Sociology & Cultural Research Review (SCRR)
Available Online: https://scrrjournal.com
Print ISSN: 3007-3103 Online ISSN: 3007-3111
Platform & Workflow by: Open Journal Systems

Utilizing New Technologies to Solve Problems of Evidence: The Case of Pakistan and India Legal Systems' Integration into a Digital World

Sheza Iqbal
Legal Associate at Axis Law Chambers, Lahore, Pakistan
shezaiqbal1632k@gmail.com
Sundus Rauf (Corresponding Author)
HOD/Associate Professor, M A Raoof College of Law, The University of Lahore
sundas.rauf@law.uol.edu.pk
Sobia Sifarish
Assistant Professor, M A Raoof College of Law, The University of Lahore
sobia.sifarish@law.uol.edu.pk

ABSTRACT
The rapid transformation of legal frameworks has reshaped the process of collection, presentation and preservation of evidence in legal forums across the world. In Pakistan in India, the notion of blending new technologies onto the evidentiary mechanism provides for opportunities and risks. This paper attempts to examine how blockchain authentication, digital forensics as well as artificial intelligence are revamping the evidentiary principles in these countries, with specific reliance on admissibility, relevance, reliability and integrity of such electronic evidence. It discovers the legislative instruments such as the Qanun-e-Shahadat Order as well as the India's Evidence Act, and determine their competency in addressing the technicalities of cyber evidence, cross-border data transfers and digital chain of custody. The paper identifies major gaps in the judicial system such as the lack of proper standards, technological and infrastructural defects which hinder ideal application. Through analyzing comparative reforms and judicial decisions, the paper suggests ways for harmonizing evidentiary framework with the international standards, while striking a balance between due process and innovation. Lastly, the paper argues that Pakistan and India needs to meet the requirements of a rapidly advancing legal environment through incorporating secure and efficient digital tools in their legal systems.

Keywords: *Digital Evidence, Electronic Records, Blockchain, Artificial Intelligence, Comparative Legal System.*

1. INTRODUCTION

The development of new technologies has fundamentally changed the processes involved in the creation, storage, transmission, and analysis of legal evidence within a legal system. As example, block-chain technology, AI, and digital forensics significantly enhance capability to resolve problems pertaining to the admissibility, trustworthiness, and preservation of evidence. As societies evolve and adapt to modern means of interaction, trade, and governance, courts are routinely presented with evidence generated through emails, mobile applications (apps), sophisticated surveillance equipment, metadata, and advanced digital ledgers. Many traditional evidentiary rules, most of which stem from physical documents and witness accounts, often fall short of addressing such materials. This gap between rapid technological advancements and legal principles that are still rooted in antiquated practices

necessitates an overhaul of evidentiary systems of countries like Pakistan and India where the use of digital evidence is on the rise in legal proceedings (Taylor et al., 2010).

It is telling that both the Indian Evidence Act 1872 and Pakistan's Qanun-e-Shahadat Order 1984 stem from a bygone era devoid of technology, suggesting a disparity between their approach to evidence and contemporary technological advancements. These legislations seem to determine the value of statements and evidence on the basis of direct human observation and narration—an idea described by doctrines such as Res Gestae which hinge on spontaneity and direct causation. Nonetheless, the creation of digital evidence often occurs without human engagement, created automatically and stored in ways vulnerable to edits and erasure, which straddle traditional thresholds of admissibility and reliability (Coffey, 2022).

This legal modification goes beyond simple changes to legislation; it requires the creation of comprehensive models which apply technological functionalities to the procedural and evidentiary frameworks. An example would be blockchain technology which digitally stores records in a way that prevents tampering and is thus useful in aiding the verification of the chain of custody, strengthening the trustworthiness of digital evidence. AI technology is also capable of assisting forensic analysts in detecting fraud, performing large-scale data analyses, and issuing real-time notifications. This helps in both criminal and civil disputes (Tian et al., 2019).

Digital technologies are becoming foundational in the context of legal proceedings, making integration reforms essential rather than optional. Should the discrepancy between law and technology go unattended, it might result in legal and social inefficiencies, injustices and the erosion of public trust in legal institutions. Therefore, this paper defends the idea that both Pakistan and India need to practice anticipatory legal adaptation through reforms in legislation, procedures, and public institutions to take advantage of new technologies, in order to ensure justice in a swiftly digitalizing world (Mayernik, 2019).

2. EVIDENTIARY CHALLENGES IN THE DIGITAL ERA

The digital evolution of today's communication and record-keeping technologies has added new layers of evidential complexity, especially in relation to authenticity, integrity, and admissibility. Evidence law was traditionally rooted in a context where documents and testimonies were physical in nature. Such a system granted the benefit of a simple assumption in relation to material presented in court: it had provenance and physical continuity. Unlike physical pieces of evidence, digital evidence is extremely easy to alter, delete, replicate, or fabricate. So, concerns regarding authenticity and chain of custody are difficult to address (Casey, 2011).

Section 65B of the Indian Evidence Act, 1872, tries to capture that technical reality by demanding a formal certificate whenever an electronic record is introduced, thereby placing the burden squarely on the party offering the proof. The Supreme Court's ruling in *Anvar P.V. v. P.K. Basheer* turned that statutory formality into an inflexible barrier, declaring that the evidence simply will not come in unless the prescribed document is present. Legal commentators applauded the clarity but soon noticed that such rigid enforcement could, ironically, deny parties the very justice the rules were intended to protect.

In recent years India has expanded its forensic capability in cyberspace more decisively than many expected. The Central Forensic Science Laboratory and several state laboratories now maintain dedicated cybercrime units that specialize in encrypted files, network traces, and electronic surveillance logs. Even so, the units are sometimes overwhelmed; case backlogs

build up, regional funding varies sharply, and strict procedural protocol is not always observed, which dulls the overall impact of the investment (Underwood, 2019).

Perhaps the most challenging evidentiary doctrine in the face of modern digital realities is Res Gestae. This doctrine allows for the admissibility of spontaneous utterances or acts that are so closely tied with a central event as an exception to the hearsay rule. Yet, certain forms of digital evidence such as system logs, sensors, and CCTV footage are recorded and created absent intention or thought. This fundamentally challenges the requirement of spontaneity and contemporaneity that Res Gestae relies on. For instance, a WhatsApp message timestamped during the commission of a crime is positively corroborative. However, it does not qualify as a stress-laden utterance as required under Res Gestae (Hameed, 2021).

However, this has also resulted in a hyper formalistic legal framework whereby relevant evidence may be ignored due to failing to follow procedures. Unlike India, Pakistan does not have clear statute-based frameworks or judicial precedents relevant to the issue at hand. Though Article 164 of the Qanun-e-Shahadat Order gives courts the right to accept digital evidence, its application is erratic. There is no counterpart provision to India's Section 65B, which deals with the standardized criteria for the admissibility of evidence. Litigants and the courts consequently find themselves in a jurisdictional limbo that compromises the certainty and justice of trial results. In addition, there are still systematic issues such as lack of forensic laboratories and inadequate systems for digitally archiving relevant case materials, restricted training opportunities for judges and legal practitioners within the country, as well as lacking institutional frameworks. These countries have not only failed to meet the challenges posed by the digital age, but also hinder any kind of comprehensive legal and procedural change aimed at resolving such conflicts (Hameed, 2021).

3. THE IMPORTANCE OF USING BLOCKCHAIN TECHNOLOGY IN VERIFICATION OF EVIDENCE

The block chain industry is the new decentralized geospatial technology with the most potential technological advancement in the area of preserving digital evidence due to its trustless ledgers. Essentially, a block chain functions as a distributed database with append-only transaction records, secured by a chain of cryptographic hashes. Block chain's immutability structure guarantees that data, such as addition of new blocks, becomes impossible to change after being secured to a chain. This form of near impossible alteration ensures a tedious process to alter tokens (Brokowski et al., 2019).

While both India and Pakistan have yet to officially adopt block chain-based evidence management systems, they demonstrate encouraging advances through pilot initiatives and scholarly debates. Telangana, one of the states in India, has implemented block chain technology in public registries, which may facilitate its use in other legal areas later. In Pakistan, there are some private ventures in fin-tech and academic studies looking into block chain applications in legal technology, although broader acceptance in the legal field remains nascent (Ying et al., 2017).

The legal admissibility of blockchain-stored records depends on the recognition by courts of the evidentiary integrity and compliance with the procedures of such technologies. There is no explicit provision addressing blockchain evidence in Pakistan's Qanun-e-Shahadat Order 1984 or India's Evidence Act 1872. However, both systems have some overarching common provisions that allow for the admissibility of electronic evidence (Article 164 in Pakistan and Section 65B in India) which would generously be construed to cover logs and entries of block chains (Ying et al., 2017).

These changes stand to influence legal policy development in Pakistan and India. India's judiciary has demonstrated an acceptance of advanced technology in regard to evidence with the use of CCTV footage and call detail records, albeit under strict adherence to the Evidence Act. This willingness might be useful for implementing block chain records, particularly when they can prove authenticity, integrity, and unbroken custody. Pakistan's judiciary, generally more rigid, may change if defined steps are introduced through statutory changes or judicial frameworks (Salam, 2022).

The use of block chain technology is applicable in many ways within civil and criminal litigation. In criminal matters, a block chain can be utilized to record custody of digital pieces of evidence such as video surveillance, biometrics, and reports from forensic labs. This is critical for cybercrime investigations that rely on digital evidence since such evidence is at risk of being manipulated. With block chain, every action taken in the handling of the evidence is recorded and cannot be altered, limiting the possibility of fraudulent alteration or disputes (Salam, 2022). Block chain technology has the potential to verify commercial transactions, smart contracts, and intellectual property rights in civil litigation. For example, in patent disputes block chain technology can be used to timestamp invention disclosures which then serves as prima facie evidence for ownership claims? In both jurisdictions, the automation of compliance with procedural actions like the issuance of Section 65B certificates and evidence of compliance with Article 164 may increase the reliability of evidence and streamline administrative processes (Tian et al., 2019).

4. INTEGRATING DIGITAL FORENSICS WITH INNOVATIONS IN LAW: A CASE STUDY OF INDIA AND PAKISTAN

The discipline of digital forensics has emerged as a critical component of the modern evidentiary system, particularly with criminal justice systems [sic] straining under the weight of electronic data. Digital forensics encompasses the recovery, preservation, and analysis of data from an ever-growing list of sources spanning computer hard drives and mobile phones to cloud storage and even encrypted cyberspaces. Noteworthy innovations include the analysis of metadata, where attributes—sometimes referred to as timestamps, GPS coordinates, and device logs—are generated and analyzed to corroborate a claimed event and establish a timeline for the series of occurrences.

In relation to the submission of evidence, these methods shift significantly enhance the credibility and preservation of digital materials as they allow investigators to verify that files are indeed authentic and were created in the context alleged (Balhera, 2018). Tools such as hash functions, which create unique digital fingerprints, are now a standard in verifying data integrity to preemptively removing digital evidence. Expert forensic testimony, based on scientifically validated methods, is pivotal in explaining sophisticated digital evidence in simplified terms and articulating convincing legal strategies.

Both countries' legal systems are beginning to change because technological evidence is becoming more important to resolving legal issues, but there is a difference in how fast and deep these changes go. India is in the process of modernizing its laws regarding digital forensics due to its changes in the Information Technology Act 2000, implementing new judicial educational modules tailored to specific cyber issues, and amending cyber laws. Subsequent decisions have built upon these foundational requirements, defining the submission procedure for electronic evidence. Furthermore, the Indian judiciary has shown receptiveness towards these new forensic approaches when adjudicating matters pertaining to cyber fraud, digital impersonation, and crimes involving crypto-currencies (Bebortta et al., 2020).

In Pakistan, Article 164 of the Qanun-e-Shahadat Order 1984 permits the use of modern technological devices for gathering evidence, although adherence to such practices remains uneven. The Lahore High Court in *Zaheeruddin v State* affirmed the use of CCTV and telephone call text records, albeit with stipulations requiring corroborating expert testimony and verification of the data's authenticity. Notwithstanding this, the lack of comprehensive procedural rules, fusion of legal guidelines, and a sovereign statutory structure on digital forensics has constrained the probative value such materials possess in the courts of Pakistan. There is a legislative proposal which as a new country focused on protecting its data requires the consideration of bills like the data protection and policies of regulating digital evidence.

Countries like the United States of America, the United Kingdom, and Singapore, have embraced digital forensics and invested in forensic capacity building through the establishment of comprehensive digital forensics policy frameworks with articulated evidentiary standards. The UK's Digital Evidence Framework directs protocol compliance in the collection, analysis, and presentation of digital exhibits. Such India and Pakistan have much to learn from these jurisdictions in adopting policies for the digital collection of evidence, accreditation of forensic laboratories and experts, and developing a comprehensive hybrid law that systematically integrates forensic science into procedural law. In both countries, partnership of the judiciary, law enforcement, education, and technological specialists is essential to ensure the application of technology turns into evidence that is legally permissible for prosecution without breaching constitutional rights (Kizza & Kizza, 2011).

5. CHANGING THE LEGAL STRUCTURE FOR TECHNOLOGY BASED SYSTEMS

There is an urgent need for statutory reform in both Pakistan and India, as the scope of crime, trade, and communication becomes more digitized. The evidence laws in both jurisdictions, Qanun-e-Shahadat Order 1984 in Pakistan and the Indian Evidence Act 1872, were formulated long before concepts such as digital footprints, cybercrimes, and the internet of things existed. Although both jurisdictions have tried to address this problem through incremental changes, the modifications made do not represent the comprehensive overhaul required to fulfill the evidentiary requirements of today's digital landscape (Ceil, 2015).

Legal academics have suggested that an approach where language meant to define the technology used is broadened could be employed to enable the law to keep pace with advancing digital formats and devices. In addition, as noted in PACE 1984, UK legislation has provided for the establishment of operational leeway concerning reliance on some forms of evidence, suggesting that setting legal presumptions about the reliability of data generated by machines can serve as a practical approach.

Specialized procedures addressing the collection, storage, transfer, and presentation of digital evidence in courts need to be established alongside statutory reforms. The absence of a defined chain-of-custody applicable to digital materials in India and Pakistan undermines the credibility and legal weight of such evidence.

The proposed procedural framework should cover the following aspects:

- Mandatory hash verification at the point of seizure and at the point of presentation.
- Evidence logs and inventory for digital materials are to be maintained in standardized templates.
- Orders for preservation and retention of data during the investigations.
- Procedures for mirror imaging and forensic analysis.
- Preservations for confidentiality and privacy, more so with data stored on the cloud or encrypted (Ceil, 2015).

India's Information Technology (Amendment) Act 2008 along with other rules and regulations crafted under it address some of these issues; however, they are lacking in cohesive application across all regions and comprehensive uniformity. Pakistan PECA 2016 allows the Federal Investigation Agency (FIA) to manage digital evidence, but the absence of robust procedural guidelines has led to evidentiary lapses in numerous prosecutions. The development of judicial bench books and toolkits of digital evidence as UK's Judicial College produced, may enhance uniformity and efficiency greatly. The National Judicial Academy of India, along with state-level judicial academies, has launched training programs on cyber law and digital forensics, although judges still face problems with technical concepts like metadata, encryption, or blockchain. On the lower side of the spectrum, Pakistan's Judicial Academy and FIA Cyber Crime Division have made some strides in that direction. The lack of specialized training for law enforcement and trial court judges creates gaps in the reliable use of digital evidence, leading to a dismissive approach towards its interpretation and invalid acceptance as rejection (Jamshed et al., 2022).

All outlined problems confirm the importance of focus areas for building capacity, which include:

- Interdisciplinary cooperation with IT specialists and forensic scientists
- Creation of designated units for cybercrime within police and prosecution services
- Regular workshops and teaching seminars aimed at judges and prosecutors
- Training programs for digital forensic professionals
- Specialized digital analysis tools for data, secure storage, and certified forensic laboratories (Jamshed et al., 2022).

Moreover, the collaboration with UNODC and SAARC Law can aid the need of South Asian jurisdictions by providing them with funding, model practices, and technical aid. For a more meaningful integration of advanced technologies, comprehensive reform centered on the statutory lies at the core need for procedural, and institutional areas of the evidentiary process.

6. PRIVACY, SURVEILLANCE, AND RIGHTS-CENTRIC ISSUES

The growing reliance on digital evidence and technological advancements within the Pak-India nexus of justice raises some deep ethical and constitutional dilemmas, especially relating to privacy and surveillance. Article 14 of the Constitution of Pakistan and Article 21 of the Constitution of India recognize fundamental human rights and grant protection against arbitrary state action and upholds personal dignity and privacy. The widespread application of surveillance technologies, including but not limited to, CCTV, geo-location tracking, and data interception poses serious risks to these rights of privacy if unchecked (Greenleaf, 2019). Privacy issues are also attached to the unethical practices of data mining and mass surveillance, which are prone to unbalanced or disproportionate targeting. Legal scholars have argued that the systems of justice must balance the scales of individual freedoms with the prevention of crime, and must also ensure that the collection of digital evidence is conducted in a manner compliant with constitutional frameworks and global human rights treaties (Greenleaf, 2019).

7. GUARANTEEING DUE PROCESS IN REMOTE JUSTICE SYSTEMS

Due process remains essential to any sort of fair adjudication. It includes the granting of notice, confrontation, evidence evaluation, as well as the evaluation of the evidence provided dispassionately. The provision of complex digital evidence raises the danger that litigants and courts unfamiliar with technical details will be inundated, which can undermine equity. Courts

must safeguard the right of parties to challenge the authenticity and reliability of digital evidence, and provide expert testimony that is subjected to rigorous cross-examination. Both legal systems face the possibility of technological bias, which occurs when judges give undue reverence to forensic professionals or automated systems and their conclusions without appropriate analysis. This justifies protective measures such as forensic methodology disclosures, scrutiny of software validations, and monopoly claims on third party expert assessments (Baig et al., 2017).

The use of technology within the criminal justice system raises issues of transparency and accountability. In Pakistan and India, there are no overriding regulations that require disclosure of any sources of digital evidence, forensic methods, and chain-of-custody procedures to the defense and the court. Judicial and legislative branches must protect law enforcement, technology, and forensic service companies from operating with no documentation and no outside accountability by mandating oversight. Such transparency could be enforced through audits, compliance instruction-reporting, and monitoring systems for errors in digital evidence within a set period (Underwood, 2019).

8. TOWARDS A FUTURE-READY EVIDENCE SYSTEM: INTEGRATING TECHNOLOGY WITH EVIDENCE LAW

The justice system must be regarded as credible, and thus emerging technologies should be aligned with evidence principles such as Res Gestae. These doctrines advocate for spontaneity, immediacy, and trust, which need to recalibrate to make room for digital evidence. For instance, blockchain can provide immutable time stamping, which compliance with the Res Gestae requirements but needs education to the judiciary and legislation to be fully useful. Obsolescence is a risk with technologies that are governed by rigid rules, as those technologies are outpaced by innovations. In the context of evidential legal standards, both Pakistan and India should adopt principle-based standards based on governance frameworks that focus on core principles business authenticity, document integrity, and content relevance so that courts have the flexibility to evaluate new evidential paradigms free from narrow definitions. Such frameworks promote fairness while allowing adaptability regarding legal perspectives (Baig et al., 2017).

Pakistan has attempted to locate a foothold in cyberspace law through the Prevention of Electronic Crimes Act (PECA) 2016, yet the enterprise feels unfinished. Courts still lean heavily on the Qanun-e-Shahadat Order of 1984, whose dusty rules falter when confronted with cloud storage, end-to-end encryption, and the fast-moving grammar of digital communication. No legal overhaul of this magnitude can thrive in solitary confinement. India and Pakistan must share notebooks if they intend to keep pace with the dataverse, and cross-border cooperation is no longer a policy choice but a regional necessity. A few quick ways to bridge the divide would include:

- Collaborative legal-technical research panels that map the blind spots in both rulebooks and highlight where the PECA meets its limit. Joint workshops for judges, police, and prosecutors so everyone speaks the same dialect of digital evidence-from packet captures to metadata dumps.
- Expert committees that mix coders, legal scholars, and frontline practitioners to hash out thickets such as encryption backdoors, data sovereignty, and the shifting admissibility bar for electronic proof. Acting in concert might deliver South Asia a lexicon of law that feels less like a patch job and more like a coherent system. Shared risk and shared experience could spark ideas neither country would dream up alone.

9. CONCLUSION

This paper has scrutinized how Pakistan and India are trying to fit digital evidence into legal frameworks that were not designed for it. By examining the role of blockchain, artificial intelligence, and cutting-edge forensic gear, the discussion highlights the strain those novelties place on old doctrines-like Res Gestae-that depend on spoken testimony and on-the-spot physical proof. Practitioners in both countries meet the same three headaches: shaky statutes, uneven judicial rulings, and lopsided procedures. The result is two different but equally troubling paths. A legal system that waits for a headline-grabbing trial before lifting its pen is watching the future race by. Proactive lawmaking instead asks: Shared colonial statutes, intertwined histories, and lean-forward tech cultures give India and Pakistan an unusual launching pad for joint digital justice experiments. Neighbors can build courtrooms equipped for side-by-side screens that let jurors watch a block chain ledger while hearing witness testimony. Interdisciplinary think-tanks that update the law every time a new encryption standard goes public. Judges who protect free speech but also know when an AI-generated image crosses a dangerous line. Model legislation emerging from forums such as the SAARC Legal Network could cut the duplication and hand states a draft that already speaks global. If both Pakistan and India embrace a policy of deliberate, broadly participatory modernization, they may simultaneously safeguard the rule of law in a fast-digitizing environment and emerge as benchmark jurisdictions for handling electronic evidence in South Asia.

BIBLIOGRAPHY

Anvar P.V v. P.K. Basheer & Ors (2014 10 SCC 473). Retrieved from https://indiankanoon.org/doc/187283766

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3–13. https://doi.org/10.1016/j.diin.2017.06.015

Balhera, A. (2018). A Study about First Information Report (FIR) and Its Various Aspects under Criminal Law. *International Journal of Research*, *5*(4), 47–55. https://journals.pen2print.org/index.php/ijr/article/download/12030/11328

Bebortta, S., Senapati, D., Rajput, N. K., Singh, A. K., Rathi, V. K., Pandey, H. M., Jaiswal, A. K., Qian, J., & Tiwari, P. (2020). Evidence of power-law behavior in cognitive IoT applications. *Neural Computing and Applications*, *32*(20), 16043–16055. https://doi.org/10.1007/s00521-020-04705-0

Borkowski, M., Sigwart, M., Frauenthaler, P., Hukkinen, T., & Schulte, S. (2019). DEXTT: Deterministic Cross-Blockchain Token Transfers. *IEEE Access*, *7*, 111030–111042. https://doi.org/10.1109/access.2019.2934707

Casey, E. (2011). *Digital Evidence and Computer crime: Forensic science, computers and the internet*. http://ci.nii.ac.jp/ncid/BB06007590

Ceil, C. (2015). Police and Criminal Evidence Act 1984. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2597219

Coffey, R. (2022). Fight, flight, freeze. . .or lie? Rethinking the principles of res gestae evidence in light of its revival. *The International Journal of Evidence & Proof*, *27*(1), 51–82. https://doi.org/10.1177/13657127221139505

Greenleaf, G. (2019). Advances in South Asian data privacy laws: Sri Lanka, Pakistan and Nepal. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3549055

Hameed, U. (2021). Admissibility of Digital Evidence: A perspective of Pakistani Justice System. *Pakistan Social Sciences Review*, *5*(IV), 518–530. https://doi.org/10.35484/pssr.2021(5-iv)40

Indian Evidence Act 1872. Retrieved from https://www.indiacode.nic.in/bitstream/123456789/15351/1/iea_1872.pdf

Jain, P. (2018). Artificial intelligence for sustainable and effective justice delivery in India. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3284903

Jamshed, J., Rafique, W., Baig, K., & Ahmad, W. (2022). Critical analysis of cybercrimes in Pakistan: legislative measures and reforms. *International Journal of Business and Economic Affairs*, *7*(1). https://doi.org/10.24088/ijbea-2022-71002

Kizza, J., & Kizza, F. M. (2011). Digital evidence and computer crime. In *IGI Global eBooks*. https://doi.org/10.4018/9781599043791.ch015

Mayernik, M. S. (2019). Metadata accounts: Achieving data and evidence in scientific research. *Social Studies of Science*, *49*(5), 732–757. https://doi.org/10.1177/0306312719863494

Prevention of Electronic Crimes (Amendment) Act, 2025. Retrieved form https://khalidzafar.com/wp-content/files_mf/1747235902PECAamendment2025.pdf

Prevention of Electronic Crimes Act, 2016. Retrieved from https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj

Qanun-e-Shahadat Order 1984 (Pakistan). Retrieved from https://punjabpolice.gov.pk/system/files/qanun-e-shahadat-order-1984.pdf

Salam, H. (2022). An Appraisal on Digital Forensic and Computer Tools involved in Investigation process: The Case of Pakistan. *Annals of Human and Social Sciences*, *3*(III). https://doi.org/10.35484/ahss.2022(3-iii)21

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Review*, *26*(3), 304–308. https://doi.org/10.1016/j.clsr.2010.03.002

Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences*, *491*, 151–165. https://doi.org/10.1016/j.ins.2019.04.011

Underwood, T. (2019). *Distant Horizons: digital evidence and literary change*. https://experts.illinois.edu/en/publications/distant-horizons-digital-evidence-and-literary-change

Wahyudi, A. V., & Winanti, A. (2025). Evidentiary Strength of Electronic Evidence in Civil Disputes within the Framework of Bayyinah: A Case Study of Decision No. 22/PDT.G/2021/PN DGL. *Diktum Jurnal Syariah Dan Hukum*, *24*(1), 1–13. https://doi.org/10.35905/diktum.v24i1.14748

Ying, W., Jia, S., & Du, W. (2017). Digital enablement of blockchain: Evidence from HNA group. *International Journal of Information Management*, *39*, 1–4. https://doi.org/10.1016/j.ijinfomgt.2017.10.004

Zaheeruddin v. State (1993 SCMR 1628)