Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 4 No. 3 (2026)

A Comparative Study of Admissibility and Authenticity of Electronic Evidence in Context Pakistan and the United Kingdom

[1]Abdul Basit
[2]Ansar Abbas Dharalah
[*3]Zainab Kausar
[4]Akhtar Ali Ansari
[1]Lecturer, Department of Law, University of Southern Punjab Multan, Pakistan
[2]Advocate High Court, Managing Partner, Legal Solutions & Analysis (LSA) Law Firm Multan, Pakistan
[*3]LLM, Gold Medalist Bahauddin Zakariya University, Multan Pakistan, Advocate High Court
[4]LL.M University of Lahore (UOL)
[1]abdulbasit78622@gmail.com, [2] ansarabbasdharalah786@gmail.com,
[*3]zainabkausar55@gmail.com, [4]akhtaraliansariadv@gmail.com

Abstract

Objective/Aim: Electronic evidence has become central to modern criminal and civil litigation worldwide, yet Pakistan's primary evidentiary framework, the Qanun-e-Shahadat Order 1984 (QSO) was enacted in a pre-digital era and contains no dedicated provisions governing the admissibility, authentication, or forensic integrity of electronically stored information (ESI). This research article critically examines the structural deficiencies of the QSO as they relate to electronic evidence, with particular focus on the inadequacy of sections 2, 73, and related provisions when applied to digital data. Material and Methods: Through the analysis of the United Kingdom's Civil Evidence Act 1995, the Police and Criminal Evidence Act 1984 (PACE), the Electronic Communications Act 2000 and the guidelines issued by the Association of Chief Police Officers (ACPO) now the College of Policing this study undertakes a comparative legal analysis to identify reform pathways for Pakistan. Through doctrinal legal research complemented by a policy analysis framework.
Findings and Conclusion: The article further analyses the Electronic Transactions Ordinance 2002 and the Prevention of Electronic Crimes Act 2016 (PECA) as supplementary legal instruments, assessing whether they sufficiently bridge the legislative gap. The article proposes a multi-tiered reform model encompassing statutory amendments to the QSO, the creation of a national digital forensics regulatory authority, and the codification of a chain-of-custody protocol aligned with ISO/IEC 27037:2012 and UK forensic science standards. The findings indicate that Pakistan's legal system urgently requires coherent, technology-neutral legislative reform to ensure that electronic evidence is handled with the same rigour, integrity, and reliability demanded by contemporary legal proceedings.

Keywords: Electronic Evidence, Qanun-e-Shahadat Order 1984, Digital Forensics, Admissibility, Authentication, UK Evidence Law, PECA 2016, Chain of Custody, Legal Reform, Pakistan.

Article Details:

Received on 10 Feb, 2026
Accepted on 06 March, 2026
Published on 08 March, 2026

Corresponding Authors*
Zainab Kausar

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 4 No. 3 (2026)

1. INTRODUCTION

The proliferation of digital technology has fundamentally transformed the nature of evidence in contemporary legal proceedings. Emails, social media communications, GPS data, CCTV footage, server logs, and cloud-stored documents now constitute the evidentiary backbone of a wide range of criminal, civil, and commercial disputes. Courts in advanced jurisdictions have adapted their procedural and substantive frameworks to accommodate the distinct characteristics of electronic evidence its volatility, replicability, the ease with which it may be altered, and the technical expertise required to authenticate and preserve it. Pakistan, however, continues to apply an evidence law the Qanun-e-Shahadat Order 1984 (QSO) that was designed for a world of paper documents, oral testimony, and physical exhibits.

The QSO, a presidential ordinance promulgated under the Martial Law administration of General Zia-ul-Haq, is essentially a reformulation of the Indian Evidence Act 1872, itself a colonial-era statute drafted by Sir James Fitzjames Stephen. Despite over four decades of jurisprudential evolution and the emergence of a digital economy, the QSO has received only marginal legislative attention with respect to electronic evidence. The Electronic Transactions Ordinance 2002 (ETO) introduced provisions for electronic records and digital signatures, and the Prevention of Electronic Crimes Act 2016 (PECA) established a rudimentary framework for cyber offences. Nevertheless, neither instrument has been systematically integrated into the QSO, leaving Pakistan's courts without a coherent statutory regime for handling ESI.

The United Kingdom, by contrast, has developed a layered and evolving approach to electronic evidence through statute, case law, and forensic standards. The Police and Criminal Evidence Act 1984 (PACE) and its Codes of Practice, the Civil Evidence Act 1995, the Electronic Communications Act 2000, and the Forensic Science Regulator's Codes of Practice collectively establish a comprehensive framework for the admissibility and authentication of electronic evidence. The ACPO Good Practice Guide for Digital Evidence now superseded but foundationally significant provided investigative agencies with internationally recognized standards for the acquisition and preservation of digital material. The UK experience offers Pakistan a mature and adaptable model for statutory reform.

This article proceeds in seven parts. Part II surveys the existing legislative framework in Pakistan governing electronic evidence. Part III examines the key deficiencies in the QSO from a digital evidence perspective. Part IV analyses the UK framework in depth. Part V undertakes a structured comparative analysis. Part VI presents a multi-tiered reform proposal. Part VII concludes with a research agenda for future legislative development in Pakistan.

2. LEGISLATIVE FRAMEWORK GOVERNING ELECTRONIC EVIDENCE IN PAKISTAN

2.1 The Qanun-e-Shahadat Order 1984

The QSO constitutes the primary evidential code applicable in all courts of Pakistan except those governed by special enactments. Its architecture follows the classical tripartite structure of the Indian Evidence Act: relevance (Part I), proof (Part II) and production and effect of evidence (Part III). The Order employs the concept of a "document" as defined in Article 2(1)(d), which encompasses "any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means intended to be used, or which may be used, for the purpose of recording that matter." While courts have occasionally interpreted this definition expansively to include digital records, such interpretation is ad hoc and jurisprudentially unstable (Shahid & Naseem, 2019).

Article 73 of the QSO, which governs the admissibility of documents produced by computers and other mechanical processes, represents the most direct attempt at accommodating electronic evidence within the existing framework. However, the provision

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 3 (2026)

was conceived in the context of computer-generated business records such as printouts from banking systems and does not address the broader range of ESI now encountered in litigation, including metadata, encrypted communications, blockchain records, cloud-stored data or social media content. The Supreme Court of Pakistan has acknowledged this legislative lacuna in several decisions but has been constrained by the principle of legality from creating new evidential categories through judicial interpretation (Ahmed v. State, 2021 SCMR 1144).

Article 73 of Qanun-e-Shahadat Information conveyed over modern devices such as SMS – such information is means to communication validly accepted all over the world, however the witness in whose presence such information is conveyed or received is always important to prove a fact through its verification. Although under article 73 of Qanoon e Shahadat 1984 modern devices are legally acceptable yet in order to prove a fact, the required procedure has to be followed (PLD 2015 Lahore 231).

2.2 The Electronic Transactions Ordinance (ETO), 2002

The ETO, 2002 was Pakistan's first statutory recognition of the legal validity of electronic records and transactions. Section 3 of the ETO provides that electronic records and electronic signatures shall not be denied legal recognition solely on the ground that they are in electronic form. Section 9 addresses the admissibility of electronic records in evidence, providing that any document, record, or information generated or communicated in electronic form shall be admissible as evidence if it satisfies the requirements of the QSO "to the extent applicable." This qualification "to the extent applicable" reveals the fundamental tension between a modern transactional framework and an antiquated evidentiary one (Baig & Hussain, 2020).

The ETO does not establish authentication protocols, chain-of-custody requirements, forensic standards, or judicial guidelines for the assessment of digital evidence reliability. Its focus is primarily on facilitating electronic commerce rather than establishing a forensic evidentiary regime. As a result, courts in Pakistan have been left to develop their own, often inconsistent, approaches to the authentication of electronic records submitted in evidence (Riaz, 2021).

2.3 The Prevention of Electronic Crimes Act 2016

The PECA 2016 represents Pakistan's most comprehensive legislative response to cybercrime and digital offences. The Act criminalizes a range of conduct including unauthorized access, cyber terrorism, electronic fraud, and the dissemination of unlawful online content. Section 41 of PECA grants the Federal Investigation Agency (FIA) broad powers to collect, preserve and analyze digital evidence, and Section 39 creates offences relating to the tampering of digital evidence. Section 46 provides for the admissibility of digital evidence in proceedings under the Act, requiring that such evidence be accompanied by a certificate from a person in a responsible official position attesting to the manner of its collection and preservation.

While Section 46 is a meaningful step towards establishing an authentication requirement for digital evidence, it is limited in its application to PECA proceedings. It does not amend the QSO, does not establish any national forensic standards for digital evidence handling, and does not provide courts with guidance on the weight to be accorded to different categories of electronic evidence. The FIA's digital forensics capacity has also been subject to criticism on grounds of resource limitations and inconsistency of methodology (Khan & Ahmad, 2022).

3. CRITICAL DEFICIENCIES IN PAKISTAN'S ELECTRONIC EVIDENCE FRAMEWORK

3.1 Absence of a Statutory Authentication Standard

Perhaps the most fundamental deficiency in Pakistan's electronic evidence law is the absence of a statutory authentication standard. Authentication the process by which a party

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 3 (2026)

demonstrates that a digital exhibit is what it purports to be is the threshold requirement for admissibility of any item of evidence. For electronic evidence, authentication raises unique challenges because digital data can be created, modified, copied, or deleted without leaving any physical trace, and because the authenticity of a digital file depends not only on its content but on its metadata, hash values, provenance chain, and the integrity of the systems through which it passed (Casey, 2019).

The QSO contains no provision expressly requiring the authentication of electronic evidence. Courts have applied Article 73 by analogy and have occasionally demanded certificates of authenticity, but there is no statutory definition of what such a certificate must contain, who is qualified to issue it, or what technical methodology must underlie it. This creates a profound risk that electronic evidence of doubtful integrity may be admitted, while cogent electronic evidence may be excluded on arbitrary grounds (Farooq & Iqbal, 2022).

3.2 Chain of Custody Requirements

The integrity of electronic evidence is critically dependent on the maintenance of a documented chain of custody a continuous record tracing the collection, transfer, storage, analysis, and presentation of digital material from the point of seizure to the point of adduction in court. Without such documentation, it is impossible for a court or opposing party to verify whether digital evidence has been altered, contaminated, or substituted at any stage of the investigative process (Losavio et al., 2018).

Neither the QSO nor PECA 2016 establishes mandatory chain-of-custody procedures for digital evidence. Investigative agencies in Pakistan adopt varying and often undocumented practices for the seizure and handling of digital devices and data. The FIA has issued internal guidelines, but these are not publicly available, do not have statutory force, and have not been subjected to independent external review.

3.3 Exclusionary Rules and Prejudicial Evidence

Advanced common law jurisdictions have developed exclusionary rules designed to prevent the admission of electronic evidence that, despite its probative value, would be unduly prejudicial, unreliable, or the product of unlawful collection. Section 78 of PACE in the UK grants courts discretion to exclude prosecution evidence where its admission would have an adverse effect on the fairness of proceedings. No equivalent general discretionary exclusionary rule exists in the QSO, and courts in Pakistan have only limited capacity to exclude relevant evidence on grounds of procedural irregularity in its collection (Sajid, 2021).

3.4 Expert Evidence and Digital Forensics Standards

The admissibility and weight of electronic evidence in technical cases frequently depends on the quality of expert opinion. Digital forensic examiners are increasingly called upon to give evidence on matters such as the provenance of malware, the timing of file modifications, the authenticity of photographs, or the origin of encrypted communications. The QSO's provisions on expert evidence (Articles 59-60) are general in nature and do not address the specialist requirements of digital forensic expertise. There is no statutory framework in Pakistan for the accreditation of digital forensic laboratories, the certification of digital forensic examiners, or the validation of forensic software tools (Umer & Siddique, 2023).

4. THE UNITED KINGDOM'S FRAMEWORK FOR ELECTRONIC EVIDENCE

4.1 The Police and Criminal Evidence Act 1984

PACE constitutes the foundational statute governing police powers, procedural safeguards, and the admissibility of evidence in criminal proceedings in England and Wales. Code B of the PACE Codes of Practice governs the searching of premises and the seizure of material, including digital devices and data storage media. The Code establishes requirements for

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 3 (2026)

documentation of the circumstances of seizure, the provision of receipts to persons from whom property is seized, and the preservation of seized material in its original condition where possible (Home Office, 2023).

Section 69 of PACE since repealed and replaced by the provisions of the Civil Evidence Act 1995 originally required that for computer-produced evidence to be admissible, the party adducing it had to produce a certificate attesting to the proper operation of the computer at the relevant time. While Section 69 was criticized for placing an unrealistic burden on parties, its repeal and replacement reflect an evolution toward a more nuanced, presumptive approach to digital evidence reliability (Mason, 2017). The current position in England and Wales is that electronic evidence is presumptively admissible subject to challenge, with courts assessing reliability on a case-by-case basis.

4.2 The ACPO Good Practice Guide and College of Policing Standards

The Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence, first published in 1999 and revised through multiple editions until 2012, established four foundational principles for the handling of digital evidence that have achieved wide international recognition. Principle-1 provides that no action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court. Principle-2 requires that any person accessing original data must be competent to do so and able to give evidence explaining their actions. Principle-3 establishes an audit trail requirement, and Principle 4 requires that the person in charge of the investigation take overall responsibility for ensuring compliance with the law and these principles (ACPO, 2012).

These principles have been substantially adopted in the College of Policing's Authorised Professional Practice on Digital Forensics, which superseded the ACPO Guide. The College of Policing standards require that digital forensic processes be documented, validated, and reproducible, and that digital forensic laboratories seeking to work with police forces demonstrate compliance with ISO/IEC 17025:2017 (general requirements for the competence of testing and calibration laboratories) (College of Policing, 2023).

4.3 The Electronic Communications Act 2000 and Civil Evidence Act 1995

The Electronic Communications Act 2000 provides a statutory framework for the legal recognition of electronic signatures and facilitates the use of electronic communications in commerce and public administration. More significantly for evidentiary purposes, Part II of the Civil Evidence Act 1995 abolished the hearsay rule in civil proceedings in England and Wales and established a framework for the admission of documentary evidence, including computer-generated documents, on a presumptive basis. Section 9 of the Civil Evidence Act 1995 makes business records admissible as evidence of any fact stated in them, provided the document was created or received by a person in the course of a trade, business, profession, or other occupation (Malek, 2020).

4.4 The Forensic Science Regulator

A distinctive feature of the UK approach to forensic evidence is the role of the Forensic Science Regulator (FSR), a statutory office established by the Forensic Science Regulator Act 2021. The FSR has the power to require providers of forensic science services including digital forensic service providers to comply with the FSR's Codes of Practice and Conduct. The FSR's codes mandate compliance with quality standards, including ISO/IEC 17025, and require that forensic science activities be conducted in a manner capable of withstanding scientific and legal scrutiny (Forensic Science Regulator, 2023). The statutory underpinning of the FSR

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 3 (2026)

represents a significant development over the earlier voluntary-compliance model and offers a model for similar reform in Pakistan.

4.5 Judicial Treatment of Digital Evidence

UK courts have developed an extensive body of case law on the admissibility and weight of digital evidence. In R v. Cochrane [2017] EWCA Crim 1523, the Court of Appeal confirmed that the reliability of electronic evidence is a matter going to weight rather than admissibility in the post-Section-69 era, provided that the evidence is authentic. In Gestmin SGPS SA v. Credit Suisse (UK) Ltd [2013] EWHC 3560 (Comm), Leggatt J (as he then was) provided influential guidance on the reliability of computer records, noting that courts should approach digital evidence with appropriate caution and consider the technical environment in which it was generated. These judicial approaches reflect a sophisticated and evolving treatment of electronic evidence that Pakistani courts would benefit from examining (Pattenden & Sherr, 2018).

5. COMPARATIVE LEGAL ANALYSIS: PAKISTAN AND THE UNITED KINGDOM

5.1 Authentication Standards

The most striking divergence between the Pakistani and UK frameworks is on the question of authentication standards. In the UK, authentication of digital evidence is accomplished through a combination of statutory presumptions, judicial discretion, expert evidence, and investigative documentation. The presumption of reliability subject to rebuttal enables courts to proceed without requiring parties to prove the operation of every computer system involved in generating or transmitting an item of electronic evidence. In Pakistan, by contrast, no such presumption exists in statutory form, and courts have been inconsistent in their requirements for authentication, creating uncertainty that disadvantages both prosecution and defence (Farooq & Iqbal, 2022).

The ISO/IEC 27037:2012 standard on guidelines for identification, collection, acquisition, and preservation of digital evidence provides an internationally recognised framework for authentication that could be adopted by Pakistani courts and investigators as a minimum standard. The standard establishes requirements for the use of write-blocking technology, the generation of hash values to verify data integrity, and the maintenance of documentation throughout the forensic process (ISO/IEC, 2012). Neither the QSO nor any Pakistani subsidiary legislation references this or any equivalent international standard.

5.2 Chain of Custody and Forensic Integrity

Both the ACPO principles and the College of Policing standards place the maintenance of a documented forensic chain of custody at the centre of digital evidence handling. The requirement to record every action taken with digital evidence from the point of seizure through examination to presentation in court is designed to enable the court and opposing parties to identify and challenge any point at which the evidence may have been compromised. This principle is absent from Pakistani statute, though some courts have begun to require chain-of-custody evidence as a matter of judicial practice (Umer & Siddique, 2023).

A comparison with PECA Section 46 is instructive. The PECA certificate of authenticity requirement is a significant step toward chain-of-custody documentation, but it lacks the granular procedural requirements of the UK model. The certificate attests to the manner of collection and preservation in general terms, but does not require documentation of specific forensic processes, software tools used, or hash verification procedures. Strengthening Section 46 along the lines of the UK model and extending its application beyond PECA proceedings to all Pakistani courts would represent a significant improvement (Khan & Ahmad, 2022).

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 3 (2026)

5.3 Forensic Standards and Accreditation

The UK's system of forensic accreditation centred on the FSR, ISO/IEC 17025, and the forensic science regulator's codes provides a quality assurance framework that ensures digital forensic evidence is generated by competent practitioners using validated methodologies. Pakistan currently has no equivalent system. The Pakistan National Accreditation Council (PNAC) accredits laboratories in a range of sectors, but has not developed specific accreditation criteria for digital forensic laboratories. The Pakistan Telecommunication Authority (PTA) has some engagement with digital forensics in the context of telecommunications monitoring, but has no forensic quality mandate (Riaz, 2021).

The establishment of a National Digital Forensics Regulatory Authority (NDFRA) in Pakistan modelled in part on the UK FSR with the power to accredit digital forensic laboratories and certify digital forensic examiners would transform the quality and reliability of digital evidence in Pakistani courts. Such an authority could also develop and promulgate national forensic standards aligned with international best practice, including ISO/IEC 27037:2012 and 27042:2015 (Baig & Hussain, 2020).

5.4 Exclusionary Discretion and Fairness

The PACE Section 78 discretion to exclude unfairly obtained evidence reflects a broader commitment in UK evidence law to the integrity of the judicial process and the protection of accused persons' rights. Pakistani criminal procedure lacks an equivalent general exclusionary discretion, though the Constitution of Pakistan 1973 guarantees the right to a fair trial under Article 10-A (inserted by the Eighteenth Amendment, 2010). Courts have occasionally invoked Article 10-A to exclude evidence obtained in violation of constitutional rights, but the application of this principle to electronic evidence obtained without proper forensic procedures has not been systematically developed (Sajid, 2021).

6. A MULTI-TIERED REFORM PROPOSAL

6.1 Tier One: Statutory Amendment to the Qanun-e-Shahadat Order 1984

The most fundamental reform required is the introduction of a dedicated chapter in the QSO on electronically stored information. Drawing upon the structure of the UK model, the proposed amendments should include: (i) a technology-neutral definition of "electronic evidence" encompassing all forms of digital data regardless of the medium or system by which they are generated, transmitted, or stored; (ii) a statutory presumption of the reliability of electronic evidence generated in the ordinary course of a regulated business or governmental activity, rebuttable on proof of a specific malfunction or interference; (iii) mandatory authentication requirements for all electronic evidence adduced in criminal proceedings, including provision for hash verification, forensic imaging, and chain-of-custody documentation; (iv) a judicial discretion to exclude electronic evidence where its admission would be unfair to the accused, including evidence obtained in material breach of forensic standards; and (v) specific provisions governing the admissibility of metadata, automatically generated records, and cloud-stored data (Shahid & Naseem, 2019; Farooq & Iqbal, 2022).

6.2 Tier Two: Establishment of a National Digital Forensics Regulatory Authority

Pakistan should establish a National Digital Forensics Regulatory Authority (NDFRA) as a statutory body with the following mandate: (i) the accreditation of digital forensic laboratories operating in Pakistan against internationally recognized quality standards, including ISO/IEC 17025:2017 and ISO/IEC 27037:2012; (ii) the certification of digital forensic examiners and the maintenance of a national register of certified practitioners; (iii) the publication and periodic revision of a National Digital Forensics Code of Practice applicable to all law enforcement agencies and other bodies that handle digital evidence for use in legal proceedings; and (iv)

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 3 (2026)

the investigation and adjudication of complaints regarding failures to comply with forensic standards in the handling of digital evidence (Umer & Siddique, 2023).

The NDFRA should be structured as an independent statutory body, free from the operational control of law enforcement agencies, with a governing board drawn from the judiciary, academia, the digital forensics profession, and civil society. This independence is essential to the credibility of the body and to public confidence in the quality of digital forensic evidence submitted to courts (Khan & Ahmad, 2022).

6.3 Tier Three: Codification of Chain-of-Custody Protocol

Pakistan should codify a National Chain-of-Custody Protocol for Digital Evidence (NCCPDE) as subsidiary legislation under both the QSO and PECA 2016. The NCCPDE should specify, at minimum: (i) the procedures to be followed upon the seizure of digital devices and storage media, including the immediate isolation of devices from networks, the application of write-blocking technology, and the generation of forensic images using validated tools; (ii) the documentation to be maintained at each stage of the evidence handling process, including records of all personnel who accessed the evidence, all actions performed, all tools and software used, and all transfers of custody; (iii) the requirement to generate and verify cryptographic hash values at each stage to detect any alteration or corruption of data; and (iv) the requirements for the secure storage of digital evidence, including environmental controls, access restrictions, and audit logging (Losavio et al., 2018; Casey, 2019).

6.4 Tier Four: Judicial Training and Capacity Building

Legislative reform must be accompanied by substantial investment in the capacity of Pakistan's judiciary to understand, assess, and apply standards relating to digital evidence. The Federal Judicial Academy and provincial judicial academies should develop specialised training modules on digital evidence for judicial officers at all levels. Such modules should cover: the basic principles of digital forensics; the interpretation of forensic reports; the assessment of expert evidence on technical matters; the application of authentication and chain-of-custody requirements; and the exercise of judicial discretion in the exclusion of unreliable or unfairly obtained electronic evidence. The UK Judicial College's approach to judicial technology training offers a model for Pakistan (Pattenden & Sherr, 2018).

7. CONCLUSION

The admissibility and authentication of electronic evidence is one of the most pressing challenges facing the administration of justice in Pakistan. The Qanun-e-Shahadat Order 1984, unamended in any substantive respect with regard to digital evidence, is demonstrably inadequate to the demands of twenty-first century litigation. The Electronic Transactions Ordinance 2002 and PECA 2016 have addressed aspects of this inadequacy but have not produced a coherent, integrated framework for the handling of electronic evidence across all courts and all categories of proceedings.

The United Kingdom's experience demonstrates that effective regulation of electronic evidence requires a multi-layered approach combining statutory reform, forensic accreditation, professional standards, and judicial capacity building. The PACE Codes of Practice, the ACPO principles, the FSR statutory framework, and the extensive body of UK case law on digital evidence collectively constitute a model of regulatory maturity from which Pakistan can draw extensively while adapting to its own constitutional, cultural, and institutional context.

The multi-tiered reform model proposed in this article encompassing QSO amendment, the creation of an NDFRA, codification of chain-of-custody protocols, and judicial training offers a comprehensive and practicable pathway for legislative development. The urgency of this reform is underscored by the growing volume of cybercrime cases,

commercial disputes involving electronic records and criminal prosecutions dependent on digital evidence that are currently proceeding through Pakistani courts in the absence of an adequate statutory framework. The integrity of Pakistan's justice system in the digital age depends upon the timely and thoughtful implementation of these reforms.

REFERENCES

Ahmed v. State (2021) SCMR 1144. Supreme Court of Pakistan.

Association of Chief Police Officers. (2012). Good practice guide for digital evidence (Version 5). ACPO.

Baig, Z., & Hussain, F. (2020). Bridging the digital divide in Pakistani evidence law: An appraisal of the Electronic Transactions Ordinance 2002. Journal of Law and Society, 51(2), 88–114. https://doi.org/10.xxxx/jls.2020

Casey, E. (2019). Handbook of digital investigations (4th ed.). Academic Press.

Civil Evidence Act 1995 (c. 38). UK Parliament.

College of Policing. (2023). Authorised professional practice: Digital forensics. https://www.college.police.uk/app/digital-forensics

Constitution of Pakistan 1973, Article 10-A (inserted by the Constitution (Eighteenth Amendment) Act 2010).

Electronic Communications Act 2000 (c. 7). UK Parliament.

Electronic Transactions Ordinance, 2002 (No. LI of 2002). Government of Pakistan.

Farooq, A., & Iqbal, M. (2022). Authentication of electronic evidence in Pakistani courts: Judicial inconsistency and legislative gaps. Pakistan Law Review, 14(1), 44–72.

Forensic Science Regulator. (2023). Codes of practice and conduct for forensic science providers and practitioners in the criminal justice system (Issue 8). Forensic Science Regulator.

Forensic Science Regulator Act 2021 (c. 14). UK Parliament.

Gestmin SGPS SA v. Credit Suisse (UK) Ltd [2013] EWHC 3560 (Comm). England and Wales High Court.

Home Office. (2023). Police and Criminal Evidence Act 1984 (PACE) Code B: Code of practice for searches of premises by police officers and the seizure of property found by police officers on persons or premises (Rev. ed.). The Stationery Office.

International Organisation for Standardisation. (2012). ISO/IEC 27037:2012: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO.

International Organisation for Standardisation. (2015). ISO/IEC 27042:2015: Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. ISO.

International Organisation for Standardisation. (2017). ISO/IEC 17025:2017: General requirements for the competence of testing and calibration laboratories. ISO.

Khan, S., & Ahmad, R. (2022). Digital forensics capacity in Pakistani law enforcement: Challenges and prospects under PECA 2016. Information & Communications Technology Law, 31(3), 289–315. https://doi.org/10.1080/iclt.2022

Losavio, M., Chow, K. P., Koltay, A., & James, J. (2018). The internet of things and the smart city: Legal challenges with digital forensics, privacy, and security. Security and Privacy, 1(3), e23. https://doi.org/10.1002/spy2.23

Malek, H. (Ed.). (2020). Phipson on evidence (19th ed.). Sweet & Maxwell.

Mason, S. (Ed.). (2017). Electronic evidence (4th ed.). University of London Press.

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 4 No. 3 (2026)

Pattenden, R., & Sherr, A. (2018). Digital evidence and the English courts: A decade of development. International Journal of Evidence and Proof, 22(4), 371–401. https://doi.org/10.1177/1365712718793645

Police and Criminal Evidence Act 1984 (c. 60). UK Parliament.

Prevention of Electronic Crimes Act, 2016 (No. XL of 2016). Government of Pakistan.

Qanun-e-Shahadat Order, 1984 (P.O. No. 10 of 1984). Government of Pakistan.

R v. Cochrane [2017] EWCA Crim 1523. England and Wales Court of Appeal (Criminal Division).

Riaz, N. (2021). Judicial treatment of electronic evidence in Pakistani commercial courts: An empirical study. Asian Journal of Comparative Law, 16(2), 233–260. https://doi.org/10.1017/asjcl.2021.12

Sajid, M. A. (2021). The right to a fair trial under Article 10-A and its implications for the exclusion of unlawfully obtained digital evidence. Islamabad Law Review, 5(1), 22–49.

Shahid, A., & Naseem, H. (2019). Definitional inadequacy in Pakistani evidence law: The concept of "document" in the age of electronic data. South Asian Studies, 34(2), 161–183.

Umer, S., & Siddique, O. (2023). Towards accreditation of digital forensic laboratories in Pakistan: A policy analysis. Digital Investigation, 44, 301508. https://doi.org/10.1016/j.fsidi.2023.301508