ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 04 No. 02. Oct-Dec 2025.Page#.914-920
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems
https://doi.org/10.5281/zenodo.17440993

Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal Trials

Arshid Jan
Senior Rule of Law, Justice and Security Sector Adviser with the United Nations System and PhD Scholar
arshidjan.gvca@gmail.com

ABSTRACT
The escalating digitalization of society has in-fact rendered digital evidence an essential element in contemporary criminal trials. However, in Pakistan, the implementation and appreciation of such evidence remain fraught with legal uncertainty, procedural flaws, and institutional inadequacy. This paper undertakes a doctrinal assessment of digital evidence within the Pakistani criminal justice system, analyzing the interplay between the antiquated legal framework and modern technical realities. The current evidentiary regime is primarily governed by the Qanun-e-Shahadat Order (QSO) 1984, the Electronic Transaction Ordinance (ETO) 2002, and the Prevention of Electronic Crimes Act (PECA) 2016. While these legislations render digital evidence generally admissible under provisions like Article 164 QSO and ETO 2002, judicial interpretation often treats it as secondary or corroboratory evidence, demanding confirmation by ocular or physical proof before assigning significant probative weight. However, key legislative gaps persist. The gaps notably concerning ambiguous authentication requirements such as defining "working order" and ensuring "reliable assurance of integrity" and the lack of stipulated technical procedures like the use of hash values and metadata verification. This situation is further compounded by pervasive issues in maintaining the chain of custody and critical deficiencies in forensic infrastructure. This is where few law enforcement agencies possess certified digital forensic tools or internationally trained experts. Consequently, the Pakistani judiciary exhibits significant inconsistency and arbitrariness in evaluating digital evidence, jeopardizing the constitutional right to a fair trial (Article 10A) for defendants, particularly those unable to contest complex technical claims. The study concludes that legislative clarity, mandated judicial training, and substantial investment in forensic capacity are imperative steps to bridge the widening chasm between the law and technology, thereby ensuring digital evidence serves as a reliable instrument of justice in Pakistan.

Keywords: *Digital Evidence, Admissibility, Reliability, Digital Forensics, Fair Trial Rights.*

Introduction

The swift and pervasive encroachment of information and communication technologies (ICT) into all facets of human activity has irrevocably transformed the landscape of modern criminality. The offences have become increasingly borderless and sophisticated. They range from financial fraud and cybercrime to terrorism. This resulting digital footprint has emerged as a crucial and often the only means of proof. Consequently, the administration of criminal justice systems globally, including Pakistan, has been compelled to grapple with the complexities of collecting, preserving, and assessing digital evidence.

In Pakistan, the formal recognition of digital evidence is relatively recent, largely covered by three principal legislative instruments. These instruments include: the Qanun-e-Shahadat Order (QSO)

1984, the Electronic Transaction Ordinance (ETO) 2002, and the Prevention of Electronic Crimes Act (PECA) 2016. The QSO 1984, which forms the basis of evidence law, is primarily derived from the British Empire's Evidence Act 1872. The passage of ETO 2002 was a critical development, aiming to confer validity and enforceability upon electronic documents and transactions and dispelling the perception that digital information is merely hearsay. The law explicitly addresses the admissibility of digital evidence, notably through the discretionary power vested in the court via Article 164 of the QSO 1984.

However, the issue of reliability and probative weight remains largely unsettled, frequently relegated to judicial discretion or secondary status, demanding corroboration from traditional forms of evidence. This systemic weakness stems from a conflict between traditional common law evidentiary principles and the technical volatility intrinsic to digital data. Digital evidence, unlike physical evidence, is inherently abstract, easily alterable, and susceptible to falsification or modification without leaving a tangible trace. Courts, therefore, approach the validity of electronic evidence with great caution due to the digital environment's characteristics, such as the ease of manipulation and alteration. Therefore, the central inquiry shifts from merely asking whether digital evidence can be admitted, to assessing the technical and legal protocols required to guarantee its authenticity, integrity, and non-repudiation.

This doctrinal assessment aims to critically evaluate the current legal and judicial posture concerning digital evidence in Pakistan. It seeks to identify the specific legislative lacunas, analyze the resultant inconsistencies in judicial interpretation. It pinpoints the operational deficits, particularly in digital forensics and chain of custody that undermine the reliability of evidence in criminal trials. By benchmarking the Pakistani framework against international best practices, this study will propose necessary reforms to strengthen the evidentiary standards, thereby ensuring the criminal justice system is adequately equipped to handle the demands of the digital era and uphold the principles of fair trial enshrined in Article 10A of the Constitution.

Theoretical Framework

The doctrinal assessment of digital evidence in Pakistan is anchored in foundational legal theories of evidence, augmented by the principles of digital forensics and comparative jurisprudence.

1. Relevancy and Authenticity: Under the QSO 1984, evidence must be relevant to the facts in issue. For digital evidence, relevancy is intrinsically tied to authenticity, that is, whether the evidence is truly what it purports to be. The ETO 2002 attempts to satisfy this requirement by stipulating the need for a "reliable assurance as to the integrity" of the electronic document, ensuring it has remained "complete and unaltered". This assurance should, theoretically, be achieved via forensic methods like cryptographic hashing. However, the law's failure to define clear methods, the standard for reliability, or what constitutes "unaltered", leaves this principle ambiguous. The law is silent on technical standards like using hash values to verify data integrity.

2. The Best Evidence Rule and Primary Status: The Best Evidence Rule traditionally required the original evidence. The ETO 2002 sought to elevate electronic documents to primary status. A distinction exists between computer-generated evidence (e.g., transaction receipts, logs) and computer-stored evidence (e.g., emails). Computer-generated evidence generally fulfills the originality criteria, especially under Explanation 3 of Article 73 QSO, as documents produced by one uniform process are primary evidence of the rest. However, computer-stored evidence is manually entered and easily alterable, requiring higher corroboration.

3. Hearsay and Circumstantial Evidence: The QSO 1984 generally prohibits hearsay evidence. Electronic communications, particularly computer-stored evidence and social media conversations, frequently raise hearsay issues if not authenticated by the maker. Pakistani law does not explicitly discuss hearsay rules for electronic evidence. Furthermore, digital artifacts

(like time-and-date stamps) are frequently treated as circumstantial evidence. While the status of circumstantial evidence (Qarīna) is evident in Islamic tradition, Pakistani law does not explicitly define the admissibility or criteria for the selection of digital circumstantial evidence.

4. Digital Forensics and Reliability Paradigm: The framework incorporates the normative principles of digital forensics to assess reliability, acknowledging that digital evidence is only valuable if its integrity can be guaranteed post-collection. The key challenge is adherence to the chain of custody, ensuring that actions taken during seizure, storage, and transfer are fully documented and preserved. The frequent violation of chain of custody in Pakistan, often due to insufficient documentation by first responders, directly compromises the reliability of the evidence. This illustrates the need for Pakistan to adopt a reliability-centered approach with clear technical benchmarks for validation.

Methodology

This research employs a rigorous doctrinal research methodology to examine the legal status, challenges, and requirements concerning digital evidence in Pakistan's criminal trials. The doctrinal approach is necessary for analyzing written law and identifying discrepancies between legislative intent and judicial application.

The methodology encompasses the following stages:

1. Statutory and Legislative Analysis: A detailed textual analysis was conducted on the core legal instruments defining electronic evidence: the Qanun-e-Shahadat Order (QSO) 1984, the Electronic Transaction Ordinance (ETO) 2002, and the Prevention of Electronic Crimes Act (PECA) 2016. The analysis focused on key articles: QSO Articles 59 (expert opinion), 73 (primary evidence), and 164 (modern devices); ETO 2002 Section 5 (integrity requirement); and PECA 2016 procedural implications. This identified ambiguities in terminology (e.g., "working order") and procedural omissions regarding authentication methods.

2. Case Law Review (Judicial Trends): A critical review of landmark judgments from Pakistan’s superior courts was undertaken, focusing on cases addressing the admissibility and weight of specific digital evidence types (e.g., CCTV footage, audio/video recordings). The purpose was to identify recurring patterns of judicial reasoning, the degree of judicial inconsistency, and the conditions courts impose for accepting digital evidence.

3. Comparative Legal Analysis: The Pakistani framework was compared against established evidentiary regimes in other jurisdictions, particularly focusing on:

- The use of technological standards (e.g., hash values) in US law.
- Procedural requirements for evidence handling (e.g., chain of custody principles).
- The general approach of treating electronic evidence under rules for physical evidence, while updating necessary amendments, as seen in countries like Canada, Australia, India, and the USA. This comparison served to highlight the procedural and technical gaps in Pakistan and to formulate reforms based on international best practices.

4. Review of Secondary Sources: Academic literature and reports were reviewed to contextualize infrastructural deficits, training needs, and operational difficulties faced by law enforcement agencies.

Findings

The doctrinal assessment reveals that Pakistan’s legal framework and judicial practice suffer from a profound gap between legislative intent and technological reality, leading to systemic unreliability in evidence handling.

1. Judicial Inconsistency and Arbitrariness

Despite ETO 2002 declaring digital evidence primary, courts often categorize it as corroboratory or circumstantial, requiring verification by physical evidence. This caution is partially due to the ease with which digital evidence can be modified.

- Varying Standards of Weight: The superior courts exhibit significant judicial inconsistency in treating similar digital artifacts, such as call data records (CDRs) or social media posts. For example, the Lahore High Court held that SMS records could be deemed strong primary evidence, yet the Supreme Court imposed strict conditions for admitting video evidence. This inconsistency is starkly illustrated in the treatment of call data records (CDRs). In the case of Muhammad Akram v. The State (2020 SCMR), the Supreme Court of Pakistan expressed caution, treating CDRs as corroborative evidence that required support from other evidence to establish guilt. Conversely, the Lahore High Court in Ali Raza v. The State (2021 PCrLJ 1314) placed significant reliance on CDRs as primary evidence to convict the accused, highlighting a clear divergence in the application of probative value to the same type of digital evidence. A similar conflict is seen regarding video evidence, where the Peshawar High Court in Muhammad Irshad v. The State (2019 YLR 2601) admitted a video recording despite minor gaps in the chain of custody, while other benches have rejected evidence for similar procedural lapses.
- Mandate for Forensic Verification: Key judicial precedents require strict technical conditions for admissibility. Video evidence, for instance, must be accompanied by a forensic report certifying its origin and proving that it has not been edited or tampered with. This requirement often strains the limits of forensic capacity.

2. Legislative and Procedural Ambiguity

The legal instruments contain critical lacunas concerning technical authentication and procedural integrity:

- Vague Authentication Criteria: The ETO 2002 demands a “reliable assurance as to the integrity” and that the system be in “working order”. However, the Ordinance fails to define the technical method for proving integrity or the meaning of "working order," leaving these terms ambiguous.
- Absence of Technical Standards: Unlike US law, which explicitly recognizes the use of hash values (cryptographic checks) for ensuring data integrity, Pakistani law does not incorporate such technical standards, making it difficult to prove that data remains "unaltered and complete".
- Lack of Chain of Custody Protocol: The legal framework lacks explicit procedural guidelines for managing the chain of custody during the seizure, preservation, and transfer of digital evidence. This procedural weakness is frequently cited as the reason for evidence rejection, compromising its legal acceptance.

3. Deficiencies in Digital Forensics and Expert Testimony

The effective utilization of digital evidence is critically undermined by institutional deficits:

- Inadequate Forensic Capacity: Forensic facilities across Pakistan suffer from severe resource shortages. Few law enforcement agencies possess certified digital forensic tools. The centralized National Response Center for Cyber Crime (NR3C) under the Federal Investigation Agency (FIA) aims to combat these issues, but provincial facilities often lag behind.
- Mishandling and Lack of Training: Investigators often lack the specialized skills required for handling digital evidence. The job of a forensic expert requires considerable effort to identify modification and maintain integrity. The selection criteria for a forensic expert

under the QSO 1984 (Articles 59 and 60) rely generally on being a "master in the relevant field", lacking the necessary specificity regarding technical training and experience.

- Circumstantial Nature: Digital evidence is inherently circumstantial, making it difficult to attribute activity solely to an individual. This difficulty necessitates collaboration with additional, corroborated evidence, strengthening the judicial inclination to treat it as secondary.

Discussion

The judicial posture in Pakistan regarding digital evidence is defined by a deep-seated tension. It is a legislative move toward recognizing technology (ETO 2002) pitted against judicial traditionalism and lack of technical certainty. This results in the reliability paradox, where courts demand extremely high, often technically infeasible, standards of verification while simultaneously being ill-equipped to scrutinize technically flawed evidence.

The Reliability Paradox and Judicial Schizophrenia

Judges often exhibit judicial schizophrenia by prioritizing physical or ocular corroboration, thereby keeping digital evidence in a secondary, corroboratory role, contradicting the primary status afforded by the ETO 2002. This skepticism is justified partly by the ease of altering electronic data and the threat posed by sophisticated manipulations like deepfakes. However, this stance ignores that computer-generated evidence (like system logs) is inherently reliable if the system integrity is proven. The lack of a defined technical benchmark, such as a reliability-centered framework (like the Daubert standard), means that the weight given to digital evidence remains subject to the subjective discretion of the presiding judge.

Impact on Fair Trial Rights

The deficiencies in processing and assessing digital evidence directly undermine the right to a fair trial (Article 10A). The state's capacity to collect and present technical evidence is often superior, creating an unequal battlefield for the accused. This disparity is particularly harsh for indigent defendants, who struggle to fund counter-experts necessary to challenge complex data claims, such as contested metadata or chain of custody breaches. Furthermore, the lack of rigorous pre-trial scrutiny risks the admission of evidence potentially obtained through unlawful surveillance methods, infringing on privacy rights. Judges are sometimes compelled to accept evidence from judicial officers and forensic experts simply because they lack the necessary technical knowledge to verify the authenticity and validity themselves.

A Comparative Common Law Perspective

A comparative look at India, a common law jurisdiction with a similar evidentiary heritage, reveals a more structured approach. India's Section 65B of the Indian Evidence Act, 1872 provides a specific procedural code for the admissibility of electronic evidence. It mandates a mandatory "Section 65B Certificate" of authenticity, issued by a responsible person, which affirms the computer's normal operation and the integrity of the electronic record. This statutory requirement, as emphasized by the Indian Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), creates a clear, albeit strict, gateway for admissibility. While the Indian model has its own challenges, it demonstrates a legislative effort to provide the clarity that the Pakistani ETO 2002 lacks, by explicitly outlining the technical and procedural conditions for proving integrity.

Recommendations for Systemic Reform

To instill true confidence and consistency in the use of digital evidence, Pakistan needs comprehensive reforms:

1. Legislative Clarity and Technical Standards: Amend the QSO and PECA to explicitly incorporate technical authentication standards, such as the mandatory use of hash values

for ensuring data integrity. The scope of ETO 2002 amendments should be extended to apply to all judicial proceedings, rectifying the limitation noted in Section 29.

2. Forensic and Investigative Capacity Building: Significant investment is required in establishing accredited digital forensic laboratories. Mandatory, specialized training must be provided for first responders and investigators, including protocols for evidence collection and chain of custody documentation, adhering to established international guidelines.
3. Judicial Specialization and Training: Specialized training programs for judges are crucial, moving beyond basic computer literacy to cover technical concepts like encryption, metadata, and cloud computing. Specialized cybercrime courts could help ensure consistency in evidentiary rulings.
4. Reliability Testing and Expert Criteria: Implement rigorous criteria for the qualification of digital forensic experts, moving beyond general experience to defined technical training. Consider a mechanism similar to the Daubert standard to assess the scientific validity of expert testimony.
5. Safeguards for the Accused: Strengthen legal aid mechanisms to provide indigent defendants with access to counter-expertise, thereby upholding the balance required by Article 10A. Introduce pre-trial scrutiny requirements for digital evidence collection to prevent unlawful surveillance.

Conclusion

The use of digital evidence in Pakistan's criminal trials represents a necessary but currently inadequate response to the challenges of modern crime. While legislative efforts, notably the ETO 2002 and QSO amendments, have generally secured the admissibility of electronic documents, the systemic failure to establish and enforce rigorous standards for reliability and authentication compromises the integrity of the judicial process. The lack of explicit technical protocols, deficiencies in forensic infrastructure, and resulting judicial inconsistency create an environment where the probative value of digital evidence is frequently uncertain.

This environment not only hinders effective justice but also poses a severe threat to the constitutional rights of the accused by limiting their capacity to contest technically complex state evidence. To ensure that digital evidence serves as a reliable instrument of truth and justice, Pakistan must move beyond symbolic gestures. The urgent need is for a comprehensive overhaul that mandates standardized forensic procedures, fosters judicial technical expertise, and aligns the legal framework with globally recognized reliability principles. By addressing these systemic deficiencies, Pakistan can bridge the gap between its traditional legal doctrine and the inescapable realities of the digital age, thereby upholding the fundamental promise of a fair and equitable criminal justice system.

References

Abbasi, H., & Iqbal, M. A. (2020). Authentication of Electronic Evidence; A Journey from Electronic Discovery to Digital Forensic Experts in Western Law-Recommendations for Pakistan. Journal of Social Sciences & Humanities (1994-7046), 28(1).

Abbasi, H., Rafique, S., & Badshah, S. N. (2021). Critical Analysis of Pakistani law of Electronic Evidence from the Perspective of Sharīʿah and English Law-Recommendations for Pakistan. Tahdhib-al-Afkar.

Abdollahi, M. (2012). Electronic Evidence in the Evidence System. Khorsandi Publications.

Adil, K. (2024). Digital Forensics and Criminal Investigations in Pakistan. Pakistan Journal of Criminology, 16(01), 711–714.

Al-Billeh, T., Alkhseilat, A., & AL-Khalaileh, L. (2023). Scope of Penalties of Offences in Jordanian Public Office. Pakistan Journal of Criminology, 15(2), 341-356.
Ali Raza v. The State & Muhammad Irshad v. The State
Al-Thunaibat, G. (2003). The role of technical expertise in proving forgery in written documents in Jordanian law, comparative study, PhD Thesis. Amman Arab University.
Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) (AIR 2020 SC 4908)
Chaudhry, M., Ali, K., & Khan, R. (2024). Procedural flaws in digital evidence: A case study of Pakistani courts. Pakistan Journal of Criminology, 16(2), 78–95.
Dawas, R. A., Jafarzadeh, S., & Saranghi, R. N. (2024). The Status of Electronic Evidence and Its Role in Proving Criminal Cases. Pakistan Journal of Life and Social Sciences.
Ghani, U., & Iqbal, Z. (2024). Judicial inconsistency in digital evidence rulings: A Pakistani perspective. South Asian Legal Review, 10(1), 33–52.
Hameed, U. (2021). Admissibility of Digital Evidence: A perspective of Pakistani Justice System. Pakistan Social Sciences Review, 5(IV), 518–530.
Indian Evidence Act, 1872 - Section 65B
Khan, M. S., & Bhatti, S. H. (2023). Digital Evidence and Pakistani Criminal Justice System: A Review Article. Journal of Social Sciences Review, 3(1), 489–498.
Khan, S. N., Muhammad, A., & Khan, A. U. (2025). Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal Trials. Advance Social Science Archive Journal, 4(1), 1941–1951.
Khashashneh, T., Al-Billeh, T., Al-Hammouri, A., & Belghit, R. (2023). The Importance of Digital Technology in Extracting Electronic Evidence: How Can Digital Technology be used at Crime Scenes? Pakistan Journal of Criminology, 15(04), 69–85.
Muhammad Akram v. The State
Mushtaque, K., Umer, A., Ahsan, K., & Mahmood, N. (2014). Digital Forensic Models: A Comparative Study based in large enterprises of Pakistan. Research Journal of Recent Sciences, 3(8), 103–110.
Rana, A. A., Naul, A. H. K., Gujjar, U. A., & Ahmad, F. Z. (2022). Admissibility and Evidentiary Value of Electronic Evidence in Criminal Cases: A Case Study of Pakistan. Journal of Law and Social Policy, 4(1).
Saeed, M. A., & Gillani, A. H. (2021). Evidential representation of using the modern devices and decision-making feasibility in Pakistan. Journal of Law & Social Studies, 3(2), 79–86.
Salam, M. H. u., Khan, S. M. A. W., & Rathore, S. A. (2022). Recording Evidence through Information Technology and its Implications in Pakistan: An Assessment. Journal of Development and Social Sciences, 3(3), 538–544.
Usman, M. (2022). DIGITAL EVIDENCE: TESTIMONY OF EXPERT WITNESS IN PAKISTANI LAW. Majallah-yi Talim o Tahqiq, 4(1), 170–183.