ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

ARTIFICIAL INTELLIGENCE AND EVIDENCE LAW IN PAKISTAN: ADMISSIBILITY, CHALLENGES, AND JUDICIAL APPROACHES

Nisar Ahmed Chandio
Civil Judge and Judicial Magistrate, Karachi West
nisarchandiojudge@gmail.com
Shaharyar Dilshad
Advocate High Courts &Visiting Faculty School of Law, University of Karachi
s.shaharyar110@gmail.com

ABSTRACT

Research Background: *The rapid proliferation of Artificial Intelligence (AI) and automated algorithmic outputs in criminal, civil, and corporate domains has created a profound tension within traditional legal systems worldwide. In Pakistan, the procedural mechanisms for evaluating evidence remain anchored in conventional statutory frameworks.*

Research Problem: *The core legal architecture governed by the Qanun-e-Shahadat Order, 1984 (QSO), the Electronic Transactions Ordinance, 2002 (ETO), and the Prevention of Electronic Crimes Act, 2016 (PECA) was designed for human-generated electronic records, leaving severe statutory gaps regarding autonomous algorithmic outputs, generative deepfakes, and machine learning inferences.*

Objectives: *This study evaluates the legal admissibility of AI-generated evidence under Pakistani law, identifies procedural bottlenecks, critically assesses judicial precedents, and offers statutory and technical reform frameworks.*

Recommendations: *Legislative amendments to Article 164 of QSO, technical forensic validation protocols, judicial training modules at the judicial academies to the judges, and an AI certification framework are urgently required.*

Original Contribution: *This research establishes the first comprehensive statutory and jurisprudential framework tailored specifically for integrating AI evidence into Pakistan's evidentiary regime while upholding Article 10-A constitutional rights.*

Key Findings: *Pakistani courts currently lack standardized guidelines for evaluating the authenticity, explainability ("black box"), algorithmic bias, and chain of custody for autonomous AI artifacts, creating substantial risks under Constitutional guarantees of fair trial.*

Keywords: Artificial Intelligence, Evidence Law, Qanun-e-Shahadat Order 1984, Admissibility, Deepfakes, Judicial Approaches, Law Reform Pakistan, Digital Forensics.

1. Introduction

The global legal landscape is undergoing a paradigm shift driven by the integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies into public administration, law enforcement agencies, and forensic investigation. Algorithms now assist in identifying criminal suspects via facial recognition, analyzing mass surveillance CCTV feeds, extracting predictive insights from big data, and generating complex digital forensic audit logs. While these technological developments enhance investigative capacity, they introduce severe challenges to traditional evidence law, which was designed around human perception, documentary authenticity, and direct witness credibility.

In Pakistan, the administration of justice is strictly governed by statutory codes of evidence and procedure. As litigants and state prosecutors increasingly present algorithmic findings, automated forensic software outputs, and synthetically generated media (deepfakes) before courts, the legal system faces a fundamental stress test.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

Existing statutes, primarily the **Qanun-e-Shahadat Order, 1984 (QSO)**, the **Electronic Transactions Ordinance, 2002 (ETO)**, and the **Prevention of Electronic Crimes Act, 2016 (PECA)** recognize electronic documents in a broad sense. However, they lack explicit parameters to address autonomous algorithmic creation, neural network opacity, machine bias, and dynamic data processing.

Research Gap: While significant scholarship exists on electronic evidence in Pakistan, Pakistani legal literature lacks a comprehensive, doctrinally rigorous examination of *autonomous AI-generated evidence*. Existing studies blur the distinction between passive electronic storage (e.g., SMS, PDF files) and active algorithmic generation (e.g., deepfakes, ML predictive models, automated forensic analysis). This paper fills this critical scholarship gap.

Research Questions:

1. Is AI-generated evidence legally admissible under the existing statutory framework of Pakistan?
2. What specific statutory provisions regulate or restrict the admissibility of algorithmic and autonomous evidence?
3. How have Pakistani courts addressed technological and electronic evidence, and can these precedents be applied to AI systems?
4. What legislative, judicial, and technical reforms are required to establish robust admissibility standards for AI evidence in Pakistan?

Objectives & Significance: This research aims to provide an exhaustive legal evaluation of AI evidence under Pakistani jurisprudence, benchmark local standards against leading global jurisdictions (US, UK, EU), and propose concrete statutory amendments to preserve the integrity of the administration of justice and protect the constitutional right to a fair trial under Article 10-A of the Constitution of Pakistan, 1973.

2. Literature Review

The academic discourse on legal admissibility of AI evidence has expanded rapidly in Western jurisdictions, though scholarship in South Asia remains emergent. Scholarly literature can be categorized into four primary streams: international AI evidence doctrine, machine learning in criminal justice, digital forensics, and Pakistani electronic evidence literature.

International scholars such as Roth (2017) and Lederer (2019) have examined the problem of "machine testimony," arguing that traditional hearsay rules and confrontation rights are ill-equipped for automated system outputs. Roth contends that treating computer-generated data as traditional physical evidence fails to account for software bugs, training set biases, and algorithmic design errors. In the realm of machine learning in criminal justice, Ferguson (2018) highlights how predictive policing and automated risk-assessment algorithms perpetuate historical policing biases under the guise of objective mathematics.

In digital forensic science, Casey (2020) and Horsman (2021) emphasize that machine learning models introduce an unprecedented layer of opacity, often termed the "black box" problem where even software developers cannot fully retrace the precise decision path taken by a deep neural network. The European Legal Tech Association (2022) has emphasized the necessity of Explainable AI (XAI) in judicial proceedings to satisfy constitutional due process standards.

In Pakistan, legal scholarship has focused largely on electronic evidence under Article 164 of the QSO and PECA 2016. Scholars such as Khan (2020) and Ahmed & Chishti (2022) have analyzed judicial trends regarding CCTV footage, audio tape recordings, and mobile phone data. However, local scholarship has yet to address the specific nuances of generative AI, deepfake manipulation, autonomous algorithmic reports, or the evidentiary weight of

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

predictive algorithms. This paper addresses this exact gap by combining local statutory interpretation with advanced international AI governance frameworks.

3. Research Methodology

This study employs a multi-dimensional qualitative methodology structured around doctrinal legal research, statutory interpretation, case law analysis, and comparative law:

- **Doctrinal Legal Research:** Conducting an in-depth analytical evaluation of primary statutory texts, legislative provisions, legal rules, and judicial opinions governing evidence and technology in Pakistan.
- **Statutory Interpretation:** Applying established rules of statutory construction to analyze the scope and limits of the Qanun-e-Shahadat Order, 1984, the Electronic Transactions Ordinance, 2002, and the Prevention of Electronic Crimes Act, 2016.
- **Case Law Analysis:** Examining reported judgments from the Supreme Court of Pakistan and provincial High Courts to evaluate how judges currently interpret digital devices, forensic reports, and technical expertise.
- **Comparative Legal Analysis:** Benchmarking Pakistani standards against statutory and judicial frameworks in the United States (Federal Rules of Evidence, *Daubert* standard), the United Kingdom (PACE 1984, CJA 2003), and the European Union (EU AI Act 2024, GDPR).

Data Sources:

- *Primary Sources:* The Constitution of the Islamic Republic of Pakistan, 1973; Qanun-e-Shahadat Order, 1984; Electronic Transactions Ordinance, 2002; Prevention of Electronic Crimes Act, 2016; Punjab Forensic Science Agency Act, 2007; and binding judicial precedents (PLD, SCMR, PCrLJ, YLR).
- *Secondary Sources:* Treatises on evidence law, peer-reviewed international law journals, Law Reform Commission reports, and technical AI guidelines from recognized international standards organizations (ISO/ IEC).

Therefore, this paper utilizes doctrinal legal research, qualitative statutory interpretation, and a legal analysis involving the United States, the United Kingdom, and the European Union.

4. Understanding Artificial Intelligence and AI-Generated Evidence

To evaluate legal admissibility, law must establish clear technical taxonomies. Artificial Intelligence refers to computer systems capable of performing tasks that historically required human intelligence, such as visual perception, speech recognition, decision-making, and translation.

Technical Taxonomy of AI Technology

- **Machine Learning (ML):** Statistical algorithms that learn patterns from training data to make predictions or decisions without being explicitly programmed with rule-based instructions.
- **Deep Learning (DL):** Advanced ML utilizing multi-layered artificial neural networks capable processing high-dimensional unstructured data (e.g., images, raw audio).
- **Generative AI:** DL models (such as Generative Adversarial Networks [GANs] and Large Language Models [LLMs]) capable of creating novel content—text, realistic synthetic audio, images, and deepfake videos.
- **Predictive AI:** Systems that process historical datasets to calculate probabilities of future events, widely used in recidivism risk scores and predictive policing.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

4.1 Human-Generated vs. AI-Generated Evidence

In evidence law, a vital distinction exists between *AI-assisted evidence* and *AI-generated evidence*:

1. **AI-Assisted (Machine-Conveyed) Evidence:** Information recorded or transmitted by technology where the computer acts merely as a conduit or passive tool for human expression or basic measurement. Examples include an email, a standard CCTV recording, or a basic digital photograph. Authenticity relies on proving the device was functioning properly.
2. **AI-Generated (Machine-Created) Evidence:** Output autonomously created, synthesized, or inferred by an algorithmic system without direct human direction for the specific output content. Examples include a deepfake video generated by a GAN, an automated predictive policing risk profile, or an AI forensic software report that classifies latent fingerprints using neural network scoring.

4.2 Real-World Application Examples in Legal Proceedings

- **Automated CCTV Analytics & Facial Recognition:** AI tools that scan thousands of hours of footage, auto-identifying faces or license plates based on probability algorithms.
- **Voice Recognition & Audio Enhancement:** Algorithmic cleaning of noisy audio or automated speaker identification based on voiceprint matching.
- **Digital Forensic Software:** Automated tools (e.g., Cellebrite, EnCase AI modules) that scan raw hard drive dumps and autonomously group, flag, or reconstruct deleted files.
- **Predictive Forensic Reports:** Automated DNA probabilistic genotype software (e.g., STRmix) used to decipher complex, multi-person DNA mixtures in violent crime cases.

5. Legal Framework Governing AI-Based Evidence in Pakistan

5.1 Constitutional Framework

Any evidentiary rule in Pakistan must conform to Fundamental Rights guaranteed under Chapter 1, Part II of the Constitution of Pakistan, 1973:

- **Article 4:** Right of individuals to be dealt with in accordance with law.
- **Article 10-A:** Guarantee of the fundamental right to a fair trial and due process. Unexplainable, opaque AI outputs presented against an accused violate Article 10-A if the defense cannot cross-examine the underlying algorithmic process.
- **Article 14:** Right to privacy and dignity of person. Massive AI surveillance and facial recognition indexing without statutory safeguards directly impinge upon constitutional privacy protections.
- **Article 19-A:** Right to information, requiring state institutions to maintain transparency in algorithmic tools used in public prosecution.

5.2 The Qanun-e-Shahadat Order, 1984 (QSO)

The QSO is the primary statutory instrument governing evidence in Pakistan. Key provisions relevant to AI include:

- **Article 2(1)(e) - Definition of "Document":** Defines a document as any matter expressed or described upon any substance by means of letters, figures, or marks, including data, information, or records created or stored electronically. While broad enough to encompass AI files, it treats them as static records.
- **Article 59 - Expert Opinion:** Permits courts to form an opinion upon a point of foreign law, science, art, or identity. An AI tool itself cannot take the stand; thus, AI evidence must currently enter court through a human "expert witness" under Article 59, who must explain the system's operation.
- **Article 73 & 84 - Primary vs. Secondary Evidence:** Sets strict hierarchies for original records. Defining what constitutes the "primary original" of an AI dynamic cloud-based output remains legally challenging.
- **Article 117 & 129 - Burden of Proof & Presumptions:** The burden rests on the party

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

introducing AI evidence to establish its authenticity. However, Article 129 permits courts to presume the existence of certain facts—a presumption that must not be blindly extended to machine accuracy.

- **Article 164 - Modern Devices Provision:** The primary statutory gateway for non-traditional evidence:

> *"In such cases as the Court may consider appropriate, the Court may allow any evidence to be produced that may have become available because of modern devices or techniques."*

While Article 164 provides immense judicial discretion, it lacks explicit technical prerequisites for verifying AI reliability, neural network weight integrity, or algorithmic error rates.

5.3 Electronic Transactions Ordinance, 2002 (ETO)

Sections 3, 7 and 9 of the ETO grant legal recognition to electronic documents, signatures, and automated information systems. Section 3 gives the validity of the electronic generated documents through these are not attested by the witness. Section 7 gives recognition to the electronic signatures. Section 9 creates a presumption that an electronic document originating from an automated system was generated correctly if the system was operating normally. However, this statutory presumption was drafted for basic automated e-commerce transactions, not autonomous probabilistic AI models.

5.4 Prevention of Electronic Crimes Act, 2016 (PECA)

Sections 26, 27, 33 and 37 of PECA regulate the seizure, collection, and forensic evaluation of digital evidence by designated agencies (such as the FIA Cybercrime Wing). Section 37 provides that a digital forensic report prepared by an authorized forensic agency is admissible. Yet, PECA provides no auditing guidelines for when forensic agencies employ proprietary AI software with secret, undisclosed source code.

6. Comparative Legal Analysis

Jurisdiction	Primary Statutory / Evidentiary Framework	Admissibility & Reliability Test	Transparency & Accountability Safeguards
United States	Federal Rules of Evidence (FRE Rule 702, Rule 901)	**Daubert Standard:** Judge acts as gatekeeper evaluating (1) testability, (2) peer review, (3) known error rate, (4) standards control, and (5) general scientific acceptance.	Mandatory disclosure of software validation studies; defense access to source code under protective orders in criminal cases.
United Kingdom	Police & Criminal Evidence Act (PACE 1984); Criminal Justice Act 2003	Rebuttable presumption that computer systems are working properly, but complex AI requires independent expert testimony under CJA section 114.	Crown Prosecution Service (CPS) guidelines require full disclosure of algorithmic tools used in evidence generation.
European Union	EU Artificial Intelligence Act (2024); GDPR (Art. 22)	Strict risk-based classification. High-risk AI (forensics, law enforcement) must satisfy rigorous pre-market compliance and testing.	Mandatory Explainable AI (XAI), human oversight, complete audit trails, and prohibition of purely automated profiling without human intervention.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

Pakistan	QSO 1984 (Art. 164); ETO 2002; PECA 2016	Discretionary admission under Article 164 QSO, relying heavily on standard chain of custody and human expert endorsement under Art. 59.	No statutory requirement for algorithm auditing, source code disclosure, or XAI compliance; significant gap in procedural safeguards.

7. Judicial Responses in Pakistan

The judiciary in Pakistan has progressively addressed electronic evidence, moving from initial skepticism to structured acceptance under strict procedural conditions. However, case law remains centered on human-generated digital artifacts.

PLD 2007 Kar. 448

Audio Video CD's etc.
Audio video recorded cassettes, CDs are admissible piece of evidence; however, the authenticity of same is always subject to proof in case the party against which it can be used disputed or denied the authenticity and information contained in the said electronic documents. Production of CDs as evidence collected by prosecution through modern devices not be disallowed.

Naveed Asghar v. State (PLD 2021 SC 600)
The Apex Court emphasized that while modern electronic evidence is admissible under Article 164, its reliance as sole substantive evidence requires extreme caution. The Court held that technological evidence must satisfy constitutional standards of fair trial under Article 10-A, requiring absolute proof against fabrication or technical anomaly.

Sughra Bibi v. State (PLD 2018 SC 595) & DNA Precedents
In evaluating complex scientific evidence (DNA profiling), the Supreme Court ruled that forensic reports generated by standardized laboratories (like PFSA) carry strong corroborative value. However, the Court maintained that scientific evidence must be presented by a qualified expert who can be cross-examined on laboratory procedures.

Critique: Fitting AI into Existing Jurisprudence:
Pakistani courts currently attempt to force AI outputs into the traditional framework of "electronic records" under Article 164 or "expert testimony" under Article 59. This creates a severe legal fiction. An expert witness calling an AI forensic tool to the stand cannot explain the neural network's internal probabilistic calculations if the software is proprietary or unexplainable. Judicial reliance on traditional chain-of-custody rules fails when faced with generative deepfakes, where the physical hash of a file may be unbroken, yet the content within the file is entirely synthetic.

8. Challenges in Admissibility of AI-Generated Evidence

Integrating AI evidence into Pakistani courtrooms encounters ten severe statutory, technical, and procedural bottlenecks:

A. Authenticity and Deepfakes

Generative Adversarial Networks (GANs) can synthesize hyper-realistic video, voice, and document files. Traditional authentication under Article 73 QSO relies on verifying that a document is what it purports to be. In a deepfake scenario, traditional digital signatures or metadata can be forged, making visual or auditory verification by human judges completely

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

unreliable.

B. Reliability and Hallucination

Machine learning models, particularly generative models and probabilistic classifiers, are subject to "hallucinations" and statistical drift. Unlike deterministic software, an AI model can yield different outputs when exposed to minor environmental noise, making baseline legal reliability difficult to establish.

C. Explainability (The "Black Box" Problem)

Deep neural networks operate across millions of parameters and hidden layers. The inability to retrace step-by-step logic prevents the defense from understanding how an AI reached a specific conclusion, directly violating the right to cross-examination guaranteed under Article 133 QSO and Article 10-A of the Constitution.

D. Algorithmic Bias

AI models reflect the biases inherent in their training datasets. If an AI facial recognition system trained predominantly on Western demographic datasets is deployed in Pakistan, error rates spike significantly among local populations, leading to misidentification and wrongful prosecution.

E. Chain of Custody in Dynamic Cloud Environments

Unlike a physical hard drive seized under Section 33 of PECA, modern enterprise AI applications process data in real-time across decentralized cloud networks. Maintaining an unbroken forensic chain of custody for continuous data streams is virtually impossible under static procedural rules.

F. Privacy Concerns

Automated AI evidence gathering often relies on mass scraping of public and private data, surveillance cameras, and biometrics. In the absence of comprehensive data protection legislation in Pakistan, such collection practices violate Article 14 of the Constitution.

G. Accountability and Liability

When an AI evidence tool generates a false positive that leads to an unlawful conviction, establishing legal liability whether on the developer, the law enforcement agency, or the expert witness remains unaddressed in Pakistani tort and criminal jurisprudence.

H. Cybersecurity and Adversarial Attacks

AI models are vulnerable to adversarial attacks, where tiny, imperceptible perturbations added to an input image or file trick the algorithm into misclassifying the output (e.g., altering a stop sign image so an AI reads it as a speed limit sign).

I. Lack of Judicial Expertise

The trial judiciary and prosecution in Pakistan generally lack technical training in computer science, statistics, and machine learning, making them highly vulnerable to "automation bias" the tendency to uncritically trust automated computer outputs.

J. Absence of AI-Specific Legislation

Pakistan currently possesses no dedicated AI regulatory statute or specific evidentiary rules governing automated decision-making systems, leaving trial judges with unguided discretion under Article 164 QSO.

9. Comprehensive Recommendations

To establish a modern, constitutionally sound evidentiary framework for AI evidence, Pakistan must execute coordinated reforms across four dimensions:

9.1 Legislative Reforms

- **Amendment to Article 164 of QSO 1984:** Insert a specific Proviso establishing statutory preconditions for AI evidence:

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

> *"Provided that where evidence is generated, analyzed, or synthesized by an autonomous Artificial Intelligence or Machine Learning system, such evidence shall only be admissible if accompanied by a Technical Reliability Certificate attesting to the system's error rate, software validation, and explainability."*

- **Statutory Definition of AI Records:** Amend Article 2(1)(e) of the QSO to distinguish between passive electronic records and dynamic algorithmic outputs.
- **Enactment of an AI Governance & Data Protection Act:** Legislate comprehensive data protection and AI oversight statutes establishing mandatory standards for algorithmic systems deployed in law enforcement.

9.2 Judicial Reforms

- **Specialized Bench & Judicial Training:** Form specialized cyber and legal-tech benches in High Courts and establish comprehensive AI training modules at the Federal Judicial Academy (FJA) and the provincial judicial academies.
- **Adoption of the US *Daubert* Reliability Criteria:** Instruct trial courts to act as strict gatekeepers, evaluating AI software testability, peer-reviewed validation, known error rates, and industry standards before admitting AI reports.
- **Mandatory "Human-in-the-Loop" Doctrine:** Establish a binding judicial rule that no conviction or adverse civil decree may rest solely on an autonomous AI output without independent corroborating human evidence.

9.3 Institutional Reforms

- **National AI Forensic Regulatory Authority (NAIFRA):** Establish an independent statutory body tasked with auditing, certifying, and setting technical standards for AI tools used in forensic science.
- **Source Code Deposit Protocols:** Mandate that proprietary software vendors supplying AI forensic tools to state agencies must deposit source code into secure escrow for independent judicial auditing when challenged in court.
- **Upgradation of Forensic Laboratories:** Equip the Punjab Forensic Science Agency (PFSA) and federal laboratories with advanced deepfake detection algorithms and neural network forensic suites.

9.4 Technical Standards & Protocols

- **Implementation of Explainable AI (XAI):** Require all AI forensic reports submitted under Article 59 QSO to include interpretable feature-importance visualizations (e.g., SHAP or LIME scores) explaining the decision logic.
- **Cryptographic Hashing for Live Data Streams:** Mandate continuous blockchain-based or cryptographic timestamping for cloud-based AI logs to preserve chain of custody.
- **Bias Auditing Protocols:** Standardize mandatory demographic and contextual bias testing for any facial recognition or predictive software before deployment in criminal investigations.

10. Conclusion

Artificial Intelligence represents a double-edged sword for Pakistan's legal system. On one hand, automated analytics and forensic tools offer unprecedented capabilities to combat complex cybercrime, process vast datasets, and assist law enforcement. On the other hand, autonomous algorithms, opaque deep learning models, and deepfakes threaten to undermine core evidentiary principles, cross-examination rights, and the fundamental constitutional guarantee of a fair trial under Article 10-A.

Pakistan's existing statutory framework while flexible under Article 164 of the Qanun-e-Shahadat Order, 1984 is fundamentally inadequate for the age of autonomous AI. Treating dynamic, probabilistic machine learning outputs as traditional electronic documents creates

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

unacceptable legal vulnerabilities. To prevent miscarriages of justice, Pakistan must urgently enact legislative amendments, adopt rigorous judicial gatekeeping standards inspired by international best practices, establish institutional AI auditing bodies, and train its judiciary. By proactively constructing a robust, constitutionally aligned AI evidence framework, Pakistan can harness technological innovation while safeguarding the rule of law and human rights in the digital age.

References

1. Ahmed, S. and Chishti, M.A., 2022. 'Electronic Evidence under Pakistani Jurisprudence: A Critical Analysis of Article 164 of the Qanun-e-Shahadat Order 1984', *Pakistan Law Review*, 13(2), pp. 45-68.
2. Casey, E., 2020. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 4th edn. London: Academic Press.
3. European Parliament and Council, 2024. *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
4. Ferguson, A.G., 2018. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.
5. Horsman, G., 2021. 'Explainable AI in digital forensics', *Forensic Science International: Digital Investigation*, 38, p. 301245.
6. PLD 2007, Karachi, 448.
7. Khan, A.U., 2020. 'Forensic Science in Criminal Justice: Operational Vulnerabilities of the Punjab Forensic Science Agency', *Lahore University of Law Journal*, 8(1), pp. 112-134.
8. Lederer, F.I., 2019. 'The Regulatory and Evidentiary Implications of Artificial Intelligence in the Courtroom', *Syracuse Law Review*, 68(2),
pp. 317-348.
9. Naveed Asghar v. State, 2021. Supreme Court of Pakistan. *PLD 2021 SC 600.*
10. Roth, A., 2017. 'Machine Testimony', *Yale Law Journal*, 126(7), pp. 1972-2053.
11. Sughra Bibi v. State, 2018. Supreme Court of Pakistan. *PLD 2018 SC 595.*
12. United States Supreme Court, 1993. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579.