REVIEW OF CRIME, PEACE AND SOCIETY
ISSN (O): 3079-6105, ISSN (P): 3079-6091
Vol. 3, No. 8, 2026, 223-236

Admissibility of Digital Evidence and Use of Emerging Artificial Intelligence Tools in the Criminal Justice System of Pakistan: A Critical Analysis of the Legislative Framework

Asif Iqbal[1]

Abstract

This study critically examines the legislative framework governing the admissibility of digital evidence and the integration of emerging artificial intelligence tools within Pakistan's criminal justice system. While Pakistan has taken incremental steps through the Electronic Transactions Ordinance 2002, the Qanun-e-Shahadat Order 1984, and the Prevention of Electronic Crimes Act 2016 to recognize electronic evidence, the legal infrastructure remains fundamentally unprepared for the evidentiary complexities introduced by AI-driven investigative and adjudicative technologies. The study adopts a qualitative doctrinal methodology, analyzing secondary legal materials including statutes, case law, and scholarly commentary to identify critical gaps between statutory text and technological reality. Findings reveal that while Article 164 of the Qanun-e-Shahadat Order provides a broad discretionary gateway for modern device evidence, there exists no specific framework addressing algorithmic transparency, reliability standards, or the evidentiary weight of AI-generated outputs. The absence of disclosure obligations for automated identification systems and the lack of judicial guidance on machine-generated evidence create significant risks for fair trial guarantees. The study concludes that Pakistan requires targeted legislative reform to establish admissibility standards tailored to algorithmic evidence, alongside institutional capacity-building within the judiciary and investigative agencies.

Article History
Received 22 September 2026
Accepted 14 October 2026
Published 20 October 2026
Corresponding Author*
OPEN ACCESS
Keywords
digital evidence; artificial intelligence; admissibility; Qanun-e-Shahadat; criminal justice; Pakistan.

1. Introduction

1.1 Background of the Study

The transformation of criminal justice systems by digital technologies represents one of the most significant developments in contemporary legal practice. Across jurisdictions, courts increasingly confront evidence derived from information systems ranging from conventional electronic documents and communications metadata to sophisticated outputs generated by artificial intelligence tools deployed in policing and prosecution. Pakistan, as a jurisdiction navigating the intersection of traditional evidentiary doctrine and rapid technological change, presents a particularly instructive case study of legislative adaptation and its limits (Adil, 2024).

[1] Deputy Prosecutor General, Anti-Terrorism Court, Faisalabad, Pakistan. asifiqbalsp@gmail.com

The foundational legislative response to electronic evidence in Pakistan emerged through the Electronic Transactions Ordinance 2002, which established the legal recognition of electronic records and signatures. This was followed by amendments to the Qanun-e-Shahadat Order 1984, the primary statute governing evidence law, introducing provisions such as Article 78-A concerning proof of electronic signatures and documents. The Prevention of Electronic Crimes Act 2016 further supplemented this framework by defining key concepts including "data," "information system," and "device," while establishing investigative mechanisms for electronic crimes. These legislative developments reflected a recognition that the traditional preference for ocular testimony and documentary evidence could no longer adequately serve the ends of criminal justice in an information age (Akbar et al., 2025).

However, the trajectory of technological change has outpaced legislative reform. The contemporary landscape of criminal investigation in Pakistan increasingly features artificial intelligence applications facial recognition systems deployed in Safe City projects, automated number plate recognition technologies, predictive policing analytics, and AI-assisted legal research tools within judicial institutions. The National Guidelines for the Use of Artificial Intelligence in Judicial Institutions, issued in April 2026, acknowledged the growing role of AI in judicial functions while emphasizing human oversight and transparency principles. Yet these guidelines operate as policy instruments rather than binding evidentiary rules, leaving critical questions unanswered regarding the admissibility of AI-generated or AI-processed evidence in criminal proceedings. The gap between technological deployment and evidentiary regulation constitutes the central problematic of this study (Javed et al., 2026).

1.2 Significance and Scope of the Study

The significance of this research derives from the convergence of two pressing concerns within Pakistan's criminal justice system. First, the admissibility of digital evidence remains contested and inconsistently applied despite legislative recognition. Scholarly and judicial commentary has observed that while digital evidence may have achieved formal status as primary evidence for admissibility purposes, its weight and appreciation by courts remain discretionary and often sceptical. Second, the introduction of AI tools into investigative and adjudicative processes raises profound questions about reliability, transparency, and the ability of accused persons to challenge machine-generated conclusions. These concerns are particularly acute in a jurisdiction where comprehensive data protection legislation remains unenacted and where the constitutional right to a fair trial under Article 10-A demands meaningful opportunity to confront adverse evidence (Abdullah et al., 2026).

The scope of this study is deliberately bounded to the legislative framework governing admissibility and the treatment of AI-derived evidence within criminal proceedings. It encompasses the Electronic Transactions Ordinance 2002, relevant provisions of the Qanun-e-Shahadat Order 1984, the Prevention of Electronic Crimes Act 2016, and the National Guidelines on AI in Judicial Institutions 2026. The study does not engage with substantive criminal law offences or with the operational details of specific AI systems deployed by law enforcement agencies, except insofar as these bear upon evidentiary questions. The analysis is confined to the criminal justice context, although it acknowledges that parallel issues arise in civil proceedings (Afzal, 2025).

1.3 Research Objectives

i. To critically examine the existing legislative provisions governing the admissibility of digital evidence within Pakistan's criminal justice system.
ii. To identify the extent to which the current legal framework addresses the evidentiary challenges posed by artificial intelligence tools.
iii. To analyze judicial interpretation of digital evidence admissibility through relevant case law and its implications for AI-generated evidence.
iv. To compare Pakistan's legislative approach with international standards and scholarly perspectives on algorithmic evidence.
v. To propose targeted legislative and institutional reforms to enhance the framework's capacity to accommodate emerging technologies.

2. Literature Review

2.1 Conceptual Framework and Key Definitions

The conceptual architecture of this study requires precise delineation of its central terms. "Digital evidence" encompasses any information of probative value stored or transmitted in digital form, including but not limited to electronic documents, communications metadata, computer-generated records, and outputs from information systems. The Prevention of Electronic Crimes Act 2016 provides a definitional foundation, characterizing "data" as including content data and traffic data, and defining "information system" as an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information. These definitions are broad enough to encompass most contemporary forms of digital evidence, though they do not specifically address the distinctive characteristics of AI-generated outputs (Tahir et al., 2025).

"Artificial intelligence tools" in the criminal justice context refer to computational systems capable of performing tasks that traditionally require human cognition, including pattern recognition, classification, prediction, and natural language processing. Within Pakistan's emerging landscape, these tools include facial recognition technologies deployed in surveillance infrastructure, automated number plate recognition systems, predictive policing algorithms, and AI-assisted legal research platforms used by courts. The National Guidelines on AI in Judicial Institutions characterize AI as an "assistive technology" intended to support rather than replace human judgment, emphasizing principles of human-centricity, transparency, and accountability.

"Admissibility" denotes the legal threshold determining whether evidence may be considered by a court in adjudicating a matter. In Pakistan's evidence law framework, admissibility is governed by the Qanun-e-Shahadat Order 1984, which establishes categories of relevance and specific rules for documentary and electronic evidence. Article 164 of the Order provides a discretionary gateway for evidence "that may have become available because of modern devices or techniques," a provision that has been central to judicial acceptance of digital evidence. The conceptual tension animating this study lies in the fact that Article 164's broad language was conceived before the emergence of algorithmic systems whose evidentiary

reliability cannot be assessed through conventional authentication mechanisms (Rafique et al., 2026).

2.2 Theoretical Perspectives and Models

The theoretical foundations for analyzing digital evidence admissibility draw upon several intersecting frameworks. The "reliability principle" in evidence law holds that the admissibility of any evidence depends fundamentally upon its capacity to assist the trier of fact in reaching accurate conclusions, which in turn requires some assurance of authenticity and integrity. For digital evidence, this principle manifests in requirements relating to chain of custody, forensic verification, and system reliability. The challenge posed by AI tools is that their internal operations the weighting of variables in a neural network, for instance are often opaque even to their developers, creating what scholars term the "black box" problem. This opacity complicates the application of reliability-based admissibility standards (Nazir et al., 2025).

A second theoretical lens is provided by the "fair trial" framework enshrined in Article 10-A of the Constitution of Pakistan. The Supreme Court has interpreted this provision as requiring procedural fairness, including an effective opportunity to challenge evidence relied upon in legal proceedings. For AI-generated evidence, meaningful challenge requires access to information about the system's functioning, its error rates, and the basis for its outputs information that is frequently unavailable or protected as proprietary. The theoretical tension between the adversarial system's assumption of party access to evidence and the proprietary nature of algorithmic systems constitutes a significant doctrinal challenge.

Third, the "precautionary approach" to technological evidence suggests that where the reliability of a novel evidentiary source cannot be adequately assessed, courts should exercise caution in admitting it, or should require corroboration or enhanced disclosure as conditions of admissibility. This approach finds expression in Pakistani judicial decisions requiring forensic verification of video evidence and testimony from the person who prepared CCTV footage. Extending this logic to AI-generated evidence would suggest that admissibility should be conditioned upon disclosure of the algorithmic basis for the output, absent which the evidence should be excluded (Muhammad, 2026).

2.3 Review of National Literature

The Pakistani legal literature on digital evidence has developed incrementally alongside legislative and judicial developments. Commentary on the Electronic Transactions Ordinance 2002 has emphasized its transformative effect in declaring electronic records admissible as primary evidence, thereby dispelling the perception that digitally stored information constitutes hearsay. The amendments to the Qanun-e-Shahadat Order introducing Articles 73 (Explanation 3) and 78-A have been analyzed as establishing presumptions of system reliability and requirements for proving electronic signatures and documents. Judicial decisions have applied these provisions to admit emails, SMS records, and video footage, while consistently emphasizing the necessity of proof of authenticity and genuineness (Iqbal et al., 2025).

The more recent literature on AI in Pakistan's justice system remains nascent but is growing. The Oxford Institute's AI Justice Atlas entry for Pakistan, published in 2026, documented the rapid adoption of AI tools in law enforcement and judicial administration while noting the absence of comprehensive AI-specific legislation. The National Guidelines for AI in Judicial Institutions have been characterized as an important first step toward principled governance, though their non-binding character and limited focus on evidentiary questions have been noted. Scholarly analysis has identified a significant regulatory gap: the Qanun-e-Shahadat Order and the Prevention of Electronic Crimes Act do not expressly address issues such as algorithmic transparency, auditability, or disclosure requirements for AI-generated evidence. This gap has been framed as constitutionally problematic given the fair trial implications of admitting unchallengeable algorithmic conclusions (Ali et al., 2026).

2.4 Review of International Literature

The international literature on digital evidence and AI in criminal justice offers frameworks that, while not directly transplantable to Pakistan's legal system, provide valuable comparative perspectives. European scholarship has emphasized the criteria of authenticity, reliability, and integrity as the tripartite foundation for digital evidence admissibility, with particular attention to chain of custody documentation in digital contexts. The "expert paradox" has been identified as a challenge: as AI and automated tools become more sophisticated, courts may become more reliant on expert testimony to interpret their outputs, potentially exacerbating inequality of arms between prosecution and defence (Javaid & Saleem, 2025).

International human rights frameworks have increasingly addressed the implications of algorithmic decision-making in criminal justice. The principles of transparency, accountability, and the right to an effective remedy have been applied to AI systems in policing and prosecution, with scholars arguing that defendants have a right to understand the basis of evidence used against them. The concept of "algorithmic evidence disclosure" has gained traction, with proposals that any algorithmic identification evidence should be subject to mandatory pre-conditions of disclosure regarding the system's role, confidence levels, and known error rates. These perspectives resonate with Pakistan's constitutional fair trial guarantees, suggesting that international standards may inform the interpretation of domestic provisions (Shah & Ahmed, 2026).

2.5 Research Gap

Despite growing recognition of AI's integration into Pakistan's criminal justice institutions, no comprehensive doctrinal analysis has examined the specific question of admissibility standards for AI-generated or AI-processed evidence under the existing legislative framework. The literature addresses digital evidence and AI governance as separate concerns, leaving the intersection where algorithmic tools produce evidentiary outputs subject to the Qanun-e-Shahadat Order unexamined. This study addresses that gap by critically analyzing whether current admissibility provisions can accommodate algorithmic evidence and identifying the specific legislative reforms required.

3. Research Methodology

3.1 Research Design: Qualitative Doctrinal Approach

This study adopts a qualitative doctrinal research design, which is appropriate for legal scholarship concerned with the interpretation, coherence, and adequacy of legislative provisions. Doctrinal methodology involves the systematic analysis of legal rules derived from primary legal sources, their interpretation by courts, and their evaluation against internal and external criteria of coherence and effectiveness. The qualitative dimension of this design acknowledges that legal doctrine is not merely a collection of rules but a system of meaning that must be understood in context including the technological, institutional, and constitutional environment within which it operates.

The doctrinal approach is particularly suited to the research questions posed. The study does not seek to measure the frequency of AI evidence admission or to survey judicial attitudes; such empirical inquiries would require methodologies outside the scope of this project. Instead, it asks whether the existing legislative framework provides adequate resources for courts confronting AI-generated evidence, and if not, what specific doctrinal reforms would address the deficiency. These questions are answered through close reading of statutory text, analysis of judicial interpretation, and critical comparison with international standards and scholarly commentary. The qualitative orientation permits attention to nuance and ambiguity in legal language that quantitative approaches might obscure.

3.2 Sources of Data: Secondary Legal Materials

Consistent with the doctrinal design, this study relies exclusively on secondary legal materials. No primary data collection through interviews, surveys, questionnaires, or fieldwork was undertaken. The sources consulted include: (a) legislative instruments, principally the Electronic Transactions Ordinance 2002, the Qanun-e-Shahadat Order 1984, and the Prevention of Electronic Crimes Act 2016, together with the National Guidelines for the Use of Artificial Intelligence in Judicial Institutions 2026; (b) reported judicial decisions of Pakistani superior courts addressing digital evidence admissibility; (c) scholarly articles, commentaries, and monographs on evidence law, digital evidence, and AI governance; and (d) policy documents and reports from governmental and non-governmental institutions.

The exclusive reliance on secondary materials is a deliberate methodological choice rather than a limitation imposed by circumstance. The research questions concern the content and adequacy of legal doctrine, not the practices or perceptions of legal actors. Doctrinal analysis of legislative and judicial texts, supplemented by scholarly interpretation, constitutes the appropriate evidentiary basis for answering such questions. The absence of empirical data does not diminish the validity of the study's conclusions regarding the textual and interpretive resources available within the legal framework, though it does mean that claims about how courts actually handle AI evidence in practice must be framed with appropriate caution.

3.3 Method of Data Collection and Analysis

Data collection proceeded through systematic identification and retrieval of relevant legal materials. Legislative texts were obtained from official sources, including the Pakistan Code repository and the Law and Justice Commission of Pakistan. Judicial decisions were identified through searches of reported case law databases and through citation analysis of leading

authorities on digital evidence. Scholarly literature was located through academic databases and through the references contained in the legal and policy documents identified in the initial search phase. The collection process was iterative, with each source consulted yielding references to further materials of relevance.

Analysis proceeded through three stages. First, textual analysis of statutory provisions involved close reading of the relevant articles and sections to identify their scope, conditions, and ambiguities. Second, interpretive analysis examined how courts have applied these provisions to digital evidence, identifying patterns and inconsistencies in judicial reasoning. Third, normative analysis evaluated the adequacy of the existing framework against the requirements of reliability and fair trial, drawing upon scholarly commentary and comparative perspectives to identify deficiencies and propose reforms. This three-stage process permits both descriptive accuracy and critical evaluation.

3.4 Scope, Limitations and Ethical Considerations

The scope of this study is confined to the criminal justice context and to the specific question of admissibility of digital and AI-generated evidence. It does not address civil evidence, administrative proceedings, or the substantive law of electronic crimes. The temporal scope extends from the enactment of the Electronic Transactions Ordinance 2002 to the present, with particular attention to developments since the Prevention of Electronic Crimes Act 2016 and the 2026 AI Guidelines.

Several limitations should be acknowledged. The absence of empirical data means that conclusions about judicial practice rest upon reported decisions, which may not be representative of unreported cases or of the routine handling of digital evidence in trial courts. The rapidly evolving nature of both technology and regulation means that the analysis reflects the legal position at the time of writing and may require revision as new legislation or judicial decisions emerge. The study does not purport to offer a comprehensive account of AI deployment in Pakistani law enforcement, but rather focuses on the evidentiary implications of such deployment.

Ethical considerations in doctrinal research centre on accuracy and fairness in the representation of legal sources and scholarly positions. All legislative provisions and judicial decisions are discussed with fidelity to their text and context. Where the study advances critical evaluations, these are grounded in reasoned analysis rather than polemic. The absence of human subjects means that the research poses no risks of harm to individuals, and the use of publicly available legal materials raises no confidentiality concerns.

4. Results and Discussion

4.1 Presentation of Key Legal Findings

The analysis reveals a legislative framework that has achieved formal recognition of digital evidence while leaving critical gaps in its capacity to govern AI-generated outputs. The Electronic Transactions Ordinance 2002 established the foundational principle that no document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity, proof or enforceability on the ground that it is in

electronic form. This provision removed the categorical barrier to electronic evidence that had previously characterized Pakistani evidence law. The Qanun-e-Shahadat Order was amended to introduce Explanation 3 to Article 73, providing that a printout or other output of an automated information system shall not be denied the status of primary evidence solely for the reason that it was generated, sent, received or stored in electronic form, with a presumption that the system was in working order at all material times.

Article 78-A of the Qanun-e-Shahadat Order addresses the proof of electronic signatures and documents, requiring that where an electronic document is alleged to have been signed or generated by a person through an information system and such allegation is denied, the application of a security procedure must be proved. Article 164, the provision most frequently invoked for digital evidence, permits courts to allow production of "any evidence that may have become available because of modern devices or techniques". The Prevention of Electronic Crimes Act 2016 provides definitions of data, information system, device, and related concepts that are broad enough to encompass AI outputs, but the Act is primarily an offence-creating and investigative statute rather than an evidentiary one.

The National Guidelines for the Use of Artificial Intelligence in Judicial Institutions, issued in 2026, represent the most recent policy development. The Guidelines articulate principles of human-centricity, ethical and responsible use, data protection, and capacity building, and they permit AI-assisted applications including case management, legal research, and the preparation of initial summaries. Critically, however, the Guidelines are addressed to judicial institutions and their internal use of AI; they do not establish admissibility standards for AI-generated evidence produced by investigative agencies or private parties. They therefore leave the core evidentiary question unaddressed.

4.2 Analysis of Statutory Provisions and Case Law

Judicial interpretation of the digital evidence provisions reveals a consistent emphasis on authenticity and proof of genuineness, but an absence of engagement with the distinctive challenges of algorithmic evidence. In the context of video evidence, courts have held that mere production of CCTV footage is insufficient unless the person who prepared the footage is examined and a forensic report establishes that it has not been edited. This requirement of authentication through testimony and forensic verification reflects a sound appreciation of the manipulability of digital recordings. However, it presumes that the evidence in question is a recording of a physical event that can be verified against its source. AI-generated evidence, by contrast, may involve no recording of an external event at all a facial recognition match, for instance, is an algorithmic conclusion rather than a recording, and there is no "person who prepared" it in the sense contemplated by the case law.

The Supreme Court's decision in the Ahmed Omar Sheikh case established conditions for video evidence admissibility, requiring explanation of acquisition and a forensic report confirming absence of editing. The Lahore High Court has admitted SMS records as strong evidence under Article 164, treating such records as primary evidence. These decisions demonstrate judicial willingness to engage with digital evidence within the existing statutory framework. Yet they also reveal the framework's limitations: the authentication paradigm

assumes evidence that can be verified against an external reality, not evidence that is itself the product of an algorithmic process whose internal logic is not transparent to the court.

The constitutional dimension is significant. Article 10-A's guarantee of a fair trial has been interpreted to require procedural fairness, including an effective opportunity to challenge evidence relied upon in legal proceedings. When evidence consists of an algorithmic output whose basis cannot be examined because the system's proprietary nature prevents disclosure, or because the algorithm's complexity defies human comprehension the meaningfulness of the opportunity to challenge is called into question. The existing statutory provisions provide no mechanism for compelling disclosure of algorithmic methodology, error rates, or the basis for a particular output. The court's discretion under Article 164 to admit modern device evidence is not accompanied by any corresponding power to order disclosure of the information necessary for effective challenge.

4.3 Comparison with Existing Scholarly Views

The findings align with scholarly observations that Pakistan's legislative framework for digital evidence is both formally progressive and substantively incomplete. The characterization of digital evidence as primary for admissibility purposes but still regarded as circumstantial in weight reflects a judicial caution that has been noted in policy discussions. Scholarly analysis has identified the absence of provisions addressing algorithmic transparency, auditability, or disclosure requirements for AI-generated evidence as a significant constitutional deficiency. The proposals advanced in that analysis including a new Article 164-A establishing an Algorithmic Evidence Disclosure Standard, a statutory Right to Explanation, and mandatory Algorithmic Impact Assessments for high-risk systems represent the most detailed reform agenda currently available.

International scholarship on digital evidence admissibility emphasizes the tripartite criteria of authenticity, reliability, and integrity, and identifies AI and automation as challenges for authentication and expert interpretation. The observation that machine-generated evidence lacks transparency and raises questions about who constitutes the "witness" to an algorithmic conclusion resonates with the Pakistani context, where the adversarial system presumes that evidence can be tested through cross-examination of a person who can explain its basis. Where no such person exists or where the explanation is inaccessible the adversarial mechanism is disabled.

The National Guideline's articulation of human oversight and transparency principles provides a policy foundation that could be extended into evidentiary rules, but the Guidelines themselves are not framed in terms of admissibility. The gap between policy principle and binding evidentiary doctrine remains unbridged.

4.4 Implications of the Findings

The implications of these findings are both doctrinal and institutional. Doctrinally, the absence of specific provisions for AI-generated evidence means that courts must stretch the existing framework principally Article 164 and the authentication requirements developed in case law to accommodate a category of evidence for which it was not designed. This stretching risks

either the uncritical admission of unreliable algorithmic outputs or the exclusion of potentially probative evidence for want of a party capable of satisfying authentication requirements. Neither outcome serves the interests of justice.

Institutionally, the findings suggest that judicial capacity to evaluate AI-generated evidence is a critical variable. The National Guideline's emphasis on capacity building is apposite, but training alone cannot substitute for legal standards that specify what must be disclosed and what conditions must be satisfied before algorithmic evidence is admitted. The absence of such standards places judges in the position of adjudicating admissibility without a legislative framework to guide their discretion, increasing the risk of inconsistency and of outcomes driven by the relative resources of the parties rather than by the reliability of the evidence.

The fair trial implications are particularly significant. If accused persons cannot obtain information about the algorithmic systems used to generate evidence against them, their Article 10-A right to challenge that evidence is rendered illusory. The existing framework provides no statutory right to such information, and the discretionary power under Article 164 does not carry with it any disclosure obligation. This constitutional dimension elevates the reform agenda from a matter of technical evidentiary improvement to a question of fundamental rights protection.

5. Conclusion

5.1 Summary of Major Findings

This study has examined the legislative framework governing digital evidence admissibility in Pakistan and assessed its capacity to accommodate AI-generated evidence within criminal proceedings. The findings reveal a framework that has successfully established the formal admissibility of electronic records through the Electronic Transactions Ordinance 2002 and the amendments to the Qanun-e-Shahadat Order 1984, including Article 73 Explanation 3 and Article 78-A. Article 164 has provided courts with broad discretion to admit evidence from modern devices, and judicial decisions have applied this provision to video recordings, SMS records, and other digital materials, consistently emphasizing requirements of authenticity and forensic verification.

However, the framework contains no provisions specifically addressing AI-generated or AI-processed evidence. The definitions in the Prevention of Electronic Crimes Act 2016 are broad enough to encompass such evidence, but the Act does not establish admissibility standards. The National Guidelines on AI in Judicial Institutions 2026 articulate important principles of human oversight and transparency but are directed at the judiciary's internal use of AI rather than at the evidentiary status of AI outputs in criminal proceedings. The result is a significant gap: courts confronting algorithmic evidence must rely on a discretionary provision designed for a different technological era, without legislative guidance on disclosure, reliability assessment, or the conditions under which such evidence should be excluded.

5.2 Achievement of Research Objectives

The first objective to critically examine existing legislative provisions has been achieved through detailed analysis of the Electronic Transactions Ordinance, the Qanun-e-Shahadat

Order, and the Prevention of Electronic Crimes Act, identifying both their achievements and their limitations. The second objective to identify the extent to which the framework addresses AI challenges has been achieved through the finding that it does so only indirectly and inadequately, through general provisions that lack the specificity required for algorithmic evidence. The third objective to analyze judicial interpretation has been achieved through examination of case law on video and digital evidence, revealing an authentication paradigm that presumes verifiable recordings rather than algorithmic conclusions.

The fourth objective to compare with international standards and scholarly perspectives has been achieved through engagement with European and international literature on digital evidence admissibility and algorithmic transparency, which confirms that Pakistan's framework lags behind jurisdictions that have begun to develop specific standards for AI evidence. The fifth objective to propose reforms is addressed in the following section, drawing upon the findings of the preceding analysis.

5.3 Limitations of the Study

The study's exclusive reliance on secondary legal materials, while methodologically appropriate for its doctrinal research questions, means that its conclusions about judicial practice rest upon reported decisions. Unreported cases and the routine handling of digital evidence in trial courts may present a different picture. The study's focus on admissibility rather than weight means that the question of how courts should evaluate the probative value of AI evidence, once admitted, receives less attention than the threshold question of admission. The rapidly evolving technological and regulatory landscape means that the analysis reflects the position at the time of writing, and new legislative or judicial developments may require its revision. Finally, the study does not address the operational deployment of specific AI systems by Pakistani law enforcement agencies in detail, except insofar as such deployment bears upon the evidentiary questions that are its central concern.

5.4 Concluding Remarks

Pakistan's legislative framework for digital evidence represents a significant achievement of legal adaptation to the information age, but it has not kept pace with the subsequent transformation wrought by artificial intelligence. The framework's foundational provisions Article 164's discretionary gateway and the authentication requirements developed in case law were designed for evidence that can be verified against an external reality and challenged through cross-examination of a person who can explain its origins. AI-generated evidence challenges both assumptions. Its origins lie in algorithmic processes that may be opaque even to their operators, and there may be no person capable of explaining the basis for a particular output in terms that permit meaningful cross-examination.

The constitutional guarantee of a fair trial under Article 10-A demands that this gap be addressed. The National Guidelines on AI in Judicial Institutions provide a policy foundation, but they must be translated into binding evidentiary rules that specify the conditions under which algorithmic evidence may be admitted, the disclosures that must accompany it, and the consequences of non-disclosure. Until such rules are enacted, courts will continue to exercise discretion without legislative guidance, and the fairness of proceedings involving AI evidence

will depend upon factors that the legal framework does not control. The reform agenda is therefore not merely a matter of technical legal improvement but of constitutional obligation.

6. Recommendations

6.1 Legal and Policy Recommendations

The most urgent reform is the insertion of a new provision in the Qanun-e-Shahadat Order 1984 establishing an Algorithmic Evidence Disclosure Standard as a condition of admissibility for AI-generated identification or classification evidence. Such a provision should require, as pre-conditions for admission, disclosure of the algorithm's role in the investigative or prosecutorial process, the basis and confidence level of any identification or classification, and the system's known error rates, including demographic error rates where applicable. Evidence that fails to satisfy these conditions should be excluded.

Complementing this admissibility standard, a statutory Right to Explanation should be enacted as a legislative implementation of Article 10-A in algorithmic contexts. Any person subject to arrest, charge, or conviction in which algorithmic evidence played a material role should have a right to receive, within a specified period of written request, a plain-language explanation of the algorithm's role in the decision, the basis and confidence level of any identification, and the system's known error rates. Trade secret protection should not be available to deny this right in criminal proceedings. Where a compliant explanation cannot be produced, the algorithmic evidence should be excluded.

A further legislative measure should establish a classification system for AI systems used in criminal justice, distinguishing between low-risk applications that may be deployed without specific authorization, moderate-risk applications requiring registration and periodic accuracy audits, and high-risk applications such as facial recognition for population scanning or predictive policing requiring prior judicial authorization before deployment. The classification system should be accompanied by mandatory Algorithmic Impact Assessments before any high-risk system is deployed or upgraded, documenting accuracy on Pakistan-specific demographic validation data, false positive and negative rates disaggregated by relevant characteristics, and human review requirements.

6.2 Institutional Reforms

Legislative reform must be accompanied by institutional capacity-building within the judiciary and investigative agencies. A dedicated forensic unit or centre of expertise on algorithmic evidence should be established, capable of providing courts with independent assessments of the reliability of AI systems and the validity of their outputs. This unit should be resourced to conduct or commission technical evaluations and to produce reports accessible to judges without specialized technical training. The unit's independence from law enforcement agencies is essential to its credibility.

Judicial training on digital and algorithmic evidence should be expanded and systematized. The National Judicial Automation Committee, which developed the AI Guidelines, is appropriately positioned to oversee the development of training curricula addressing the evidentiary implications of AI, including the limitations of algorithmic outputs, the

significance of error rates, and the questions that judges should ask when confronted with AI-generated evidence. Training should extend to prosecutors and defence counsel, whose capacity to engage with algorithmic evidence is essential to the adversarial process.

The investigative agencies deploying AI systems should be required to maintain comprehensive documentation of their systems' validation, operation, and outputs, and to make such documentation available to courts and to accused persons upon request, subject to appropriate protections for genuinely sensitive information that do not extend to the evidentiary basis of conclusions used in criminal proceedings.

6.3 Recommendations for Future Doctrinal Research

Future research should examine the application of the proposed reforms in specific evidentiary contexts, including facial recognition evidence, automated number plate recognition outputs, and predictive policing analytics, to assess whether the general standards proposed here require contextual refinement. Doctrinal analysis of how courts in comparable jurisdictions have handled motions to exclude algorithmic evidence would provide valuable comparative insight. Research on the intersection between algorithmic evidence and the confessional and identification evidence rules of the Qanun-e-Shahadat Order would illuminate additional areas requiring reform. Empirical research, beyond the scope of the present study, on the actual deployment of AI systems by Pakistani law enforcement agencies and on judicial experiences with digital evidence would provide an evidentiary basis for refining the reform agenda.

6.4 Way Forward

The path forward requires recognition that the evidentiary challenges posed by AI are not speculative or distant but present and growing. Safe City projects are operational, facial recognition systems are deployed, and AI-assisted legal research tools are in use within judicial institutions. The question is not whether Pakistan's criminal justice system will confront algorithmic evidence, but whether it will do so with a legal framework adequate to the task of ensuring reliability and fairness.

The reforms proposed here an Algorithmic Evidence Disclosure Standard, a Right to Explanation, a risk-based classification system, institutional capacity-building, and expanded training are interconnected components of a coherent response. None alone is sufficient; together they provide a framework within which courts can meaningfully assess algorithmic evidence, accused persons can exercise their fair trial rights, and the integrity of criminal proceedings can be maintained in the face of technological change. The National Guidelines on AI in Judicial Institutions provide a foundation of principle. What is now required is the translation of principle into binding evidentiary doctrine, and the institutional investment necessary to make that doctrine effective in practice. The constitutional guarantee of a fair trial demand no less.

References

Abdullah, H. O., Darwaish, M. I., Chaudhry, M. J., & Ehsan, M. (2026). AI Generated Evidence in the Courtroom: Deepfakes, Evidentiary Authenticity, and the Threat to Fair Trial Rights in Pakistan. *Journal of Global Social Transformation*, *2*(5), 224–242.

Adil, K. (2024). Digital forensics and criminal investigations in Pakistan. *Pakistan Journal of Criminology*, *16*(01).

Afzal, J. (2025). Comparative review on acceptance of digital evidence within the legal frameworks of Pakistan and China. *International Journal of Law and Legal Advancement*, *1*(1).

Akbar, S. A., Mehdi, T., & Azam, S. (2025). The Scope of Artificial Intelligence in Evidence Evaluation in Judicial Proceeding. *ASSAJ*, *4*(01), 3628–3641.

Ali, A., Bilal, M., & Malik, S. (2026). Legal Challenges of Digital Evidence in Criminal Proceedings: Comparative Perspectives from Pakistan, Indonesia, and Malaysia. *International Journal of Law and Social Science (IJLSS)*, *2*(2), 69–102.

Iqbal, S., Rauf, S., & Sifarish, S. (2025). *Utilizing New Technologies to Solve Problems of Evidence: The Case of Pakistan and India Legal Systems' Integration into a Digital World*.

Javaid, B., & Saleem, S. (2025). Admissibility of Artificial Intelligence-Based Evidence in Pakistan: Legal Standards and Judicial Responses. *UCP Journal of Law & Legal Education*, *3*(3), 59–86.

Javed, K., Khan, A. S. Y., & Ahmad, I. (2026). Artificial Intelligence and the Integrity of Criminal Evidence: Authentication, Admissibility, and Fair Trial Rights. *ASSAJ*, *5*(01), 7706–7717.

Muhammad, O. (2026). Criminal Liability for Autonomous AI-Generated Crimes: Accountability Challenges in Pakistan's Criminal Justice Syste. *Review of Crime, Peace and Society*, *3*(3), 101–109.

Nazir, S., Asif, M., & Khan, A. U. A. (2025). Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal Trials: https://doi. org/10.55966/assaj. 2025.4. 1.0107. *ASSAJ*, *4*(01), 1941–1951.

Rafique, M. Z., Aleem, Y., Umar, M., & Fatima, M. (2026). The Digital Age of Justice: Technology, Fair Trial, and Article 10-A of the Constitution of Pakistan. *ASSAJ*, *5*(01), 5581–5595.

Shah, S. M. N. A., & Ahmed, M. I. (2026). Artificial Intelligence and Criminal Justice Efficiency in Pakistan: A Critical Analysis of Machine Learning Applications for Case Backlog Reduction, Investigative Enhancement, and Fair Trial Safeguards. *Social Science Review Archives*, *4*(2), 900–918.

Tahir, M. I., Saeed, A., Murtaza, M., & Abdullah, H. O. (2025). The Impact of Artificial Intelligence on Evidence in Criminal Trials. *Social Science Review Archives*, *3*(3), 1882–1894.