric comparison, multimedia analysis, and automated database searching are now central to many investigations (Casey, 2021; Faehndrich et al., 2023). This shift creates opportunities for AI because many forensic tasks involve classification, pattern recognition, anomaly detection, data filtering, and comparison across large datasets (Ball, 2018; Ketsekioulafis et al., 2024).

AI adoption in forensic science may support several institutional objectives. First, it may improve efficiency by helping forensic professionals process large volumes of evidence more quickly. Second, it may support consistency by applying structured analytical procedures to repetitive tasks. Third, it may improve investigative support by identifying patterns or links that are difficult to detect manually. Fourth, it may strengthen public security by improving the speed and quality of evidence analysis (Choudhury et al., 2022; Morán-Torres et al., 2025).

The UAE provides a particularly important context for discussing forensic AI. The country has invested strongly in digital government, smart policing, cybersecurity, and AI-supported public services. This strategic environment supports the development of AI-enabled forensic capabilities (Alsharqi et al., 2022; UAE Ministry of Artificial Intelligence, 2020, 2023). At the same time, UAE forensic institutions operate within a legal and institutional environment that requires careful attention to electronic evidence, data protection, cybercrime regulation, and public trust (Othman & Al Hammadi, 2023; Raed, 2020).

However, the benefits of AI are conditional. AI does not automatically produce better forensic outcomes. The value of AI depends on the quality of data, the validity of algorithms, the appropriateness of deployment, the competence of users, and the strength of institutional governance (Mavroeidis et al., 2022; Wang & Zhao, 2023). Forensic AI also raises difficult questions about explainability, bias, privacy, accountability, evidential admissibility, and professional responsibility (Leslie, 2023; Singh & Dastidar, 2023). These questions are especially important because forensic conclusions can affect suspects, victims, courts, investigators, and the wider public.

Therefore, UAE forensic institutions require clear policy requirements that define how AI should be selected, tested, used, monitored, explained, and governed.

3. Why Policy Requirements Are Necessary

Policy requirements are necessary because forensic AI operates at the intersection of technology, law, science, ethics, and public security. Without clear policies, AI adoption may

become fragmented, vendor-driven, inconsistent, or difficult to defend in legal settings. Responsible AI literature emphasises that trustworthy AI requires more than abstract ethical principles; it requires operational mechanisms for accountability, transparency, risk management, and verification (Brundage et al., 2022; Floridi et al., 2022; Ghosh et al., 2023; Jobin et al., 2019).

The first reason policy requirements are necessary is scientific reliability. Forensic evidence must be based on methods that are tested, valid, and reliable. If an AI tool is used to classify evidence, generate a match suggestion, prioritise digital artefacts, or support expert interpretation, the institution must know how well the tool performs under realistic conditions (Ketsekioulafis et al., 2024; Veldhuis et al., 2022). This includes information about error rates, false positives, false negatives, data limitations, and the conditions under which the system should not be used.

The second reason is legal defensibility. Forensic outputs may be used in investigations or courts. Therefore, AI-supported results must be explainable, documented, and compatible with evidentiary procedures (McNeive et al., 2020; Schroeder, 2019; Singh & Dastidar, 2023). If a forensic expert cannot explain how an AI-supported conclusion was produced, what the output means, and what its limitations are, the result may be difficult to defend.

The third reason is ethical responsibility. AI systems may produce unfair or biased outcomes if they are trained on unrepresentative data or used in inappropriate contexts. In forensic science, such risks are serious because they may affect individuals' liberty, reputation, and access to justice. Research on bias and fairness in AI has shown that algorithmic systems can produce unequal error patterns across populations or contexts if they are not carefully designed, tested, and monitored (Berk et al., 2021; Buolamwini & Gebru, 2018; Mehrabi et al., 2021). Ethical policies must therefore address fairness, accountability, transparency, privacy, proportionality, and human oversight.

The fourth reason is institutional consistency. Different forensic departments may use different tools, procedures, and documentation standards. Without a common policy framework, AI adoption may vary across laboratories, police units, and forensic disciplines. This can create inconsistency in quality assurance, reporting, procurement, and evaluation. Studies of AI implementation in public-sector and safety institutions indicate that institutional readiness, organisational learning, and stakeholder coordination are crucial for successful AI adoption (Kumar & Raj, 2023; Sivarajah et al., 2021; Tian et al., 2022).

The fifth reason is public trust. Forensic science depends not only on technical competence but also on confidence that evidence is handled fairly, professionally, and transparently. Responsible AI policy can help reassure courts, practitioners, policymakers, and the public that AI tools are used as controlled decision-support systems rather than unaccountable automated decision-makers (Bryson et al., 2014; Cath et al., 2018; Ghosh et al., 2023).

4. Core Policy Requirements for Responsible AI Adoption

4.1 Establish Forensic-Specific AI Governance Structures

The first policy requirement is the creation of forensic-specific AI governance structures. General AI policies are useful, but forensic science requires additional safeguards because of its legal and evidential consequences. UAE forensic institutions should establish internal AI governance committees or oversight boards that include forensic scientists, digital forensic experts, legal professionals, data protection specialists, cybersecurity experts, ethics representatives, and institutional leaders.

These governance structures should review AI tools before adoption, assess risks, approve use cases, define accountability, and monitor implementation. Public-sector AI governance literature suggests that responsible adoption requires clear institutional roles, transparent procedures, and mechanisms for evaluating risks and benefits (Ghosh et al., 2023; Sivarajah et al., 2021). In forensic science, governance structures should also distinguish between AI used for investigative support and AI used to support evidential conclusions. This distinction is important because a tool used for triage or lead generation may require different standards from a tool whose output is presented in court (Casey, 2021; Singh & Dastidar, 2023).

4.2 Require Validation Before Operational Use

The second policy requirement is mandatory validation before AI tools are used in forensic casework. Validation should examine whether the AI system performs accurately and reliably under the conditions in which it will be used. For example, a facial comparison system should be tested on relevant image qualities, lighting conditions, demographic characteristics, and operational scenarios. A digital forensic triage tool should be tested on realistic device types, file systems, languages, and data volumes.

Validation should not rely only on vendor claims. Vendors may provide useful technical information, but forensic institutions should require independent or institutionally supervised testing. Validation reports should include the purpose of the tool, testing data, performance metrics, limitations, failure conditions, and appropriate use boundaries (Brundage et al., 2022; Zhou & Xu, 2024). This requirement is especially important because forensic AI models may perform differently across datasets, populations, and operational environments (Han et al., 2023; Veldhuis et al., 2022).

4.3 Maintain Human Oversight and Expert Responsibility

The third policy requirement is strong human oversight. AI should support forensic experts, not replace them. Forensic professionals should remain responsible for interpreting AI outputs, assessing relevance, considering case context, and preparing reports. Policies should make clear that AI-generated outputs are not final forensic conclusions unless they have been reviewed, interpreted, and approved by qualified professionals.

Human oversight is especially important because AI systems can produce outputs that appear objective or precise while still being affected by poor data quality, bias, uncertainty, or inappropriate use. Human-in-the-loop approaches are increasingly recommended in criminal

justice and forensic AI contexts because they preserve professional judgement while allowing AI to support complex analytical tasks (Guttman et al., 2024; O'Neil et al., 2023). Policies should therefore guard against automation bias, where users over-trust AI results simply because they are produced by a technical system.

4.4 Ensure Explainability and Transparent Reporting

The fourth policy requirement is explainability and transparent reporting. Forensic professionals must be able to explain the role of AI in the analysis. This does not mean that every mathematical detail of a complex algorithm must be described in court. However, the institution should be able to explain the system's purpose, input data, general method, validation status, performance limitations, and the way the output was used.

Explainability is a major concern in forensic AI because legal actors must be able to understand, question, and evaluate AI-supported evidence (Gilpin et al., 2018; Leslie, 2023; Liu et al., 2024). Forensic reports should clearly state when AI was used. They should identify whether AI was used for screening, triage, comparison, classification, reconstruction, or evidential interpretation. Reports should also state the limitations of the AI-supported analysis and avoid overstating certainty (Veldhuis et al., 2022).

4.5 Protect Data Privacy and Security

The fifth policy requirement is strong data privacy and cybersecurity protection. Forensic AI systems may process sensitive information, including biometric data, personal communications, location data, medical information, images, videos, and criminal investigation records. Policies should define how data are collected, stored, accessed, transferred, anonymised, retained, and deleted. Privacy-preserving AI literature shows that smart public-sector systems require careful data governance because large-scale AI applications can create risks of misuse, surveillance overreach, or unauthorised access (Alamri et al., 2021; Wang & Zhao, 2023).

Cybersecurity is also essential. If forensic AI systems are connected to databases, cloud services, or external vendors, institutions must protect them from unauthorised access, tampering, data leakage, and adversarial attacks. Security failures in forensic systems can damage investigations, compromise evidence, and undermine trust (Broadhurst & Choi, 2023; Casey, 2021).

4.6 Preserve Chain of Custody and Auditability

The sixth policy requirement is chain-of-custody protection and auditability. AI tools should not create uncertainty about how evidence was handled. Every interaction with forensic data should be logged, including data input, processing steps, user actions, system outputs, changes, and review decisions. These logs should be secure, tamper-resistant, and available for internal review or legal scrutiny when required.

Auditability is particularly important in digital forensics, where AI tools may filter, prioritise, or classify large volumes of data. If an AI system excludes certain files from review or highlights specific artefacts, the institution must be able to explain and reproduce that process.

Data provenance and interoperability are therefore central requirements for responsible forensic AI (Li & Wang, 2024; Wang & Zhao, 2023; Zhou & Xu, 2024).

4.7 Develop AI-Specific Training and Certification

The seventh policy requirement is professional training. AI adoption will not succeed if forensic professionals do not understand how to use AI tools appropriately. Training should cover the purpose of AI systems, input requirements, output interpretation, limitations, error risks, ethical issues, legal responsibilities, and reporting standards.

Organisational learning theory suggests that institutions improve when they develop, retain, and transfer knowledge across people, processes, and routines (Argote, 2013). In forensic AI adoption, learning is especially important because professionals must adapt existing forensic workflows to new technological capabilities. Studies on barriers to AI implementation in forensic laboratories and public safety agencies show that training, institutional readiness, user confidence, and organisational support are key conditions for effective AI adoption (Kumar & Raj, 2023; Tian et al., 2022).

Training should not be limited to technical staff. Prosecutors, investigators, laboratory managers, legal professionals, and policymakers also need a basic understanding of forensic AI. This is because AI-supported evidence may move across different parts of the justice system. A shared understanding among stakeholders can reduce misinterpretation and improve confidence in AI-supported forensic practice.

4.8 Strengthen Stakeholder Engagement

The eighth policy requirement is stakeholder engagement. Responsible forensic AI cannot be developed by technical teams alone. It requires collaboration among forensic scientists, police authorities, legal actors, courts, policymakers, AI vendors, academic researchers, and public accountability bodies.

Stakeholder engagement helps ensure that AI tools are aligned with operational needs, legal standards, ethical expectations, and professional realities. Public value governance literature emphasises that institutions should create value through collaborative governance, legitimacy, accountability, and stakeholder participation (Bryson et al., 2014). In forensic AI, stakeholder engagement is also consistent with socio-technical systems theory, which argues that technology must be understood together with people, organisational structures, and institutional processes (Bostrom & Heinen, 1977).

For example, a tool that performs well in a laboratory setting may raise concerns about courtroom explanation, public trust, or cross-agency data sharing. Stakeholder engagement can help identify such concerns before implementation.

4.9 Establish Procurement Standards for AI Tools

The ninth policy requirement is responsible procurement. Forensic institutions should not purchase AI systems only on the basis of promised speed, innovation, or vendor reputation. Procurement standards should require vendors to provide documentation on model

development, training data, validation, limitations, update procedures, cybersecurity safeguards, bias testing, explainability, and support arrangements.

AI accountability literature emphasises the importance of verifiable claims, documentation, auditability, and responsible development practices (Brundage et al., 2022; Caruso et al., 2024). Contracts should also address institutional control over data, access to audit information, conditions for system updates, responsibilities for errors, and procedures for discontinuing or replacing systems. Vendor dependence is a serious risk if institutions cannot inspect, test, or explain the tools they use.

4.10 Implement Lifecycle Monitoring and Continuous Evaluation

The tenth policy requirement is continuous evaluation. AI systems may change over time because of software updates, new data, environmental changes, emerging crime patterns, or shifts in forensic workflows. A system that performs well at the time of adoption may become less reliable if conditions change.

Therefore, AI tools should be monitored throughout their lifecycle. Institutions should conduct regular audits, performance reviews, error analysis, user feedback exercises, and revalidation when systems are updated or used in new contexts. Continuous learning loops are especially important in AI-enabled public organisations because AI systems interact with changing institutional environments (Chen et al., 2023). In forensic contexts, lifecycle monitoring should be treated as a normal part of forensic quality assurance and risk management (Mavroeidis et al., 2022; Zhou & Xu, 2024).

5. Methodology

This study adopted a qualitative conceptual and policy-oriented methodology to examine the policy requirements for responsible artificial intelligence adoption in UAE forensic science institutions. The approach was appropriate because the study does not seek to test a specific AI tool or measure current adoption levels, but rather to develop a structured understanding of the governance, legal, ethical, scientific, and institutional conditions needed for responsible implementation. The study relied on a narrative review of academic literature, forensic science research, responsible AI scholarship, public-sector AI governance studies, and UAE policy materials related to artificial intelligence, digital transformation, smart governance, cybersecurity, and law enforcement innovation.

The reviewed literature was analysed thematically to identify recurring issues and policy needs associated with AI use in forensic contexts. Particular attention was given to themes such as AI governance, scientific validation, legal admissibility, ethical compliance, explainability, data protection, chain of custody, human oversight, procurement standards, professional training, stakeholder engagement, and continuous evaluation. These themes were then synthesised into ten core policy requirements and organised into a five-pillar framework covering AI governance and accountability, validation and scientific reliability, legal, ethical and evidential compliance, professional capability and human oversight, and stakeholder engagement and institutional coordination.

The methodology was both literature-informed and context-sensitive. It drew on international discussions of responsible AI and forensic reliability while also considering the UAE's national priorities for AI-enabled government, public security, and digital transformation. Since the study is conceptual, it did not involve primary data collection through interviews, surveys, or case studies. This is acknowledged as a limitation, and future research could extend the study by gathering empirical evidence from forensic scientists, investigators, legal professionals, policymakers, AI developers, and regulatory bodies in the UAE. Overall, the methodology enabled the study to translate broad responsible AI principles into a practical policy framework suitable for forensic science institutions in the UAE.

6. Proposed Policy Framework

Building on the ten policy requirements discussed in the previous section, this section proposes a five-pillar policy framework for responsible AI adoption in UAE forensic science institutions. The framework was developed through a process of thematic consolidation. The ten policy requirements were first identified from the literature on forensic AI, responsible AI governance, public-sector innovation, legal admissibility, ethical accountability, and forensic quality management. They were then grouped according to their main institutional function: governance, scientific reliability, legal and ethical compliance, professional capability, and stakeholder coordination. This process allowed the framework to move from a list of individual policy requirements to a more integrated institutional model.

The five pillars were therefore not selected arbitrarily. They represent broader categories that organise the ten policy requirements into a coherent structure. The first pillar, AI governance and accountability, consolidates requirements relating to governance structures, procurement standards, institutional responsibility, and lifecycle monitoring. The second pillar, validation and scientific reliability, reflects the requirement that AI tools must be tested, validated, documented, and monitored before and during forensic use. The third pillar, legal, ethical and evidential compliance, brings together requirements relating to explainability, privacy, data protection, legal admissibility, chain of custody, auditability, and ethical safeguards. The fourth pillar, professional capability and human oversight, incorporates the requirements for AI-specific training, expert review, human responsibility, and protection against automation bias. The fifth pillar, stakeholder engagement and institutional coordination, reflects the need for collaboration among forensic institutions, police authorities, legal actors, policymakers, vendors, researchers, and oversight bodies.

This framework also aligns with existing responsible AI governance models. Responsible AI literature commonly emphasises accountability, transparency, fairness, human oversight, privacy, safety, risk management, and continuous evaluation (Cath et al., 2018; Floridi et al., 2022; Ghosh et al., 2023; Jobin et al., 2019). These principles are reflected across the five pillars. For example, accountability is addressed through governance structures and defined institutional responsibilities; transparency is addressed through explainable reporting and auditability; fairness is addressed through bias testing and ethical review; human oversight is addressed through professional capability and expert responsibility; and risk management is addressed through validation, procurement controls, monitoring, and periodic evaluation. In

this way, the proposed framework translates general responsible AI principles into forensic-specific policy requirements.

The framework is also consistent with forensic quality assurance principles. Forensic science depends on validated methods, competent personnel, documented procedures, traceable evidence handling, impartial analysis, reliable reporting, and continuous quality improvement. These expectations are reflected in international laboratory and forensic quality frameworks, including ISO/IEC 17025 and the ISO 21043 series on forensic sciences (Miguel, Moreiraa, & Oliveira, 2021; Morrison et al., 2025).

The proposed framework adapts these quality assurance expectations to AI-supported forensic practice. Validation and scientific reliability correspond to method validation, performance assessment, and reproducibility. Professional capability and human oversight correspond to personnel competence and expert responsibility. Legal, ethical and evidential compliance corresponds to evidence integrity, chain of custody, auditability, and defensible reporting. Governance and lifecycle monitoring correspond to quality management, corrective action, risk management, and continuous improvement.

The framework is further grounded in UAE policy priorities. The UAE's national AI agenda emphasises digital transformation, smart government, public-sector innovation, security, competitiveness, AI investment, talent development, and responsible governance. These priorities create a supportive environment for AI adoption in forensic science, but they also require institutional safeguards to ensure that AI is used in ways that protect public trust, legal reliability, and professional accountability. The proposed framework therefore connects national AI ambitions with the operational realities of forensic science. It recognises that AI-enabled forensic capability should not be measured only by technological sophistication or speed, but also by validity, transparency, accountability, lawful practice, professional competence, and institutional coordination.

As shown in Figure 1, the proposed framework consists of five interconnected pillars: AI governance and accountability; validation and scientific reliability; legal, ethical and evidential compliance; professional capability and human oversight; and stakeholder engagement and institutional coordination. These pillars are supported by four cross-cutting foundations: data governance, chain of custody, auditability, and continuous evaluation. These foundations cut across all five pillars because they are necessary for every stage of responsible forensic AI adoption, from tool selection and data processing to expert interpretation, reporting, review, and long-term monitoring.

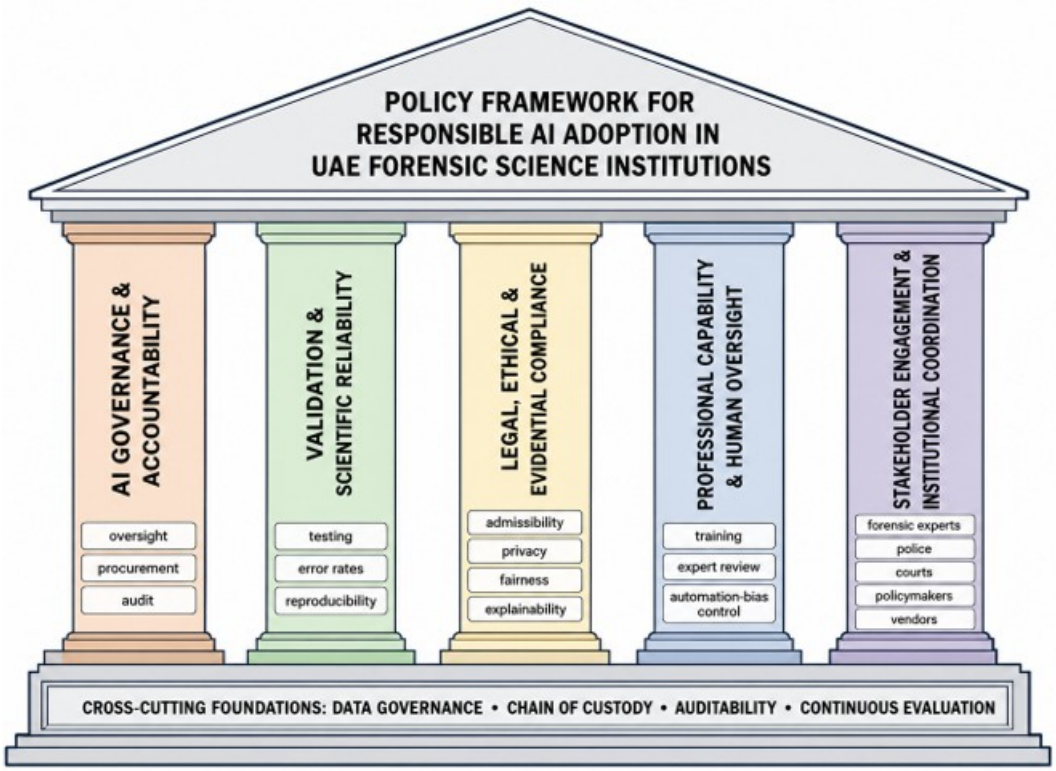

Figure 1. Policy framework for responsible AI adoption in UAE forensic science institutions

The first pillar is AI governance and accountability. Since AI systems used in forensic science may influence investigative decisions and evidential interpretation, institutions must clearly define who is responsible for approving, monitoring, reviewing, auditing, and discontinuing such systems. Governance should include legal, technical, ethical, cybersecurity, data protection, and forensic expertise so that AI-related decisions are not driven by technological considerations alone. This pillar includes internal AI governance committees, risk assessment procedures, procurement controls, tool registers, approval processes, and post-deployment review mechanisms. Clear accountability structures are necessary to ensure that AI systems are used responsibly, transparently, and consistently across forensic disciplines (Ghosh et al., 2023; Sivarajah et al., 2021).

The second pillar is validation and scientific reliability. Because forensic evidence must be scientifically defensible, AI tools should be validated before operational use, tested under realistic forensic conditions, and monitored throughout their lifecycle. Validation should include evidence on accuracy, error rates, reproducibility, limitations, uncertainty, data suitability, and conditions of appropriate use. Vendor claims should not be accepted without independent or institutionally supervised assessment. This pillar reflects the forensic quality assurance principle that methods used in casework must be reliable, documented, and fit for purpose. Without validation, AI may increase analytical speed but weaken evidential reliability, legal defensibility, and professional confidence (Ketsekioulafis et al., 2024; Veldhuis et al., 2022; Zhou & Xu, 2024).

The third pillar is legal, ethical and evidential compliance. Since forensic AI operates within the justice system, its use must comply with legal standards, ethical principles, and evidential requirements. AI-supported outputs should respect privacy, fairness, proportionality, accountability, transparency, human rights, data protection, and legal admissibility. Institutions should ensure that AI-generated or AI-assisted findings can be explained, challenged, reviewed, and defended in investigative and judicial contexts. This pillar also includes chain-of-custody protection, audit logs, secure data handling, disclosure of AI use in forensic reports, and avoidance of overstated certainty. It is essential because forensic AI must not only be technically useful, but also lawful, ethical, proportionate, and evidentially reliable (Cath et al., 2018; Floridi et al., 2022; Singh & Dastidar, 2023).

The fourth pillar is professional capability and human oversight. Since AI should support rather than replace forensic expertise, forensic professionals must be trained to understand AI tools, interpret their outputs, recognise their limitations, and avoid over-reliance. Continuous professional development should address AI functionality, uncertainty, validation results, bias, explainability, ethical risks, data protection, evidential implications, and automation bias. Human oversight ensures that qualified professionals remain responsible for reviewing AI outputs, interpreting results in case context, and making final forensic conclusions. This pillar is particularly important because AI outputs may appear objective or authoritative even when they are affected by data limitations, model uncertainty, or inappropriate use (Argote, 2013; O'Neil et al., 2023; Tian et al., 2022).

The fifth pillar is stakeholder engagement and institutional coordination. Responsible forensic AI cannot be implemented by forensic laboratories alone. It requires coordination among forensic institutions, law enforcement agencies, prosecutors, courts, policymakers, regulators, AI vendors, academic researchers, cybersecurity specialists, and public accountability bodies. Stakeholder engagement helps ensure that AI systems are aligned with operational needs, legal requirements, ethical expectations, courtroom realities, and national policy objectives. It also strengthens shared understanding, professional trust, institutional legitimacy, and public confidence in AI-supported forensic evidence (Bostrom & Heinen, 1977; Bryson et al., 2014).

In addition to these five pillars, the framework includes four cross-cutting foundations. Data governance ensures that forensic data are collected, stored, accessed, processed, shared, retained, and deleted securely and lawfully. Chain of custody protects the integrity and traceability of evidence throughout AI-supported analysis. Auditability ensures that AI-related decisions, system outputs, user actions, model updates, and review decisions can be examined and reproduced when necessary. Continuous evaluation ensures that AI systems remain reliable, fair, secure, and suitable as technologies, datasets, forensic practices, crime patterns, and legal expectations evolve.

Overall, the proposed framework shifts AI adoption in forensic science from a narrow technology-acquisition model toward a broader institutional governance model. It demonstrates how the ten policy requirements can be organised into five mutually reinforcing pillars that reflect responsible AI governance principles, forensic quality assurance

expectations, and UAE national AI priorities. For UAE forensic science institutions, the framework provides a policy-oriented foundation for integrating AI in a way that supports forensic accuracy, operational efficiency, transparency, legal defensibility, professional responsibility, and public trust.

Table 1. Consolidation of ten policy requirements into the five framework pillars

Consolidated framework pillar	**Ten policy requirements**	**Rationale for consolidation**
AI governance and accountability	Establish forensic-specific AI governance structures	This requirement defines the institutional structures, roles, approval mechanisms, and accountability arrangements needed to govern AI use in forensic institutions.
	Establish procurement standards for AI tools	Procurement is part of governance because it determines how AI systems are selected, assessed, approved, contracted, and controlled before adoption.
	Implement lifecycle monitoring and continuous evaluation	Continuous evaluation supports governance by ensuring that AI systems remain reliable, accountable, and suitable after deployment.
Validation and scientific reliability	Require validation before operational use	Validation directly supports scientific reliability by requiring evidence of accuracy, error rates, reproducibility, limitations, and fitness for forensic use.
Legal, ethical and evidential compliance	Ensure explainability and transparent reporting	Explainability and disclosure are necessary for legal scrutiny, ethical transparency, evidential interpretation, and courtroom defensibility.
	Protect data privacy and security	Privacy and cybersecurity safeguards ensure that forensic AI systems comply with legal, ethical, and institutional responsibilities for sensitive data.
	Preserve chain of custody and auditability	Chain of custody and auditability protect evidence integrity, traceability, reproducibility, and legal defensibility throughout AI-supported analysis.
Professional capability and human oversight	Maintain human oversight and expert responsibility	Human oversight ensures that AI supports, rather than replaces, professional judgement and that qualified forensic experts remain responsible for conclusions.
	Develop AI-specific training and certification	Training builds the professional competence needed to interpret AI outputs, recognise limitations, avoid automation bias, and apply AI responsibly.
Stakeholder engagement and institutional coordination	Strengthen stakeholder engagement	Stakeholder engagement supports coordination among forensic institutions, police, courts, policymakers, vendors, researchers, and oversight bodies.

This consolidation shows that the five pillars were derived by grouping the ten policy requirements according to their dominant institutional function. Governance-related requirements were grouped under AI governance and accountability; scientific testing requirements were grouped under validation and scientific reliability; legal, ethical, privacy, explainability, and evidential integrity requirements were grouped under legal, ethical and evidential compliance; professional learning and expert responsibility requirements were grouped under professional capability and human oversight; and collaboration requirements were grouped under stakeholder engagement and institutional coordination. This structure strengthens the framework by showing that the pillars are not arbitrary categories, but a systematic synthesis of the policy requirements identified in the literature and adapted to the UAE forensic science context.

7. Practical Recommendations for UAE Forensic Institutions

Having established the five-pillar policy framework in the previous section, this section translates the framework into practical institutional actions for UAE forensic science institutions. The purpose of these recommendations is to move from policy design to implementation by identifying concrete measures that can be embedded into daily forensic practice, procurement, validation, reporting, training, auditing, and inter-agency coordination.

Responsible AI adoption requires more than broad policy commitment. It requires clear procedures, documented responsibilities, professional capacity, and continuous oversight to ensure that AI systems are used in a scientifically reliable, legally defensible, ethically responsible, and operationally effective manner. The following recommendations therefore operationalise the proposed framework by specifying how UAE forensic institutions can implement responsible AI adoption in a structured and sustainable way.

First, UAE forensic institutions should develop internal AI governance guidelines specifically for forensic science. These guidelines should define the approved and prohibited uses of AI, classify AI applications according to risk level, and specify the procedures required before AI tools are used in forensic casework. They should also clarify institutional responsibilities for approval, monitoring, documentation, review, and accountability. Such guidelines would help ensure that AI adoption is not left to individual departments or vendors but is managed through a consistent institutional governance process.

Second, institutions should establish a formal AI tool register. This register should list all AI systems used in forensic work, including their purpose, forensic application area, validation status, authorised users, data requirements, update history, risk classification, and responsible unit. The register should also record whether the tool is used for investigative support, screening, triage, analysis, or evidential reporting. Maintaining such documentation would strengthen transparency, auditability, institutional memory, and responsible control over AI systems (Brundage et al., 2022; Caruso et al., 2024).

Third, forensic laboratories should require validation reports before AI tools are used in operational casework. These reports should provide evidence on accuracy, reliability, error rates, reproducibility, limitations, and conditions of appropriate use. Validation should be

conducted or reviewed by qualified internal experts, independent specialists, or approved external bodies. This recommendation is especially important because forensic AI tools may perform differently across datasets, case types, image qualities, languages, populations, and operational environments. Requiring validation reports would reduce the risk of relying on untested or poorly understood AI systems.

Fourth, AI-supported forensic reports should include clear disclosure statements. These statements should explain whether AI was used, what role it played in the analysis, and whether the AI output was used for screening, comparison, classification, prioritisation, reconstruction, or expert interpretation. Reports should also indicate the limitations of the AI-supported analysis and confirm that qualified forensic professionals reviewed the output. This would improve transparency and help legal actors, courts, investigators, and other stakeholders understand the evidential role of AI in forensic conclusions.

Fifth, institutions should develop AI-specific training and professional development programmes for forensic professionals, investigators, managers, and relevant legal stakeholders. Training should not focus only on technical operation. It should also address AI limitations, uncertainty, bias, explainability, evidential implications, ethical risks, data protection, and automation bias. Forensic professionals should be trained to understand when AI outputs are useful, when they require caution, and when they should not be relied upon. Continuous training would strengthen professional confidence, reduce misuse, and support responsible human oversight (Argote, 2013; O'Neil et al., 2023).

Sixth, procurement teams should apply responsible AI procurement checklists before acquiring or approving AI tools. These checklists should require vendors to provide information on model development, training data, validation procedures, bias testing, explainability features, cybersecurity safeguards, update mechanisms, data ownership, and compatibility with existing forensic workflows. Procurement contracts should also address vendor accountability, access to technical documentation, post-deployment support, and procedures for auditing or discontinuing the system. This would help prevent vendor dependence and ensure that AI tools are selected based on forensic suitability rather than technological novelty alone.

Seventh, forensic institutions should establish periodic audits and lifecycle monitoring mechanisms for AI systems. These audits should examine system performance, user behaviour, error patterns, data quality, compliance with procedures, update history, and continued suitability for operational use. AI systems should be re-evaluated when software is updated, when the operating environment changes, or when the tool is used for a new forensic purpose. Periodic auditing would ensure that AI tools remain reliable, explainable, and aligned with legal and professional expectations over time.

Eighth, UAE forensic institutions should strengthen partnerships with universities, research centres, technology providers, legal bodies, and oversight authorities. Such partnerships can support independent validation, professional training, policy refinement, and research on emerging forensic AI risks. Collaboration with academic and legal stakeholders would also help institutions keep pace with technological developments while maintaining scientific and

evidential standards. This recommendation is consistent with public value governance and stakeholder engagement approaches to public-sector innovation, which emphasise collaboration, legitimacy, and shared accountability (Bryson et al., 2014; Ghosh et al., 2023).

Overall, these recommendations provide an operational pathway for implementing the proposed policy framework. They show that responsible AI adoption in UAE forensic institutions requires coordinated action across governance, documentation, validation, reporting, training, procurement, auditing, and stakeholder collaboration. By implementing these recommendations, UAE forensic institutions can strengthen the reliability, transparency, legal defensibility, and public trustworthiness of AI-supported forensic practice.

8. Discussion

Responsible AI adoption in forensic science requires a shift in thinking. AI should not be viewed only as a tool for speed, automation, or technical modernisation. It should be understood as part of a wider socio-technical system involving people, procedures, legal standards, data, institutions, vendors, courts, and public expectations (Bostrom & Heinen, 1977; Guttman et al., 2024). This is particularly important in the UAE, where national ambitions for AI-enabled governance, smart public services, security innovation, and digital transformation create strong incentives for forensic institutions to adopt advanced AI tools (UAE Ministry of Artificial Intelligence, 2020, 2023). However, the forensic context is high-stakes because AI-supported outputs may influence criminal investigations, evidential interpretation, prosecution decisions, judicial reasoning, individual rights, and public trust. For this reason, responsible AI adoption requires not only institutional readiness, but also careful management of several tensions and trade-offs.

The first major tension concerns transparency versus proprietary AI systems. Many AI tools used in biometric analysis, digital forensics, image enhancement, pattern recognition, or automated classification may be developed by commercial vendors. These systems may offer advanced capabilities, but their underlying models, training data, source code, and performance limitations may not be fully available to forensic institutions or courts. This creates a challenge for forensic accountability. On the one hand, vendors may argue that technical secrecy is necessary to protect intellectual property, cybersecurity, and commercial competitiveness. On the other hand, forensic science requires methods that can be explained, tested, challenged, and defended in legal settings. If an institution cannot explain how an AI system works, how it was validated, what its error rates are, and under what conditions it may fail, the evidential value of AI-supported outputs may be weakened. Therefore, UAE forensic institutions should not treat vendor reputation or technological sophistication as sufficient evidence of reliability. Procurement and governance policies should require documentation, validation evidence, audit access, explainability information, performance limitations, and clear procedures for independent review. In this way, transparency does not necessarily require complete disclosure of proprietary source code, but it does require enough information for scientific evaluation, legal scrutiny, and institutional accountability.

A second tension concerns efficiency versus legal defensibility. AI can improve forensic efficiency by processing large volumes of digital, biometric, chemical, visual, and

documentary evidence more quickly than manual methods. This is especially valuable in contemporary investigations involving mobile phones, CCTV footage, cybercrime data, DNA profiles, financial transactions, and online communications. However, speed alone cannot be the main measure of forensic value. A rapid AI-generated result may create investigative momentum, but it may also create legal vulnerability if the process is not validated, documented, reproducible, or explainable. In forensic science, efficiency must therefore be balanced with evidential defensibility. A tool that accelerates case processing but produces outputs that cannot be defended in court may ultimately weaken, rather than strengthen, justice outcomes. The proposed framework addresses this tension by requiring validation, chain-of-custody protection, auditability, disclosure of AI use, and professional review. These requirements may slow adoption in the short term, but they strengthen long-term reliability, courtroom confidence, and institutional legitimacy.

A third tension concerns automation versus expert judgement. AI systems may assist forensic professionals by identifying patterns, ranking evidence, suggesting similarities, classifying artefacts, or highlighting anomalies. However, these capabilities may also create risks of automation bias, where practitioners place excessive confidence in AI outputs because they appear objective, mathematical, or technologically advanced. This risk is particularly important in forensic science because expert judgement remains central to interpreting evidence in context. AI systems do not understand legal relevance, case circumstances, alternative explanations, or the broader meaning of evidence in the same way as trained forensic professionals. Therefore, AI should be used as decision support rather than as an autonomous decision-maker. Human oversight must be substantive rather than symbolic. Forensic experts should be trained to question AI outputs, understand uncertainty, recognise limitations, and document how AI-assisted results were interpreted. This does not mean rejecting automation; rather, it means ensuring that automation strengthens expert analysis without displacing professional responsibility.

A fourth tension concerns innovation versus privacy protection. Forensic AI often depends on large volumes of sensitive data, including biometric identifiers, facial images, fingerprints, DNA-related information, voice samples, location records, mobile device data, communications, medical information, and criminal investigation files. The more data AI systems can access, the more powerful they may become for investigative and analytical purposes. However, expanded data use also increases risks of privacy intrusion, surveillance overreach, unauthorised access, data leakage, secondary use, and public mistrust. This tension is especially significant in AI-enabled public security environments, where institutional pressure to innovate may conflict with the need to protect individual rights and data confidentiality. Responsible forensic AI policy must therefore embed privacy protection into the design, procurement, deployment, and monitoring of AI systems. Data minimisation, access controls, lawful processing, retention limits, cybersecurity safeguards, anonymisation where appropriate, and clear rules on data sharing should be treated as core forensic AI requirements rather than administrative afterthoughts.

These tensions show that responsible AI adoption is not simply a matter of choosing between technology and regulation. Instead, forensic institutions must develop governance

arrangements that allow innovation while controlling risk. Excessive restriction may prevent useful AI tools from improving forensic capacity, but uncritical adoption may undermine legal defensibility, ethical responsibility, and public confidence. The central policy challenge is therefore to create a balanced model of responsible innovation. This means allowing AI to support forensic speed, scale, and analytical capability while ensuring that every use remains scientifically valid, legally defensible, ethically justified, professionally supervised, and institutionally accountable.

The policy approach proposed in this paper recognises that AI value depends on institutional readiness. Advanced technology alone is insufficient. Forensic institutions need trained professionals, validated tools, clear documentation, legal safeguards, stakeholder engagement, procurement controls, data governance, and continuous evaluation (Kumar & Raj, 2023; Sivarajah et al., 2021; Tian et al., 2022). This approach supports responsible innovation by embedding AI within forensic quality assurance systems rather than treating it as a separate technological upgrade. Ethical principles such as transparency, accountability, fairness, privacy, and human oversight must therefore be translated into operational procedures. Transparency should become AI-use disclosure and explainable reporting. Accountability should become clear responsibility for AI-supported conclusions. Fairness should become bias testing and performance monitoring. Privacy should become controlled data governance. Human oversight should become documented expert review. Continuous improvement should become lifecycle evaluation and revalidation.

A key implication for UAE forensic science institutions is that AI adoption should be guided by proportionality. Not every AI use carries the same level of risk. AI used for administrative sorting or preliminary triage may require different controls from AI used to support evidential conclusions in court. Similarly, AI used for investigative lead generation should be clearly distinguished from AI used in formal forensic reporting. A risk-based approach would allow institutions to encourage innovation while applying stronger safeguards to high-impact applications. This is particularly important in the UAE context, where national AI priorities encourage rapid digital transformation, but forensic institutions must still maintain scientific reliability, legal admissibility, ethical responsibility, and public trust.

Overall, the discussion highlights that responsible forensic AI adoption involves managing competing institutional values rather than simply applying technology. Transparency must be balanced with proprietary innovation, efficiency with legal defensibility, automation with expert judgement, and innovation with privacy protection. The proposed framework provides a way to manage these trade-offs by connecting AI governance with validation, evidential compliance, professional oversight, stakeholder coordination, data governance, auditability, and continuous evaluation. For UAE forensic science institutions, this balanced approach can help ensure that AI strengthens forensic capability while protecting the integrity of the justice process.

9. Conclusion

AI has significant potential to support forensic science in the UAE, particularly in digital forensics, biometric analysis, toxicology, crime-scene reconstruction, and investigative

decision support. However, the use of AI in forensic science must be approached with caution because AI-supported outputs may influence investigations, prosecutions, judicial decisions, individual rights, and public trust.

This paper has argued that responsible AI adoption in UAE forensic science institutions requires more than the acquisition of advanced technologies. It requires an integrated policy framework that connects AI governance, scientific validation, legal and ethical compliance, professional capability, stakeholder coordination, data governance, auditability, and continuous evaluation. The proposed five-pillar framework provides a structured approach for translating responsible AI principles into practical institutional requirements.

The paper also offered practical recommendations for UAE forensic institutions, including the development of internal AI governance guidelines, AI tool registers, validation reports, disclosure statements, training programmes, responsible procurement checklists, periodic audits, and institutional partnerships. These recommendations show how responsible AI adoption can be embedded into everyday forensic workflows rather than treated as a separate technological initiative.

Overall, the main conclusion is that AI adoption in forensic science should be understood as an institutional governance challenge rather than a purely technological project. AI can support forensic accuracy, operational efficiency, transparency, and legal defensibility only when it is implemented within systems that protect scientific reliability, ethical responsibility, human oversight, and public trust. For the UAE, such an approach can help align forensic AI adoption with national digital transformation goals while safeguarding the integrity of forensic science and the justice process.

References

Ain, A. K., & Ross, A. (2023). *Biometrics: Personal identification in networked society*. AI & Society.

Al-Ghamdi, S., et al. (2019). AI integration in law enforcement: Challenges and opportunities. *International Journal of Law Enforcement and Criminal Justice*, *8*(1), 45–58.

Alamri, A., et al. (2021). Privacy-preserving in AI system for smart city applications: Taxonomy, challenges, and solutions. *Sustainable Cities and Society*, *74*, 103214.

Alsharqi, A., AlMarashda, A., & Al Hammadi, F. (2022). Strategic foresight and diffusion of AI in the UAE's public sector. *Government Information Quarterly*, *39*(3), 101746.

Argote, L. (2013). *Organizational Learning: Creating, Retaining, and Transferring Knowledge*. Springer. https://doi.org/10.1007/978-1-4614-5251-5

Ball, R. (2018). The role of machine learning in modern forensic science. *Forensic Science International*, *284*, 22–27.

Berk, R., Heidari, H., Jabbari, S., Kearns, M., & Roth, A. (2021). Fairness in criminal justice risk assessments: The state of the art. *Sociological Methods & Research*, *50*(1), 3–44. https://doi.org/10.1177/0049124118782533

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. *MIS Quarterly*. https://doi.org/10.2307/248710

Brantingham, P. J., Mohler, G., Wang, W., & Short, M. B. (2021). From predictive policing to precision policing: Ethical challenges and technological progress. *Annual Review of Criminology*, *4*(1), 111–132.

Broadhurst, R., & Choi, K. (2023). *AI in digital forensics: Cross-border evidence challenges*. Forensic Science International: Digital Investigation.

Brundage, M., Avin, S., Wang, J., & Belfield, H. (2022). *Toward trustworthy AI development: Mechanisms for supporting verifiable claims*. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society.

Bryson, J. M., Crosby, B. C., & Bloomberg, L. (2014). Public value governance: Moving beyond traditional public administration and the new public management. *Public Administration Review*, *74*(4), 445–456. https://doi.org/10.1111/puar.12238

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, *81*, 1–15.

Caruso, L., Singh, V., & Bartoli, M. (2024). *Algorithmic accountability in forensic decision-making*. AI & Society.

Casey, E. (2021). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the "good society": The US, EU, and UK approach. *Science and Engineering Ethics*, *24*(2), 505–528. https://doi.org/10.1007/s11948-017-9901-7

Chen, Y., et al. (2023). Learning loops in AI-enabled public organisations. *Public Management Review*.

Choudhury, A., Basu, D., & Ghosh, S. (2022). Artificial intelligence in forensics: Challenges and advancements. *Forensic Science International: Reports*, *6*, 100262.

Dubai Future Foundation. (2021). *AI Governance and Policy Landscape: Challenges and Recommendations*.

Faehndrich, J., Honekamp, W., Povalej, R., Rittelmeier, H., Berner, S., & Labudde, D. (2023). Digital forensics and strong AI: A structured literature review. *Forensic Science International: Digital Investigation*, *46*, 301617. https://doi.org/10.1016/j.fsidi.2023.301617

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., et al. (2022). AI4People: An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *30*(1), 1–28. https://doi.org/10.1007/s11023-018-9482-5

Ghosh, S., Kaur, P., & Dwivedi, Y. K. (2023). Responsible AI in the public sector: A review of challenges and best practices. *Information Systems Frontiers*, *25*(2), 511–528.

Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., et al. (2018). *Explaining explanations: An overview of interpretability of machine learning*. arXiv preprint arXiv:1806.00069. https://doi.org/10.1109/DSAA.2018.00018

Guttman, A., et al. (2024). From automation to augmentation: Human-in-the-loop AI in criminal justice. *Nature Human Behaviour*.

Han, X., Zhang, Y., & Zhou, M. (2023). Bias and generalisability in deep forensic models. *Forensic Imaging*.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, *349*(6245), 255–260. https://doi.org/10.1126/science.aaa8415

Ketsekioulafis, I., Filandrianos, G., Katsos, K., Thomas, K., Spiliopoulou, C., Stamou, G., & Sakelliadis, E. I. (2024). Artificial Intelligence in Forensic Sciences: A systematic review of past and current applications and future perspectives. *Cureus*, *16*(9), e70363. https://doi.org/10.7759/cureus.70363

Kumar, R., & Raj, P. (2023). Institutional readiness for AI adoption in public safety agencies. *Government Information Quarterly*.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444. https://doi.org/10.1038/nature14539

Leslie, D. (2023). AI ethics in law and forensics: Between transparency and efficacy. *AI & Ethics*.

Li, Y., & Wang, C. (2024). Data provenance and interoperability in AI-based forensics. *Digital Evidence and Electronic Signature Law Review*.

Mavroeidis, V., et al. (2022). AI in forensic science: Opportunities and pitfalls. *Forensic Science International*.

McNeive, D., et al. (2020). Ethical challenges of using artificial intelligence in legal decision-making. *Computer Law & Security Review*, *36*, 105373. https://doi.org/10.1016/j.clsr.2019.105373

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys*, *54*(6), 1–35. https://doi.org/10.1145/3457607

Miguel, A. L. R., Moreiraa, R. P. L., & Oliveira, A. F. D. (2021). ISO/IEC 17025: History and introduction of concepts. *Química Nova*, *44*(6), 792–796. https://doi.org/10.21577/0100-4042.20170726

Morán-Torres, R., Feld, K., Hesser, J., et al. (2025). Artificial intelligence and computer vision in forensic sciences. *Rechtsmedizin*, *35*, 219–225.

https://doi.org/10.1007/s00194-025-00775-3

Morrison, G. S., Elliott, S., Guiness, J., Sonden, L., & Court, D. S. (2025). A guide to ISO 21043 Forensic Sciences from the perspective of the forensic-data-science paradigm. *Science & Justice*, *65*(5), 101304. https://doi.org/10.1016/j.scijus.2025.101304

O'Neil, C., et al. (2023). Human factors in forensic AI adoption. *Information Systems Frontiers*.

Othman, M. M. Y., & Al Hammadi, M. M. H. (2023). The use of artificial intelligence in combating crimes in the UAE: Critical review. In A. M. A. Musleh Al-Sartawi & S. Raed (Eds.), *From the Internet of Things to the Internet of Ideas: The Role of Artificial Intelligence* (Lecture Notes in Networks and Systems, Vol. 557). Springer. https://doi.org/10.1007/978-3-031-17746-0_29

Othman, M., & Al Mahaddi, H. (2023). Technology and governance: AI readiness in GCC nations. *Arabian Journal of Future Studies*, *7*(1), 55–72.

Raed, S. (2020). Digital transformation and AI in UAE's law enforcement: An overview. *Middle East Security and Technology Review*, *5*(2), 23–37.

Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

Schroeder, M. (2019). Challenges and opportunities in the use of artificial intelligence for legal reasoning and decision making: A research agenda. *Artificial Intelligence and Law*, *27*(4), 397–434.

Singh, V., & Dastidar, A. (2023). Legal admissibility of AI evidence. *Computer Law & Security Review*.

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2021). Critical review of artificial intelligence in public sector decision-making: A strategic policy framework. *Information Systems Management*, *38*(3), 234–248. https://doi.org/10.1080/10580530.2021.1928985

Tian, J., et al. (2022). Barriers to AI implementation in forensic laboratories. *Computers in Human Behavior*.

UAE Government. (2024). *We the UAE 2031: National AI Vision Implementation Report*.

UAE Ministry of Artificial Intelligence. (2020). *National Strategy for Artificial Intelligence 2031*. Government of the United Arab Emirates.

UAE Ministry of Artificial Intelligence. (2023). *National Strategy for Artificial Intelligence 2031*.

UAE Ministry of Interior. (2022). *Annual Report on Security Infrastructure Development*.

Veldhuis, M. S., Ariëns, S., Ypma, R. J., Abeel, T., & Benschop, C. C. (2022). Explainable artificial intelligence in forensics: Realistic explanations for number of contributor predictions of DNA profiles. *Forensic Science International: Genetics*, *56*, 102632. https://doi.org/10.1016/j.fsigen.2021.102632

Wang, L., & Zhao, X. (2023). Data governance for AI-driven forensics. *Forensic Science Review*.

Wiewiórowski, W., & Fila, M. (2022). *AI and data protection in judicial cooperation in criminal matters*. European Union Agency for Criminal Justice Cooperation.

Zhang, X., & Lu, Y. (2022). Longitudinal analysis of AI regulation and governance: A comparative study of the EU and UAE frameworks. *Technology in Society*, *70*, 102020.

Zhou, D., & Xu, H. (2024). Forensic data interoperability and model validation. *Expert Systems with Applications*.

Copyrights