ACADEMIA International Journal for Social Sciences
Volume 4, Issue 4, 2025 ISSN-L (Online): 3006-6638

The Impact of Digital Evidence Laws on Cybercrime Prosecution in Pakistan

Zain Ullah
zainullah1214@gmail.com
BS Criminology Student, Department of Sociology and Criminology, University of Sargodha

Malik Kaleem Ullah
kaleem.ullah@uos.edu.pk
Lecturer, Department of Sociology and Criminology, University of Sargodha

Haider Abbas
haiderabbaszahoor3535@gmail.com
BS Criminology Student, Department of Sociology and Criminology, University of Sargodha
Corresponding Author: * Zain Ullah zainullah1214@gmail.com

Received: 21-10-2025 **Revised:** 24-11-2025 **Accepted:** 06-12-2025 **Published:** 26-12-2025

ABSTRACT

The massive development of digital technologies has transformed the nature of crime, and thus, there has been a corresponding increase in cybercrime and reliance on digital evidence in criminal justice systems. Cybercrime prosecution is regulated by the Prevention of Electronic Crimes Act (PECA) 2016, Qanun-e-Shahadat Order 1984 and the Electronic Transactions Ordinance 2002, which is mainly applicable in Pakistan. Even though such laws have formally accepted the existence of electronic records and digital evidence, their application efficiency when it comes to prosecuting cybercrimes is still not very effective. This research paper critically analyses effects of Pakistan laws on digital evidence on cybercrime prosecution and its implication on evidentiary admissibility, procedures in the investigations, forensic capacity, and judicial interpretation. Through the analysis of doctrinal legal sources and the available body of scholarly literature on the topic, the paper presents the following persistent challenges: ambiguity in authentication standards, weak chain-of-custody procedures, lack of technical expertise in law enforcement and the judiciary, and disjointed interpretation of the digital evidence rules in courts. The results demonstrate that the digital evidence is often handled as secondary evidence, instead of direct evidence, which harms the success of the prosecutorial efforts and leads to the poor conviction rate. The paper contends that as long as legal reforms are not done comprehensively, there are no standardized forensic procedures or capacity building to train investigators and judges, the laws governing digital evidence will remain to be a sham. The article ends by stating that the legal system of Pakistan must be aligned with the international best practice in order to prosecute cybercrime effectively as well as not to violate the constitutional provisions on the right to a fair trial process and due process.

Keywords: *Digital evidence, Cybercrime prosecution, PECA 2016, Electronic evidence, Digital forensics, Pakistan cyber laws, Admissibility of evidence, Chain of custody, Criminal justice system, Fair trial*

INTRODUCTION

Emergent information and communication technologies have radically changed the essence of crime, evidence and criminal investigation. In modern societies, a major part of human activity takes place on the digital platform, which leads to the creation of large volumes of electronic data. Emails, social media messages, mobile phone account documents, stored in the cloud, and records of digital transactions have become the key to both legitimate and illegal activities. Thus, cybercrime has become one of the most intricate and difficult types of criminal behavior, which requires no less complex legal and evidential

treatment (Casey, 2011; Brenner and Goodman, 2002). Digital evidence is an important element of the prosecution of cybercrime, whose lawful recognition, authentication, and admissibility are significant to the operation of modern criminal justice systems.

Cybercrimes, such as online fraud, identity theft, cyber harassment, unauthorized access to data, and digital financial crimes, have also been observed to grow in Pakistan, along with internet use and the digital services (Hamad et al., 2015; Zahid et al., 2024). Such crimes are more intangible in nature and are normally transacted across borders and this makes it even more difficult to investigate and prosecute. The Pakistani legal system has been traditionally structured to handle physical and documentary evidence and provided little advice on the processing of electronic records. The Qanun-e-Shahadat Order 1984, the document regulating the evidentiary issues, has not initially considered the specifics of the digital data, including metadata, encryption, or forensic imaging (Hameed et al., 2021).

The first legislative move towards the provision of a legal status to the electronic documents and signatures in Pakistan came with the introduction of the Electronic Transactions Ordinance 2002. Although the ordinance recognized evidence worth of electronic records, its use during criminal proceedings continued to be narrow and sporadic (Kundi et al., 2014). The passing of the Prevention of Electronic Crimes Act 2016 signified the change of paradigm as the law explicitly criminalized numerous cybercrimes and gave investigative agencies the authority to gather and store digital evidence. Although such a positive development has occurred regarding legislation, researchers mention that the very presence of cyber laws cannot be considered a guarantee of effective prosecution unless it is accompanied by well-developed evidentiary norms and institutional capabilities (Baloch, 2016; Khan, 2017).

The admissibility of the digital evidence is one of the most enduring challenges when it comes to the prosecution of cybercrime in Pakistan. Courts tend to be hesitant to accept only electronic evidence because of their fears on authenticity, integrity, and possible manipulations (Losavio et al., 2006). Nowadays, digital data can be readily modified, copied, or even destroyed unlike physical evidence, and thus it is important to preserve and document it accordingly. Chain of custody may often lack a standardized process making sure that there is a defence objection and judicial suspicion and consequently, digital evidence may be excluded or its weight minimized (Ieong, 2006; Mohay, 2005).

The lack of forensic capacity in the law enforcement bodies also contributes to the ineffectiveness of digital evidence laws. To achieve evidentiary reliability, digital forensic investigations need special tools, technical skills, and compliance with internationally accepted standards (McKemmish, 2008; Goodison et al., 2015). Nevertheless, empirical research reveals that Pakistani investigators are usually not well trained and equipped and make procedural errors when collecting and analyzing evidence (Riadi et al., 2017; Lohiya & John, 2015). These inadequacies not only contribute to weakening of prosecution cases but also cast grave consideration about the due process and right to fair trial.

Another dimension of concern to cybercrime prosecution is judicial capacity. The judges are the key figures in determining the admissibility and probative value of digital evidence but most of them are not trained to handle digital evidence or cyber law (Gogolin & Jones, 2010; Losavio et al., 2006). This lack of knowledge leads to inconsistent rulings and strengthens the notion of digital evidence as a secondary or supporting evidence and not the primary one. Consequently, the deterrent impact of cybercrime legislation could be reduced as even well-documented forensic evidence is not capable of generating convictions (Singleton, 2013).

The issue of drug prosecution of cybercrime in Pakistan is also beset by the problem of jurisdiction and transnationality. Most cybercrimes have transnational origins and this brings to the fore the jurisdiction, mutual legal aid and application of foreign evidence (Lunker, 2010; Brenner & Goodman, 2002). Although mechanisms of international cooperation like INTERPOL offer good assistance in capacity

building and exchange of intelligence, the national body of law is not well aligned with the international standards of cybercrime in Pakistan (INTERPOL, 2017; Fafinski, 2008).

Moreover, the use of online evidence has a great impact on constitutional rights and human rights. The Constitution of Pakistan (Article 10-A) provides the right to a fair trial, subject to the right to object to the evidence provided by the prosecution. Researchers claim that limited access to forensic reporting, proprietary software, and technical procedures makes it difficult to challenge digital evidence by the defence, thus preventing procedural fairness (Ryan and Shpantzer, 2017; Goodison et al., 2015). The art of prosecution and the safeguarding of civil liberties continue to be one of the key issues in the digital era.

Nevertheless, the available literature reiterates that digital evidence legislation has a significant potential to bolster cybercrime prosecution in case it is implemented appropriately. The global best practice emphasizes on the need to establish clear statutory definitions, recognized forensic labs, judicial education, and institutionalized investigative models (Casey, 2011; Martini and Choo, 2012). In Pakistan, though, there is a definite disparity between the will of the legislature and how it is implemented in real life, and that necessitates wholesale reform.

The research paper will be a contribution to the body of literature since it critically investigates the influence of digital evidence laws on the prosecution of cybercrime in Pakistan. Instead of just considering the legislative texts, it also considers their application in the criminal justice system and spotting the structural and procedural vulnerabilities which are barriers to effective implementation. The article is intended to guide policy changes through legal analysis and academic research to improve the performance of prosecutors and at the same time to respect the concept of justice, fairness and due process.

LITERATURE REVIEW

Rapid digital technology has raised the face of crime and radically changed the evidential terrain of criminal justice systems. The evidence that is generated by cybercrime is mainly in electronic form; these are digital logs, metadata, emails, call detail records, and social media data that are significantly different than the traditional physical or documentary evidence in relation to volatility, reproducibility, and manipulation (Casey, 2011). Due to these factors, researchers point to the fact that the success of cybercrime prosecution is directly related to the availability of the strong digital evidence legislation, which distinctly governs the admissibility, authentication, and preservation requirements (Brenner, 2013; Kerr, 2015).

The partnership between legal recognition of digital evidence and lack of clarity in the procedure is always emphasized in international literature. Practice in technologically developed jurisdictions has indicated that clear rules on the evidences of integrity, the acquisition of data, and the chain of custody, increase the judicial confidence and prosecution achievement in computer crimes (Gercke, 2012; Nelson et al., 2019). On the other hand, unclear legal rules can make the courts distrustful of electronic evidence, thereby imposing a higher standard of corroboration or a blanket exclusion, even in cases where the evidences have a high probative value (Casey & Ferraro, 2021).

The institutional and technical constraints also increase the difficulties that come with digital evidence in creating legal systems. According to comparative research, even though statutes on cybercrime have been implemented in most nations, their laws on evidences often fall behind the technological reality, which results in a failure to match criminalization and enforcement (Wall, 2017; Broadhurst et al., 2018). Experts believe that in such cases, the practicality of the digital evidence laws is not substantially supported by weak forensic infrastructure, absence of unified investigative procedures, and untrained judicial systems (Kerr, 2015).

The laws that regulate the digital evidence in Pakistan have been developed over time and are still under much academic discussion. As the main law of evidence, the Qanun-e-Shahadat Order 1984 was designed before the digital age and lacks a comprehensive coverage of the issues of electronic authentication, information integrity, and the ability to verify the information via forensic means (Mehmood, 2017). Even though Article 164 does not forbid the use of modern devices to produce evidence, researchers claim that its discretionality has led to uneven interpretation by courts and confusion of the evidentiary standards (Shah, 2018).

The introduction of Electronic Transactions Ordinance 2002 was a significant move in that electronic documents and signatures were accorded legal status. Nonetheless, according to the views of legal experts, the main purpose of the Ordinance was to streamline the e-commerce and civil processes, which provide a scanty backing in the criminal cases related to the digital evidence (Ahmed & Qazi, 2019). Through this, the courts maintained the use of traditional principles of evidentiary standards and frequently viewed electronic records as secondary or corroborative evidence and not as independent evidence.

The enactment of the Prevention of Electronic Crimes Act 2016 was an important legislative move that criminalized a broad scope of cyber-related activities and gave the law enforcement agencies the mandate to gather and retain electronic information. Available literature recognizes PECA 2016 as the response needed to the increasing rate of cybercrime in Pakistan (Zafar & Raza, 2020). However, the Act is extensively criticized by scholars due to the focus on the evidentiary procedures, specifically, the lack of specifications that control forensic authentication, data preservation, and chain-of-custody provisions (Hameed et al., 2021).

The judicial interpretation of the laws concerning digital evidence in Pakistan has become one of the most important issues of the literature. Reported judgment analyses show that there is a high level of variation in the judicial assessment of electronic evidence, especially when it comes to the mobile phone data, call detail records, and internet communications (Nazir et al., 2025). Other courts have been progressive and accepted electronic records as per Article 164 of the Qanun-e-Shahadat Order, whereas other courts have placed onerous corroboration conditions based on the traditional evidentiary norms (Rehman, 2020). This inconsistency is explained by scholars through the lack of familiarity with the digital forensic principles by the judges instead of the intrinsic weaknesses of the evidence (Casey, 2011).

The other common theme within the Pakistani literature of cybercrime prosecution is the issue of chain-of-custody. The current international best practices emphasize that digital evidence should be gathered and stored in a way that involves forensically reliable practices that can avoid changes and contamination (Nelson et al., 2019). According to the Pakistani studies, however, the weak documentation practices, absence of accredited forensic laboratories and absence of training of investigating officers all weaken the evidentiary credibility and weaken prosecution cases (Rashid and Ali, 2021; Gul et al., 2025). There is an opportunity to have an acquittal or a long trial as the defence counsel often object to electronic evidence on procedural grounds.

Another issue that the literature addresses is the issue of tension between the effective implementation of cybercrime and the constitutional rights. Researchers warn that extensive investigative authority under PECA 2016, such as surveillance and data interception, pose very severe questions of privacy and the right to a fair trial under Article 10-A of the Constitution of Pakistan (Khan and Mahmood, 2022). As a reaction to such concerns, courts tend to be conservative about digital evidence, which, although protecting due process, can also undermine the effectiveness of prosecutors (Rehman, 2020).

The recent academic literature is starting to focus more on the necessity of institutional and procedural change as opposed to the increased legislative growth. Such recommendations as the creation of special

cybercrime courts, the certification of digital forensic labs, forensic training of investigators, and the ongoing judicial education of electronic evidence analysis should be made (Ahmed et al., 2023; Zahid et al., 2024). According to comparative analyses, these kinds of reforms have a great positive effect on the practical realization of digital evidence laws and do not impair procedural fairness (Gercke, 2012; Kerr, 2015).

Although there has been an increasing amount of information on cybercrime and digital evidence in Pakistan, there is still a acute gap in the systematic evaluation of the impact of digital evidence laws on the result of prosecution in Pakistan. The majority of available research is either statutory analysis or a solitary judicial ruling, which does not give much understanding of the longer-term interrelation between evidentiary law and forensic practice and prosecutorial efficiency. This paper aims to fill this gap by critically exploring how laws of digital evidence affect the prosecution of cybercrimes in Pakistan with a focus on admissibility tests, the practice of forensics and judicial interpretation.

METHODOLOGY

Research Design

The research design used in this paper is a qualitative doctrinal research study to examine the effects of the laws on digital evidence in regards to prosecuting cybercrimes in Pakistan. Legal research involving interpretation, application and effectiveness of statutes and judicial decisions in particular are best served using doctrinal research. The design allows conducting a systematic study of the legislation regulating the use of digital evidence and its practical dimension of cybercrime prosecution in the Pakistani criminal justice system.

Sources of Data

The research is informed by the primary and secondary sources of law. Relevant statutory instruments which include the Prevention of Electronic Crimes Act 2016, the Qanun-e- Shahadat Order 1984, the Electronic Transactions Ordinance 2002, and the relevant constitutional provisions especially Article 10-A of the Constitution of Pakistan all form part of the primary sources. Moreover, higher court judgments and trial court judgments that have dealt with cybercrime and electronic evidence have been studied in order to know how judicial interpretation works and how evidentiary practices work.

The secondary sources include peer-reviewed journal articles, books, law reviews, policy reports, and conference papers obtained in Google Scholar. These sources offer theoretical views, comparative and critical analysis of the digital evidence laws and cybercrime prosecution both nationally and internationally.

Data Analysis Technique

The analysis used in the study is qualitative content analysis used to assess statutory provisions and judicial decisions. Legal documents are examined to determine their clarity, coverage and procedural sufficiency in respect to the admissibility, authentication, and preservation of the digital evidence. Cases on judicial rulings are reviewed to come up with trends on acknowledgment or denial of electronic evidence focusing mainly on the aspects of chain of custody, forensics confirmation, and discretion by the judiciary.

Comparative Perspective

Comparative approach is limited in an attempt to frame the legal framework of Pakistan in the wider international practices. The best practices in digital evidence management and prosecution of cybercrimes

are featured with references to the selected foreign jurisdictions and international standards. This comparison is purely to provide an analysis, not to generalize the foreign legal models to Pakistan.

Scope and Limitations

The research is limited to doctrinal and qualitative research and does not entail empirical research techniques like surveys and interviews. Consequently, the conclusions are made on the foundation of the legal texts and judicial practice as opposed to the perception of the stakeholders. The analysis is further preoccupied with reported cases and available legal materials, which might not be exhaustive to capture the unreported practices at trial-level. In spite of these shortcomings, these limitations do not undermine the methodology as it is sufficient to analyze how the laws on digital evidence affect the prosecution of cybercrime in Pakistan.

FINDINGS AND DISCUSSION

Legal Advocacy in the Admissibility of the Digital Evidence

The paper arrives at the conclusion that despite considerable efforts by Pakistan to acknowledge electronic evidence under the Prevention of Electronic Crimes Act (PECA) 2016, the rule is still not applied in practice in the courts. The issue of judicial suspicion of electronic evidence is usually associated with its authenticity, integrity, and chain of custody, which results in the cautiousness of decision-making (Shah, 2018; Ahmed and Qazi, 2019). As an example, judges have often required corroborating evidence with digital evidence in cases reported, as it is an indication of mistrust in forensic examination in isolation (Nazir et al., 2025; Rehman, 2020). This reluctance not only increases the time in litigation, but also may lead to acquittals, nullifying the deterrent impact of the cybercrime laws. The variation in judicial interpretations evidences that the statutory recognition is not enough, and courts need strong forensic support and the appropriateness of procedures, so that they can be confident in admitting electronic evidence.

Furthermore, the research indicates that judges tend to experience problems in the process of decoding technicalities of digital evidence. The terminologies like hash value, metadata and encryption keys are not well known to most members of the judiciary, and thus procedural errors or cautionary judgment are made. This finding is consistent with the literature in other countries, that emphasizes judicial education on technical aspects to ensure proper adjudication of cybercrimes incidents (Casey, 2011; Nelson et al., 2019). In the absence of specific training, the judges will be unprepared to determine the admissibility and reliability of electronic evidence, which eventually influences the rate of prosecution.

Procedural and Institutional Limitations

Case law and proceeding practice analysis show that there are significant procedural constraints in Pakistan. Mobile phone records, emails, and social media messages are often inadmissible in court because evidence was not collected properly, the forensic analysis is not performed, and the documentation is not made (Rashid and Ali, 2021). In an interesting case with a result in a financial fraud committed via online banking, important transaction logs were held inadmissible since the collection was not done in accordance with the established forensic procedures. The lapses in such procedures highlight the importance of having standard operating procedures and detailed guidelines on how to handle digital evidence.

Pakistan tends to have unaccredited, inconsistent, and low-tech laboratory forensics in institutions (Gul et al., 2025). There are also issues of insufficient staffing, inappropriate technical training, and the lack of resources in law enforcement facilities, which complicates investigations (Ahmed et al., 2023). Comparative research points out that those nations where special units of cybercrime, certified

laboratories, and formalized training of judicial personnel exist record greater success rates in convicting cases of cybercrime (Casey and Ferraro, 2021; Goodison et al., 2015). These results highlight that institutional empowerment should be an addition to legislative reform to make the digital evidence laws as effective as possible.

Gaps in Legal Clarity

Although PECA 2016 is very broad in its coverage of cybercrimes such as unauthorized access, electronic fraud, child pornography, and cyber harassment- there are still some areas that are ambiguous. Such definitions as unauthorized access, critical infrastructure, or intercepted communication are not defined legally accurately, which provides defense lawyers with an opportunity to use interpretative loopholes (Hameed et al., 2021; Khan and Mahmood, 2022). Such indistinctness decreases the effectiveness of prosecutors, especially when dealing with difficult cases of financial fraud, identity theft and cyber harassment. The same arguments appear in the global literature, stating that digital evidence laws should be made transparent to prevent any uncertainty in the judges and their manipulation by the defense (Gercke, 2012; Wall, 2017).

Moreover, the lack of well-defined procedure guidelines in the collection, preservation and presentation of digital evidence adds to legal uncertainties. The inefficiency of the court process often asks the supplement of evidence or refuses to accept electronically acquired data because of the flaws in the procedure, which reduces the deterrent effect of cybercrime legislation. This disconnect between the statutory will and its practical implementation shows that it is necessary to keep the legislation under constant revision and provide clear procedural rules to keep the cybercrimes in line with their ever-changing nature.

The Problems of Cross-Border Cybercrime

The researchers conclude that a significant number of cybercrimes in Pakistan are international in nature, in which the foreign servers, cloud storage, and networks are located outside the national jurisdictions. This international character makes it difficult to prosecute and, in most cases, the national laws cannot provide enough evidence and be used to prosecute (Wall, 2017; Broadhurst et al., 2018). An example here is the fraud cases and data theft incidences that have been perpetrated by criminal elements in other nations, which end up being prosecuted or dismissed since it is difficult to retrieve evidence of a crime committed in another nation.

The countries that have established mutual legal assistance treaties (MLATs) and a system of international cooperation have a higher level of success in cross-border cybercrime prosecution (Brenner, 2013; Nelson et al., 2019). The lack of engagement in such collaborative structures limits the capability of Pakistan to follow the digital evidences across jurisdictions, which support the necessity of the formalization of international agreements and capacity building efforts. Enhancement of cross-border collaboration is important to make sure that digital evidence remains useful to prosecute cybercriminals crossing the national boundaries.

Technological Sufficiency and Forensic Standards

Another significant hindrance to effective use of digital evidence is technological inadequacies. The study reveals the weaknesses in the procedures, which in its international understanding qualify as forensically sound, on such areas as data hashing as well as write-blocking and audit trails, which need to be established to ensure the integrity and authenticity of digital evidence (Casey, 2011; Nelson et al., 2019). In Pakistan, such mishandling, unwanted alteration or partial mining of data would usually result into rejection of evidence in court. An example of such practical implications of the lack of technology adequacy is that evidence gathered without standardized forensic verification has been ignored by the

courts in cases related to email spoofing or data theft in the cloud, reflecting the practical implications of the lack.

To build more confidence in electronic evidence, there is need to adopt internationally recognized forensic tools and procedures. Such practices as forensic imaging, chain-of-custody records, and metadata confirmation contribute value not only to the admissibility of digital evidence but also brings the practices of Pakistan to the standards of the global community and improves the successful prosecution.

Judicial and Law Enforcement Training

The results indicate that there is a great necessity to train and educate not only the judicial officers but also the law enforcement officers on constant basis. The lack of technical knowledge leads to the reluctance of electronic evidence by judges who add to the time delays and procedural issues (Rehman, 2020; Ahmed et al., 2023). According to the international best practices, judicial trainings, workshops, and practical forensic exposure can substantially enhance confidence in digital evidence, minimise evidentiary challenges, and speedy and impartial processing of cybercrime cases (Goodison et al., 2015; Gercke, 2012). On the same note, police personnel would need special training in digital forensic investigation in order to guarantee that evidence is collected, preserved, and presented properly as per the legal requirements.

The most lasting obstacle to the prosecution of cybercrimes would be overcome through the implementation of extensive capacity-building programs. Through systematic training, the judges and the investigators would be able to understand the complicated digital evidence, lessen on expert testimony in situations of simple technical problems, and enhance the overall efficiency of the justice system.

Finding a balance between the Privacy and Prosecution

One of the most significant results is the conflict between the right of privacy and the investigative authority. The Constitution of Pakistan in article 10-A of the Constitution guarantees due process and protection against arbitrary interception, which poses a challenge to surveillance and collection of evidence. There is also a lack of procedural guidance that leads to judicial reluctance in analyzing the admissibility of evidence gathered via electronic communications (Khan and Mahmood, 2022). International practices provide solid foundations of privacy versus prosecution, such as encrypted boundaries of interception, the supervision, and the authorization of judiciary (Goodison et al., 2015; Wall, 2017). Similar measures in Pakistan would allow the police to gather evidence effectively without violating the constitution and its rights.

Digital Evidence Laws Effectiveness

The findings indicate that the legislative advancement can never assure effective prosecution on its own despite the existence of digital evidence laws. Procedural anomalies, the lack of forensic infrastructure, the deficiency of judicial competencies, and a lack of international cooperation limit the effectiveness of PECA 2016 and its other statutes (Hameed et al., 2021; Nazir et al., 2025). The experience of some of the most effective cybercrime systems in the world shows that a legislative foundation should be supported by institutional capability, procedural transparency, and technical expertise to deliver significant prosecutorial results (Casey and Ferraro, 2021; Gercke, 2012).

To conclude, the research paper establishes that Pakistan has achieved a lot in formulating laws against cybercrime, but various issues still hinder successful prosecution. Some of these challenges are judicial reluctance, gaps in the process, technological deficiencies, training and international collaboration. These issues can be resolved by extensive reforms of law, institutional capacity, forensic standard and training

programs, which will increase the practical usefulness of digital evidence, enhance prosecution procedures, and increase cybersecurity governance in Pakistan.

CONCLUSIONS AND RECOMMENDATIONS

Even though Pakistan has achieved a significant advancement in the field of combating cybercrime with the Prevention of Electronic Crimes Act (PECA) 2016 and other relevant laws, major obstacles still exist in the way of practical application of legislation on the use of digital evidence. Delays in the judiciary, a lack of clarity in the process, institutional constraints, technological failures, and lack of cooperation between countries collectively deter prosecutes against cybercriminals. The lack of standardized procedures in forensics work, insufficient training and lack of technical understanding often make courts question the authenticity, integrity as well as admissibility of electronic evidence. Moreover, legal uncertainties and insufficient procedures direction enable cyber criminals to take advantage of loopholes hence diminishing the deterrent power of the current laws. The rising number of cybercrimes such as financial fraud, child exploitation, and identity thefts brings forth the need to ensure that these gaps are dealt with in order to secure individuals, businesses, and the society at large.

This study brings about a number of recommendations that can be used to improve the efficacy of the laws governing digital evidences in Pakistan. One, the law enforcers and judges ought to receive relentless technical training in digital forensics, to enhance their ability to assess electronic evidence. Second, forensic laboratories and investigative agencies should embrace internationally accepted and forensically acceptable procedures that will guarantee evidence authenticity and reliability such as proper documentation, metadata integrity, and chain-of-custody. Third, the legal reforms must make clear about some confusing terms and provide extensive standards of procedure in gathering, storing, and presenting evidence that can help to minimize the loopholes in interpretation. Fourth, Pakistan is to be active in the international cooperation systems including mutual legal assistance treaties to ease international tracking and prosecution of computer crimes. Lastly, there will be the need to balance privacy rights and investigative needs; strong controls and policies on how to use electronic surveillance will ensure constitutional protections against the violations of the law and the subsequent investigation. Such recommendations put in place in organized fashion will support the cybercrime prosecution system of Pakistan, increase trust of people with digital security, and make the nation up-to-date with the international standards in cyber law and digital forensics.

REFERENCES

Ahmed, D. G. (2021). *Digital evidence and the administration of criminal justice*. Blackstone School of Law & Business.

Ahmed, F., Qazi, M. U., & Ahmad, R. (2023). Institutional and procedural challenges in digital crime investigation. *Journal of Cybercrime Studies*.

Ahmed, S., & Qazi, M. (2019). Admissibility of electronic evidence in Pakistan: Legal and practical issues. *Pakistan Journal of Law and Technology*, 7(2), 45–59.

Baig, K., Sajjad, M. H., Zafar, M. H., & Mirza, F. K. (2025). Legal and ethical implications of forensic evidence in Pakistan. *Critical Review of Social Sciences Studies*.

Baloch, M. (2016). Cybercrime legislation and prosecutorial challenges in Pakistan. *Journal of Law and Technology*, 3(1), 25–39.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2018). Cybercrime in Asia: Trends and challenges. *Asian Journal of Criminology*, 13(1), 1–17.

Brenner, S. W. (2013). Cybercrime: The need to harmonize national penal and procedural laws. *Journal of International Law*, 15(2), 201–226.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Casey, E., & Ferraro, M. (2021). Enhancing digital evidence in criminal proceedings: Forensic practices and legal standards. *Forensic Science International*, 319, 110686.

Fafinski, S. (2008). *Cybercrime and the law: Challenges, issues, and responses*. Palgrave Macmillan.

Gercke, M. (2012). *Understanding cybercrime: A guide for developing countries*. ITU Publications.

Gogolin, G., & Jones, A. (2010). Judicial capacity and technology: Challenges in evaluating digital evidence. *International Journal of Evidence & Proof*, 14(3), 145–162.

Gul, S., Ahmad, F., & Ahmad, R. (2025). Digital evidence and procedural fairness: Reforming cybercrime prosecution in Pakistan. *Journal for Social Science Archives*, 3(2), 544–554.

Hameed, U., Qaiser, Z., & Qaiser, K. (2021). Admissibility of digital evidence: A perspective of the Pakistani justice system. *Pakistan Social Sciences Review*, 5(1), 78–95.

INTERPOL. (2017). *Cybercrime legislation and international cooperation: A global perspective*. INTERPOL Publications.

Khan, U. (2017). Challenges in prosecuting cybercrime under PECA 2016. *Pakistan Law Journal*, 6(2), 33–50.

Khan, U., & Mahmood, A. (2022). Balancing constitutional rights and cybercrime investigation in Pakistan. *Journal of Constitutional Law*, 14(1), 101–120.

Kerr, O. S. (2015). Digital evidence and the new criminal procedure. *Harvard Journal of Law & Technology*, 28(2), 1–49.

Kundi, G., Nawaz, A., & Akhtar, R. (2014). Digital revolution, cybercrimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications*, 4(4), 61–71.

Losavio, M., Choo, K. K. R., & Smith, R. G. (2006). Cybercrime and digital evidence: Emerging trends and challenges. *Australian & New Zealand Journal of Criminology*, 39(3), 310–328.

Lohiya, R., & John, M. (2015). Digital forensics in developing nations: Capacity gaps and legal issues. *Journal of Digital Investigation*, 12(3), 101–110.

Lunker, J. (2010). Jurisdictional challenges in cybercrime prosecution. *Computer Law & Security Review*, 26(5), 456–465.

Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cybercrime investigation. *Digital Investigation*, 9(2), 71–80.

McKemmish, R. (2008). *Digital evidence: An introduction and guide for forensic investigators*. Charles Sturt University Press.

Mehmood, S. (2017). Digital evidence and the criminal justice system in Pakistan. *Legal Perspectives Journal*, 3(1), 55–68.

Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to digital forensic evidence collection and presentation*. Springer.

Nazir, S., Asif, M., & Khan, A. U. (2025). Digital evidence in Pakistan: A doctrinal assessment of admissibility and reliability in criminal trials. *Advance Social Science Archive Journal*, 4(01), 1941–1951.

Riadi, A., et al. (2017). Digital forensics in emerging economies: Challenges and opportunities. *International Journal of Cyber Criminology*, 11(1), 45–60.

Rashid, A., & Ali, S. (2021). Digital forensics capacity in Pakistan: Challenges and prospects. *Journal of Digital Investigation*, 18(4), 275–288.

Rehman, T. (2020). Constitutional safeguards and cybercrime evidence: Rights and procedures. *Constitutional Law Review*, 12(2), 88–105.

Ryan, J., & Shpantzer, D. (2017). Procedural fairness and electronic evidence in criminal trials. *Journal of Digital Forensics, Security and Law*, 12(1), 1–18.

Saeed, A., Abro, L., & Dastagir, G. (2022). Approach of Pakistani courts regarding admissibility of modern devices or techniques in evidence. *Pakistan Journal of International Affairs*.

Sajid, M., & Bhatti, S. H. (2024). Digital evidence and the Pakistani criminal justice system: A review article. *Journal of Social Sciences Review*.

Shah, M. (2018). Judicial interpretation of electronic evidence in Pakistan. *Legal Studies Quarterly*, 5(3), 33–50.

Singleton, C. (2013). Cybercrime and its prosecution: Evidence, challenges, and deterrence. *International Journal of Law, Crime and Justice*, 41(3), 187–201.

Usman, M., & Ahmad, M. (2025). Judicial capacity and digital evidence evaluation in Pakistani courts. *Law & Technology Journal*, 6(1), 15–29.

Zafar, R., & Raza, M. (2020). Challenges in prosecuting cybercrime under PECA 2016. *Journal of Cyber Law*, 3(2), 55–69.

Zahid, M. A., Muhammad, A., Khan Khakwani, M. A. K., & Maqbool, M. A. (2024). Cybercrime and criminal law in Pakistan: Legislative responses and societal impact. *Pakistan Journal of Criminal Justice*.

Zahoor, R., Waqar Khan Arif, S. M., & Bannian, B. (2022). Digital evidence and its admissibility under Pakistani law. *Journal of Development and Social Sciences*, 3(4), 51–60.