SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 1.1, (2026), pp. 4838-4848
Open Access. Online & Print

DOI: 10.5281/zenodo.19387654

THE ADMISSIBILITY OF AI-GENERATED EVIDENCE IN CRIMINAL PROCEEDINGS: A COMPARATIVE ANALYTICAL STUDY IN LIGHT OF QATARI LEGISLATION

Nagi Saleh Alyami

Researcher, Master of Criminal Justice Program, Lusail University, Qatar

Received: 11/12/2024
Accepted: 25/02/2025

Corresponding author: Nagi Saleh Alyami (202100326@lu.edu.qa)

ABSTRACT

This study examines the conceptual framework of automatically generated evidence, encompassing its technical and legal characteristics. It analyses the scope of its **admissibility** within the Qatari judiciary while benchmarking its efficacy against European legal precedents. Furthermore, it elucidates the procedural safeguards essential for protecting the rights of the accused. The research addresses a precise legal problem: the absence of explicit **statutory provisions** regulating the acceptance or rejection of AI-generated evidence, and the subsequent challenges posed to the integrity of criminal justice. The findings indicate that while Qatari law recognises electronic evidence in principle, it lacks specific provisions for evidence generated by Artificial Intelligence (AI). Consequently, the determination of its **evidentiary weight** remains subject to judicial discretion, leading to inconsistent rulings. Conversely, the comparative analysis highlights that the European Union has adopted a rigorous approach, classifying AI systems utilised within the judiciary as "high-risk." The study concludes by recommending an amendment to the **Qatari Criminal Proceedings Law** or the **Cybercrime Prevention Law** to incorporate a dedicated chapter on automatically generated evidence. It further suggests the development of a procedural manual to document the **chain of custody** for such evidence based on a clear and objective classification.

KEYWORDS: Criminal Evidence, Intelligent Evidence, Legal Probative Value, Criminal Proceedings, Qatari Legislation.

1. INTRODUCTION

1.1. Background of the Study

Crime is an evolving phenomenon inherent to all societies. International reports and studies indicate that crime rates continue to rise globally year-on-year, driven by the rapid evolution of modern communication technologies. This shift has seen traditional crimes superseded by cybercrimes committed in virtual spaces, unfettered by geographical boundaries. [1]

Cybercrime presents significant challenges; many nations lack sufficient **statutory legislation** to combat these offences. Although some laws exist, they fail to address the core issue regarding the distinct nature of evidence produced automatically by Artificial Intelligence. [2]

Technological advancement is of paramount importance in enhancing the capacity of judicial bodies to collect and analyse forensic evidence, particularly concerning organised crime targeting property and persons. AI has become a central tool in developing criminal investigation systems, thereby bolstering public stability and social peace. [3]

Consequently, AI provides tools to produce advanced digital evidence. This development raises a critical legal issue: the degree of **evidentiary weight** afforded to such evidence before the courts, and the feasibility of its admissibility within **criminal proceedings** under current Qatari legislation—especially as the State of Qatar seeks to integrate AI into its judicial system to ensure the efficacy and legitimacy of criminal justice. [4]

1.2. Research Problem

The core problem of this study lies in the fact that AI systems used in crime prevention are relatively novel. For the resulting evidence to be considered legally binding, it must satisfy the legal requirements established for "expert evidence" (standard technical evidence) in criminal cases.

Thus, a challenge arises from the absence of an explicit regulatory framework governing the admission or rejection of evidence derived via AI techniques within Qatari criminal legislation. Current Qatari law recognises electronic transactions and documents in general, granting them **probative value** provided they satisfy requirements of authenticity and integrity. However, automatically generated evidence (such as modified images or deepfakes) often lacks transparency or discernible traces of alteration, leaving courts sceptical of its reliability.

Accordingly, the primary research question is:

What is the evidentiary weight of evidence produced automatically by AI under Qatari legislation compared to European legislation, and what solutions can be proposed to grant it the same probative value as standard digital evidence?

From this primary question, several sub-questions emerge:

1. What is the definition of AI-generated evidence, and how does it differ from standard (traditional) evidence?
2. What technical and mandatory conditions must be met by AI-generated evidence?
3. Are there practical solutions to ensure that evidence generated or enhanced by AI is admissible as proof before the national judiciary?

1.3. Significance of the Study

The significance of this study lies in its address of a pragmatic legislative lacuna within Qatari law regarding the regulation of Artificial Intelligence in criminal evidence. This is particularly timely as numerous jurisdictions have begun developing legislative and regulatory frameworks to oversee AI within judicial operations. Notably, the **European Union Artificial Intelligence Act (AI Act)**, which entered into force in August 2024, mandates specific standards for "high-risk" systems, including those used in judicial contexts.

Conversely, the Qatari legislative landscape requires rigorous induction and effective application. Given recent state proclamations regarding the integration of AI within the judicial system and criminal proceedings, this study reflects the official impetus toward drafting future legislation in this nuanced, sensitive, and complex field.

1.4. Methodology and Literature Review

This study adopts a **descriptive-analytical approach** to examine Qatari statutory texts concerning electronic evidence and the general principles of criminal procedure. Furthermore, it employs a **comparative methodology**, benchmarking Qatari legislation against European counterparts—specifically Spain—with a focus on AI regulatory laws and relevant international guidelines. An **evaluative legal method** is also utilised to critique the stance of the Qatari judiciary regarding digital evidence and its degree of **probative force**.

While extensive literature exists regarding AI and its intersection with cybercrime and organised crime, scholarly work concerning the **admissibility**

and **evidentiary weight** of AI-derived evidence—specifically under Qatari law—remains sparse relative to its contemporary importance.

The research gap is addressed by analysing the evidentiary weight of automatically generated technical evidence before the courts. This study provides practical and legislative recommendations to ensure the **authenticity** of such evidence and defines the legal and technical conditions required to prove organised crime through technical means—aspects largely overlooked in previous scholarship.

1.5. Study Structure

In light of the aforementioned objectives, the applied treatment of these legal issues will be organised into the following three chapters:

1. **Chapter I:** Theoretical and Legal Aspects of Artificial Intelligence Technologies.
2. **Chapter II:** Criteria for the Legality of Automatically Generated Evidence in Combatting Organised Crime.
3. **Chapter III:** Legal and Ethical Challenges Associated with the Evidentiary Weight of AI-Generated Evidence.

2. CHAPTER I: THEORETICAL AND LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Before delving into the evidentiary weight of evidence derived from information systems and its practical implications, it is essential to clarify the fundamental concepts of organised crime and Artificial Intelligence (AI). This chapter defines the nature of such evidence and the various AI applications employed in combatting these crimes through the following two sections:

2.1. Section I: Conceptual Framework of Organised Crime and Artificial Intelligence

There is relative academic consensus regarding the definitions of organised crime and AI. While numerous definitions exist, this section provides a concise overview to ensure the thematic flow and conceptual clarity of the study.

1. Organised Crime Extensive efforts have been made to identify the common elements that define organised crime. Most definitions focus on the "Organised Criminal Group" as the unit of analysis rather than the isolated criminal act. Understanding the nature of these groups is vital for effective intervention. The **United Nations Convention against Transnational Organized Crime (2000)** provides a comprehensive global perspective on these offences.[5]

In general terms, organised crime may be defined as: a continuing criminal enterprise, intentionally seeking to profit from illicit activities (often in high public demand), sustained through the corruption of public officials and the use of intimidation, threats, or force to protect its operations.[6]

2. Etymologically, "Intelligence" in Arabic language denotes quick-wittedness and mental acuity, while "Artificial" (derived from the root *ṣana'a*) refers to that which is man-made.[7] In the *Al-Qamus al-Muhit* dictionary, the term implies understanding or perception represented through human-made means.[8]

Technically, **John McCarthy** defined the term in 1956 as the "the artificial intelligence problem is taken to be that of making a machine behave in ways that would be called intelligent". [9] Conversely, **Kaplan and Haenlein** describe it as "a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation."[10]

In a practical sense, AI refers to technologies seeking to produce machines or systems with cognitive capabilities analogous to the human mind.[11] Consequently, it has become a pivotal innovation in criminal investigations, utilised to extract precise data and assist authorities in combatting various forms of organised crime.[12]

3. Evidence Derived from AI Systems In legal proceedings, it is an established principle that the claims and defences of parties must be supported by specific evidence to be admissible. Such evidence is either traditional or electronic. Criminal proof is a procedural activity aimed at reaching **judicial certainty**; it is the mechanism by which a judge identifies perpetrators and accomplices.[13]

Digital Evidence is most accurately defined as evidence derived from or by information systems, including computer hardware, peripheral equipment, or modern communication networks. Following technical and statutory procedures, this data is presented to the judiciary in various forms—such as text, graphics, or recordings—to prove or disprove a criminal act.[14]

Regarding **AI-generated evidence**, Qatari law currently lacks a direct statutory definition. However, comparative Arab and European legislations provide guidance. The **EU Regulation on European Production and Preservation Orders for electronic evidence in criminal proceedings** defines it in Article 1 as: "subscriber data, traffic data, or content data stored by or on behalf of a service provider, in electronic form." (Note: This

regulation enters into force on 18 August 2026, pursuant to Article 34).[15]

Two essential elements emerge from these definitions:

1. **Element 1:** The factuality of data stored or extracted from any information system.
2. **Element 2:** The capacity to collect and analyse this information using either traditional systems or modern AI frameworks.[16]

Thus, "**Intelligent Evidence**" may be defined as: evidence extracted via AI applications—supported by advanced analytical algorithms—to identify patterns and correlate data in a manner that exceeds traditional human capability, thereby enhancing evidentiary accuracy and judicial efficiency.[17]

2.2. Section II: AI Technologies Utilised in Combatting Organised Crime

The emergence of AI in crime prevention—specifically regarding organised crime—has been transformative. States must now integrate these technologies into their security frameworks to preserve order.[18] AI plays a pivotal role in **predictive policing**, allowing for proactive measures and providing robust evidence for judicial conviction.[19]

1. AI Modalities in Crime Suppression AI systems used by security agencies range from field-deployed hardware to investigative software:[18]

1. **Expert Systems:** These simulate human expertise within a specific domain using pre-stored rules and decision-making mechanisms to solve complex problems (e.g., tracking capital flight in organised financial crime).[20]
2. **Predictive Algorithms:** These utilise historical data to forecast criminal activity, identifying high-risk locations, periods, and potential suspects by studying complex criminal behaviours.[21]
3. **Forensic Analytics:** These combine traditional criminal records with modern software to extract and reconstruct digital evidence, even if previously deleted.[22]
4. **Identity Verification Systems:** These include remote biometric identification. The **EU AI Act** defines these as AI systems intended for identifying natural persons at a distance without their active involvement.[23]

In the regional context, the UAE is a leader in this field, utilising iris and facial recognition as fundamental components of national identity, regulated by **Federal Law No. 45 of 2021 on the Protection of Personal Data**. Similarly, the Abu Dhabi Judicial Department issued **Decision No. 32 of 2020**, establishing a procedural guide for AI in judicial operations.

Notably, during the drafting of this study, Qatar enacted the **Biometric Data Law No. 17 of 2025**. Article 1 defines biometrics as physiological characteristics (voice, hand, face, eye, etc.) that can be scientifically measured to distinguish individuals. Crucially, **Article 6** grants biometric data stored in databases **prima facie evidentiary weight** (حجية الإثبات), signaling Qatar's legislative intent to embrace AI in its judicial system.

2. Procedural Integration of AI The application of "Expert Systems" in criminal investigations involves structured databases containing crime types, locations, DNA profiles, and behavioural patterns. These are compared against physical evidence through "Criminal Standards" modules.[20]

Predictive techniques categorise risks into crime prediction, offender identification, and victimisation forecasting (similar to AI-mapped security assessments used in the United States).[21] Furthermore, **facial recognition** enables security agencies to neutralise organised groups by tracking member movements and providing detailed maps for apprehension and subsequent judicial conviction.[22]

3. CHAPTER II: CRITERIA FOR THE LEGALITY OF AUTOMATICALLY GENERATED EVIDENCE IN COMBATTING ORGANISED CRIME

Criminal evidence derived from Artificial Intelligence (AI) systems possesses a unique set of technical and legal characteristics that distinguish it from traditional evidence. While these systems are formidable tools against organised crime, their inherent complexity requires a rigorous induction of the conditions governing their **admissibility**.

3.1. Section I: Characteristics of Automatically Generated Evidence

This section delineates the technical and legal attributes of AI-generated evidence and provides a comparative overview of its application within Qatari and international frameworks.

3.1.1. Technical Characteristics

1. **Precision and Velocity:** AI systems process vast datasets and execute complex analyses at speeds far exceeding human capability, ensuring high accuracy within record timeframes.[24]
2. **Big Data Analytics:** Modern organised crime relies on intricate communication networks

and financial transactions. AI excels at scrutinising these massive, unstructured datasets—a task virtually impossible for manual investigators.[25]

3. **Self-Learning and Prediction:** Machine learning models "learn" from historical data to refine analytical accuracy. This facilitates **predictive policing**, allowing law enforcement to pre-emptively allocate resources to high-risk areas.[26]
4. **Transparency and Explainability:** This remains a significant challenge. Many deep learning models operate as a "**Black Box,**" where the reasoning behind a specific output is opaque. To ensure **admissibility**, algorithms must be transparent and auditable by experts. The **EU AI Act** mandates comprehensive technical documentation for "high-risk" systems used in the judiciary.[26]

3.1.2. Legal Characteristics

1. **Admissibility in Court:** Acceptance depends on meeting traditional criteria: **reliability** and **authenticity**. While the **Qatari Electronic Transactions and Commerce Law No. (16) of 2010** recognises the **evidentiary weight** of electronic records (Articles 1 & 2), AI-generated outputs (e.g., enhanced imagery) pose new challenges regarding tampering detection, leaving their acceptance to **judicial discretion**.
2. **Transparency and Accountability:** To ensure a **fair trial**, the defence must have the right to examine the logic of the AI system that produced the evidence. This often conflicts with corporate intellectual property rights—a tension the EU AI Act addresses through mandatory registration of high-risk systems in a central database.
3. **Protection of Fundamental Rights:** AI evidence collection must align with privacy rights. This is upheld by the **Qatari Personal Data Privacy Protection Law No. (13) of 2016** and, internationally, by the **General Data Protection Regulation (GDPR)**.[27]
4. **International Standardisation:** Current legislative trends, led by the EU AI Act, adopt a risk-based classification, imposing stringent obligations on "high-risk" law enforcement tools.[28]

3. AI Applications in Qatari and Comparative Jurisprudence The Qatari Ministry of Justice has signaled a move toward integrating AI into the judicial framework. Currently, courts rely on the **Electronic Transactions Law (2010)**, admitting digital evidence if the method of creation is proven reliable (Articles 20–27).

However, Qatar lacks a specific **procedural manual** for fully AI-generated evidence. In contrast, Abu Dhabi has issued a formal guide for AI in judicial services.[29] In Spain, legislative amendments (Royal Decree-Law 6/2023) allowing AI-assisted judicial drafting to have sparked debate. Scholars like **Fernando Galindo Ayuda** argue that existing laws are insufficient, insisting that AI systems must remain under direct **human oversight** to satisfy constitutional requirements.[30]. However, The European Union's Artificial Intelligence Act (AI Act) is considered the most comprehensive regulatory framework to date.[31]

3.2. Section II: Mandatory Conditions for AI-Derived Evidence

To be considered "legally produced," AI evidence must satisfy both technical and procedural requirements.

3.2.1. Technical Conditions

Under Qatari Law No. (16) of 2010 (Article 20), data messages do not lose legal validity simply because they are electronic. Furthermore, the **Cybercrime Prevention Law No. (14) of 2014 (Article 15)** prohibits the exclusion of evidence solely due to its digital nature.

- **Persistence and Integrity:** Evidence must be stored in a retrievable format and remain unaltered (no deletions or additions).[12] This mirrors **Article 12(1) of the EU AI Act**, which requires high-risk systems to enable automatic "logging" of events throughout their lifecycle.

3.2.2. Procedural Conditions

Qatari Law No. (14) of 2014 establishes the following safeguards:

- **Public Prosecution Authorisation:** Any evidence collection from information systems requires a reasoned warrant from the **Public Prosecution**. Article 14 mandates that search warrants be specific and justified; any seized devices must be presented to the Prosecution for further action.[21]
- **Expert Testimony:** Pursuant to **Article 95 of the Qatari Criminal Proceedings Law No. (23) of 2004**, technical experts may be appointed to either:

1. Verify the integrity and health of the AI-extracted evidence.
2. Use AI tools to analyse data/images for comparison against witness testimonies.

3.2.3. Judicial Applications and Precedents

Most jurisdictions agree that AI-supported evidence must be accompanied by a human expert report detailing the **methodology** and **chain of custody**.

1. **State of Qatar:** The **Court of Cassation** has ruled that electronic documents carry the same weight as paper documents, provided they are stored in a final form that guarantees integrity and are electronically signed.[32] Another ruling equated electronic signatures on judicial documents with traditional signatures under Article 241 of the Criminal Proceedings Law.[33]
2. **UAE:** In 2023, the **DIFC Courts** discussed the admissibility of AI-generated evidence. While not a binding precedent, it indicated a cautious openness, provided there is human verification of accuracy and transparency.[34]
3. **European Union:** Despite the EU AI Act, there is currently no major published European precedent establishing a general standard for AI-generated evidence.
4. **USA:** Courts have begun rejecting expert testimonies that rely on AI-generated citations without verification.[35] A **2025 Federal Court decision in Minnesota** excluded an expert's testimony for using AI-generated citations that lacked factual basis.[36]

4. CHAPTER III: LEGAL AND ETHICAL CHALLENGES ASSOCIATED WITH THE EVIDENTIARY WEIGHT OF AI-GENERATED EVIDENCE

The deployment of automatically generated evidence in proving organised crime raises a set of complex legal and ethical challenges. Legislators and judges must navigate these with extreme caution to ensure the administration of justice and the protection of fundamental rights and freedoms. This chapter is structured into two sections: the first examines the impact of AI on the **evidentiary weight** of "intelligent evidence" and judicial discretion, while the second elucidates the legal and ethical frameworks for handling such evidence.

4.1. Section I: The Impact of AI on the Admissibility of Intelligent Evidence and Judicial Discretion

1. The Impact of AI on the Probative Force of Evidence The question of whether AI-generated evidence is binding upon the court triggers the fundamental principle of "**Free Proof**" (or the judge's "inner conviction"), as established by **Article 232 of the Qatari Criminal Proceedings Law No. (23) of 2004**.

Under this principle, information derived from AI remains subject to the judge's subjective conviction. The judge must engage in a purely cognitive process to examine the evidence, reaching a conclusion that forms a solid certainty for either conviction or acquittal. To date, this remains a matter of **judicial discretion**.[18]

However, this discretion is not absolute. **Article 15 of Law No. (14) of 2014 (The Cybercrime Prevention Law)** explicitly states:

"No evidence resulting from any information technology means, information systems, information networks, websites, or electronic data and information shall be excluded solely because of the nature of that evidence."

Therefore, a judge's conviction is constrained; a judge may not arbitrarily dismiss technical evidence extracted according to statutory requirements simply due to personal scepticism. Should this occur, the judgment becomes vulnerable to appeal or reversal by the **Court of Cassation** for error in the application of the law.[37]

2. Limits on Judicial Power to Exclude Intelligent Evidence While a trial judge enjoys wide latitude in evaluating evidence, the power to exclude it is strictly governed by the "**Exclusionary Rule.**" This applies to evidence obtained through unlawful means during the investigation phase or where there is a failure to comply with the procedural safeguards established in the **Criminal Proceedings Law** or the **Cybercrime Prevention Law**.[38]

This freedom is restricted by judicial standards that the court must adhere to when providing the **Ratio Decidendi** (legal reasoning) for its judgment. If a judge excludes AI evidence, then he is legally required to provide a justified rationale and cite the countervailing evidence supporting such an exclusion, pursuant to **Article 238 of Law No (23) of 2004 Qatari Criminal Procedure Law (Qatari Criminal Proceeding Law),** which states "The judgment must include the reasons upon which it is based. Every judgment of conviction must include a statement of the incident necessitating the penalty or measure, the circumstances under which it occurred, the evidence from which the court inferred the conviction, and the text of the law under which the judgment was rendered."

It is noteworthy that **Criminal Proof** (the final judicial determination) differs fundamentally from **Evidence Extraction** (the investigative phase). The latter is conducted to facilitate the former; while the trial judge handles the proof, the extraction is

performed by the investigative authorities. Consequently, "Proof" is the final result of the evidence upon which the judge bases the verdict in conjunction with other materials presented.[37]

To ensure procedural clarity, the following core constraints limit a judge's power to exclude AI evidence:[39]

1. **The Adversarial Principle (Discussion of Evidence):** A judge cannot base a conviction on evidence that has not been openly presented and debated during trial. AI-generated data must undergo detailed scrutiny by the Prosecution and the Defence, pursuant to **Article 232**.[40]
2. **Comprehensive Appraisal:** A judge must personally evaluate the "Intelligent Evidence" and cannot form a pre-ordained conviction. The judge may seek **Expert Evidence** to assist in the actual inspection of the data during trial to determine its true **probative value**.[39]
3. **The Standard of Certainty:** Evidence derived from AI must be certain and not based on conjecture. [40] Under **Article 234 of the Qatari Criminal Proceedings Law**, any doubt in the "Intelligent Evidence" must result in an acquittal, following the principle of *in dubio pro reo* (doubt is interpreted in favour of the accused).

4.2. Section II: Handling Automatically Generated Evidence (Legal and Ethical Dimensions)

This section delineates the legal and practical challenges, followed by the ethical dilemmas inherent in managing AI-generated evidence. It concludes with an overview of the strategies employed by Qatari and comparative legislations to mitigate these issues.

4.2.1. Legal and Practical Challenges

The proliferation of cybercriminal activities and the reliance of perpetrators on sophisticated information technology tools have facilitated the commission of crimes both locally and across borders. This has diminished the efficacy of national and international cooperation in combatting organised crime.

The primary practical and legal difficulties in handling AI-generated evidence include:

1. **Temporal Decay:** Significant intervals—often months or years—may elapse before a crime is detected, risking the corruption or loss of digital evidence.
2. **Attribution and Anonymity:** Perpetrators frequently utilise pseudonyms, public access points (such as internet cafés), or communication intermediaries. This complicates the tracking of the connection source and the identification of the suspect's location.
3. **Jurisdictional Conflicts:** Transnational crimes raise complex questions regarding **Conflict of Laws** and territorial jurisdiction, specifically determining which statutory legislation applies and which authority holds the mandate for investigation and prosecution.
4. **Liability Assignment:** The difficulty in defining criminal responsibility for third parties, such as website operators, Internet Service Providers (ISPs), or hosting providers.[41]

These obstacles underscore the urgent need to modernise legal, procedural, and technical frameworks to ensure the effective collection and investigation of reliable electronic evidence.

4.2.2. Ethical Challenges

Ethical considerations have gained paramount importance due to the risks electronic evidence poses to the moral fabric of public order. The following are the most prominent ethical challenges:

1. **Algorithmic Accountability:** If a system produces an erroneous result—such as the misidentification of an innocent individual—liability remains ambiguous. Does responsibility lie with the developing corporation, the end-user agency, or the individual programmer?
2. **Bias and Discrimination:** AI systems learn from training datasets. If these data reflect existing societal or historical biases, the system will perpetuate and amplify them, leading to the unfair targeting of minorities or marginalised groups.
3. **Privacy Rights:** Privacy is a fundamental human right protected by international treaties. The reliance of AI systems on the collection and analysis of massive volumes of personal data represents a significant threat to the **Right to Privacy**.[23]

4.2.3. Strategies for Addressing Challenges: Qatari vs. Comparative Legislation

The current framework of Qatari legislation focuses on broad principles, such as data protection and the recognition of electronic records. Despite the national impetus toward adopting Artificial Intelligence, there are currently no granular rules addressing the **admissibility** of automated evidence or its associated ethical challenges.

Consequently, these matters are left to **judicial discretion** and the application of general legal analogies.

In contrast, the **European Union Artificial Intelligence Act (AI Act)** provides the most advanced model globally. It directly addresses these challenges by classifying AI systems used in the judiciary as "**High-Risk.**" This classification imposes rigorous legal obligations designed to ensure transparency (via technical documentation), mitigate bias (through data quality requirements), ensure **human oversight**, and clearly define liabilities. This proactive approach aims to build public trust in these technologies while ensuring their use aligns with fundamental human rights.

Consequently, there are viable solutions that could serve as a foundation for the Qatari legislator to issue a **Procedural Manual** or guidelines regulating the use of AI-derived or AI-supported evidence before Qatari courts or national arbitration tribunals. These solutions centre on the creation of a **Professional Checklist** to be utilised when presenting such evidence. This would bolster its **evidentiary weight**, elevating it to the status of "proof" or a "legal presumption" even under strict judicial scrutiny.

The proposed framework includes specific steps for the submission, pleading, and admission phases of evidence as follows:

4.4. The Professional Checklist

This checklist is based on four primary pillars designed to audit AI-derived evidence across its entire lifecycle:

1. **Data Collection & Documentation:** Ensuring the integrity of the raw data used by the system.[42]
2. **Governance & Transparency Standards:** Verifying the "explainability" of the algorithms and compliance with regulatory standards.[43]
3. **Human Oversight:** Confirming that a human expert supervised the system's output to prevent automated bias.[44]
4. **Chain of Custody & Digital Fingerprinting:** Documenting every hand the evidence passed through and ensuring its digital integrity remains intact from extraction to the courtroom.[45]

Table 1:

1. Evidence Collection					
1.1	**Documentation**	Data Source Documentation	System Name	Manufacturer / Developer	Version / Release
1.2	**Chain of Custody**	Name of Handler	Date of Action	Time of Action	A non-editable copy being saved?
1.3	**Methodology**	Generation or Analysis Criteria	Are settings preserved?	Is a log file attached (detailing all analytical operations)?	

Table 2:

2. Examination and Verification

2.1	Human Review	Has it been reviewed by a human expert?	Has it been verified against scientific/technical standards?	Is a human expert report attached?	Does the report explain the algorithm and datasets?	Does the report address risks of bias or deepfakes?
2.2	Authenticity	Has post-generation data integrity been verified?	Has Digital Hash been used to prove file authenticity?			
2.3	Transparency	Is the system's explainability disclosed?	Are the algorithms proprietary (Black Box) or Open Source?			

4.5. Submission of Evidence to the Court or Arbitration Tribunal

4.5.1. Disclosure and Notification

1. Any party utilising evidence or information derived from or generated by AI must notify both the court and the opposing party of its nature and source.
2. In cases of international arbitration, disclosure is required as per the **Chartered Institute of Arbitrators (CIArb)** guidelines.[46]

4.5.2. Final Preservation

- A secured copy must be deposited with the court or within a certified evidence preservation system to preclude challenges regarding the document's integrity.

4.5.3. Pleading and Admissibility

1. If the reliability of the evidence is challenged, the response should involve submitting the professional checklist and providing proof of human review.
2. The response must also include documentation on the methodology and guarantees regarding

the **Chain of Custody**.

3. Arguments should be supported by the **OECD** [47] and **UNESCO** [48] principles on the ethics of Artificial Intelligence, as well as the practices proposed in the **EU AI Act**.[49]

5. CONCLUSION

The integration of Artificial Intelligence into criminal proceedings represents a paradigm shift in the methods used to prove organised crime. It enables judicial systems to enhance efficiency and achieve justice more rapidly and accurately. Consequently, this study emphasises the critical balance between technological innovation and legal/ethical safeguards. This ensures transparency and accountability while maintaining public trust in the judicial system. Therefore, developing legislation, establishing effective supervisory mechanisms, and training judicial personnel are strategic steps toward employing AI in a manner that serves justice and aligns with international standards.

5.1. Study Findings

1. **Legislative Gap**: Qatari legislation lacks specific provisions regulating the evidentiary weight of automatically generated evidence, leaving the matter to general rules and judicial discretion.
2. **Comparative Models**: The **EU AI Act** provides an advanced regulatory model that can serve as a guide, particularly in its classification of judicial systems as "high-risk".
3. **Fundamental Challenges**: The use of automated evidence raises profound issues regarding the defendant's fundamental right to confrontation and the "**Black Box**" dilemma which hinders the understanding of algorithmic logic. It also presents ethical risks related to bias, discrimination, and liability for systemic errors.
4. **Lack of Precedent**: There are currently no firmly established national or global judicial precedents confirming the absolute admissibility of AI-derived or generated evidence.

5.2. Recommendations

1. **Legislative Reform**: Amend the **Qatari Criminal Proceedings Law** or the **Cybercrime Prevention Law** by adding a dedicated chapter for AI-derived evidence that defines conditions for admissibility and documentation procedures.
2. **Procedural Guidelines**: Establish a procedural manual detailing the technical and legal requirements for AI evidence to ensure it attains the same legal standing and evidentiary weight as other forms of digital evidence.
3. **National Oversight**: Found an independent national authority to certify and oversee "high-risk" AI systems used in the justice sector, drawing inspiration from the European model.
4. **Chain of Custody Protocol**: Develop a technical procedural guide for documenting the "**Chain of Custody**" for automated evidence to ensure its absolute authenticity.

BIBLIOGRAPHY

1. Khamouin, F. (2019). Family and crime. Al-Ijtihad Journal for Legal and Economic Studies, 8(2).
2. Al-Musa'adah, A. (2018). The dilemma of jurisdiction in cybercrimes. International Review of Law, 2018(4). (Special Issue on the Blockade).
3. Salem, D., & Abu Al-Jadayel, M. (2023). The effectiveness of the National Cybersecurity Authority in Saudi Arabia using AI techniques as a future trend: A forward-looking study. Arab Research in Journals of Specialized Education, 1(30).
4. Amouri, A. (2018). Search and seizure in cybercrimes (Unpublished master's thesis). Deanship of Graduate Studies, Al-Quds University, Palestine.
5. [Jurisdiction/Government]. (2009). Decree No. (10) of 2009 approving the accession to the United Nations Convention against Transnational Organized Crime (2000).
6. United Nations Office on Drugs and Crime. (2018, April). *Defining organized crime*. Education for Justice: Organized crime module 1 (Definitions of organized crime)—Key issues. Organized Crime Module 1 Key Issues: Defining Organized Crime
7. Ibn Manẓūr, M. ibn M. (1993). Lisān al-ʿArab (Entry: "Thaka"). Dār Ṣādir.
8. Al-Fayrūzābādī, M. A.-D. (1987). Al-Qāmūs al-Muḥīṭ. Al-Risāla Foundation.
9. McCarthy, J., Minsky, M., Rochester, N., & Shannon, C. E. (1955). *A proposal for the Dartmouth summer research project on artificial intelligence* (for the 1956 summer project). A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE
10. Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who is the fairest in the land? On the interpretations,

illustrations, and implications of artificial intelligence. Business Horizons, 62(1), 15–25.
11. Arhim, H. E. (2024). Adapting artificial intelligence in the management of civil and commercial lawsuits. University of Sharjah Journal for Juridical Sciences, 22(3).
12. Al-Balawi, G. b. A. b. S. (2025). Procedural challenges related to the admissibility of digital evidence extracted using artificial intelligence techniques in the criminal field. The Legal Journal, 23(4).
13. Shattat, M. M. (2001). The concept of criminal protection for computer software. Dar Al-Jame'a Al-Jadeeda.
14. Afifi, T. (2015). Cybercrime – Mobile phone crimes: A comparative study. National Center for Legal Publications.
15. European Parliament, & Council of the European Union. (2024, July 12). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
16. Al-Deeb, A. B., & Amin, D. I. (2024). The reflections of artificial intelligence on the rules of evidence. In 23rd Annual International Conference: Legal and Economic Dimensions of the Litigation System in the 21st Century. Journal of Legal and Economic Research, Faculty of Law, Mansoura University.
17. Omar, A. N. A. H. H. (2025). Artificial intelligence as a mechanism for criminal evidence. Law and Political Science Notebooks Journal, 5(1).
18. Al-Omareen, W. M. S. (2022, September). Artificial intelligence in criminal detection and investigation: A comparative study. Al-Mizan Journal for Legal and Islamic Studies, 9(3), 464–478.
19. Al-Qabba', H. b. M. b. A. (2024). The role of artificial intelligence in combating crime in the Saudi system: A descriptive analytical study (Unpublished master's thesis). College of Criminal Justice, Naif Arab University for Security Sciences, Saudi Arabia.
20. Qandil, A. A. Q. (2025). The role of expert systems in the stages of criminal investigation: An applied analytical study. Journal of Security and Law, 33(2).
21. Al-Babili, A. Y. M. Z. (2021). The role of artificial intelligence systems in predicting crime. Journal of Security and Law, 29(1).
22. Ali, R. S. (2023). Utilizing artificial intelligence techniques and data analysis in detecting crimes. Journal of Legal and Economic Studies, 9(3).
23. Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)* (European Treaty Series No. 005). https://rm.coe.int/168048d4e8
24. Al-Akhnash, N. A., & Al-Aidani, M. (2023). Artificial intelligence as a mechanism to combat cybercrime. Journal of Law and Environmental Sciences, 2(2).
25. Abdul Razzaq, R. M. A. M. (2023). The role of artificial intelligence in confronting cyber-terrorism crimes. Academic Journal of Nawroz University.
26. Qasim, M. M. G. M. (2024). The role of artificial intelligence in combating cybercrime: A comparative study. Modern Journal for Legal Studies, 2(2), 97–103.
27. European Parliament, & Council of the European Union. (2016, May 4). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
28. European Parliament, & Council of the European Union. (2024, July 12). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
29. Abu Dhabi Judicial Department. (2020). Decision of the Chairman of the Judicial Department regarding the manual on AI uses in judicial services and operations (Published on the Qistas platform). Author.
30. Galindo Ayuda, F. (2025). Digital literacy in judicial justice and artificial intelligence. Revista Digital de Derecho y Democracia Electrónica, (24), 28.
31. Kaplan, A. M., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, 62(1), 15–25.
32. Qatari Court of Cassation. (2023, March 6). Challenge No. 79 of 2023 (Civil and Commercial Matters). Encyclopedia of Qatari Judgments and Legal Principles. Supreme Judiciary Council, State of Qatar.
33. Qatari Court of Cassation. (2023, November 20). Challenge No. 1166 of 2023 (Criminal Matters).

Encyclopedia of Qatari Judgments and Legal Principles. Supreme Judiciary Council, State of Qatar.
34. Shooter, S., Christie, C., Manro, N., & Daghistani, A. (2025, May 22). *Artificial intelligence 2025: UAE*. Chambers and Partners, Global Practice Guides. Artificial Intelligence 2025 - UAE | Global Practice Guides | Chambers and Partners
35. Ravia, H., & Hammer, D. (2025, January 29). U.S. judicial policy regarding use of AI in court proceedings. Pearl Cohen Zedek Latzer Baratz. U.S. Judicial Policy Regarding Use of AI in Court Proceedings - Pearl Cohen.
36. Thomas, D. (2025, January 13). Judge rebukes Minnesota over AI errors in "deepfakes" lawsuit. Reuters., Judge rebukes Minnesota over AI errors in 'deepfakes' lawsuit | Reuters
37. Tohfa, F. A. M. (2020). Limits of excluding forensic and scientific AI evidence obtained illegally: A comparative study between Anglo-Saxon and Latin systems. The Spirit of Laws Journal, (91), 701–734.
38. Al-Rawashdeh, S. H. (2017). Evidence obtained from social media sites and its role in criminal proof: A study in English and American law. International Review of Law, 2017(3), 44.
39. Al-Jasiman, A. A. A. S. (2023). The criminal judge's authority in appraising evidence according to Qatari legislation. Journal of Law for Legal and Economic Research, 2023(2, Pt. 2).
40. Arafa, M. A. H. (2018). The admissibility of digital electronic evidence in criminal matters: A comparative applied analytical study. Journal of Law for Legal and Economic Research, 1(1).
41. Al-Tai, J. H. (2007). Information technology crimes: A new vision for modern crime (1st ed.). Omar Al-Mukhtar University.
42. International Organization for Standardization, & International Electrotechnical Commission. (2023). Information technology—Artificial intelligence—Management system: Requirements (ISO/IEC Standard No. 42001:2023). ISO. https://www.iso.org/standard/81230.html
43. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
44. International Organization for Standardization, & International Electrotechnical Commission. (2012). Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC Standard No. 27037:2012). ISO. https://www.iso.org/standard/44381.html
45. International Organization for Standardization, & International Electrotechnical Commission. (2015). Information technology—Security techniques—Incident investigation principles and processes (ISO/IEC Standard No. 27043:2015). ISO. https://www.iso.org/standard/44407.html
46. Chartered Institute of Arbitrators. (2025, Septmber). *Guideline on the use of artificial intelligence in arbitration*. guideline-on-the-use-of-ai-in-arbitration_updated-sept-2025.pdf
47. Organisation for Economic Co-operation and Development. (n.d.). *OECD AI principles overview*. OECD.AI. Retrieved March 5, 2026, from https://oecd.ai/en/ai-principles/
48. UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. Ethics of Artificial Intelligence - AI | UNESCO
49. Future of Life Institute, "The Act Texts," *EU Artificial Intelligence Act*, Available: The Act Texts | EU Artificial Intelligence Act. Accessed: Feb. 5, 2026.