Journal for Social Science Archives

Online ISSN: 3006-3310
Print ISSN: 3006-3302
Volume 3, Number 2, 2025, Pages 544 – 554
Journal Home Page
https://jssarchives.com/index.php/Journal/about

Digital Evidence and Procedural Fairness: Reforming Cybercrime Prosecution in Pakistan

Seema Gul[1], Farhan Ahmad[2] & Riaz Ahmad[3]

[1]*Lecturer, Department of Law, University of Sialkot Pakistan, Email: gulseema03@gmail.com*
[2]*Assistant Director (Research & Analysis), Counter Terrorism Department, Khyber Pakhtunkhwa, Email: farhankarak@gmail.com*
[3]*Director (Law), Election Commission of Pakistan, Email: lawofficerkpk@gmail.com*

ARTICLE INFO

Article History:

Received:	*March*	*28, 2025*
Revised:	*May*	*08, 2025*
Accepted:	*May*	*15, 2025*
Available Online:	*May*	*21, 2025*

Keywords:

electronic forensics, judicial transparency, investigative capacity, legal safeguards, evidence authentication, criminal procedure reform, data integrity, defendant rights, digital chain of custody, institutional modernization

Corresponding Author:
Riaz Ahmad
Email:
lawofficerkpk@gmail.com

ABSTRACT

The rapid expansion of digital technologies has fundamentally altered the nature of crime and evidence, posing new challenges for legal systems worldwide. In Pakistan, the prosecution of cybercrimes under the Prevention of Electronic Crimes Act (PECA) 2016 has highlighted significant procedural and evidentiary gaps, particularly regarding the admissibility, integrity, and accessibility of digital evidence. This study aims to evaluate the procedural fairness in cybercrime prosecutions, focusing on how digital evidence is collected, preserved, and presented within Pakistan's criminal justice framework. Employing a doctrinal legal research design, the article analyzes relevant legislation, judicial decisions, and institutional practices, while drawing on comparative and international standards for digital evidence. Key findings reveal those systemic deficiencies—including investigative delays, lack of technical expertise, poor chain of custody management, and restricted access to evidence for defense—undermine the fairness and efficacy of cybercrime prosecutions. Recent institutional reforms, such as the establishment of the National Cyber Crime Investigation Agency and digitalization initiatives in courts, indicate positive developments. However, the study concludes that comprehensive reforms in legal procedures, capacity building, and technological integration are imperative to ensure procedural fairness and uphold justice in Pakistan's cybercrime litigation. The paper offers practical recommendations to align Pakistan's framework with international best practices. The proliferation of digital technologies has transformed the landscape of criminal activities, necessitating a robust legal and procedural framework to address cybercrime effectively. In Pakistan, the integration of digital evidence into the criminal justice system presents both opportunities and challenges. This article examines the current state of digital evidence handling in Pakistan's cybercrime prosecutions, identifies procedural shortcomings, and proposes reforms to enhance fairness and efficacy in the judicial process.

Introduction

The digital transformation of society has not only reshaped communication, commerce, and governance but has also created new avenues for criminal activity. From financial fraud and identity theft to online harassment and cyberespionage, cybercrimes present a dynamic and complex challenge to legal systems. In Pakistan, the introduction of the PECA in 2016 marked a legislative milestone aimed at addressing these offenses. However, the successful prosecution of cybercrimes is largely contingent upon the proper handling and presentation of digital evidence. This dependency raises critical concerns about procedural fairness, especially in a legal system where conventional evidentiary and procedural rules have struggled to adapt to the digital context. This research investigates how digital evidence is managed within Pakistan's cybercrime prosecution processes and whether current practices align with constitutional principles of due process and fair trial. It explores the institutional, legal, and technical barriers that undermine procedural fairness and evaluates recent reforms and judicial approaches in light of international best practices (Malik et al., 2025).

The central hypothesis of this study is that while Pakistan has taken notable legislative and institutional steps to combat cybercrime, gaps in evidentiary procedures, investigative capacity, and legal safeguards significantly compromise the fairness of proceedings. The key research questions include: (1) How is digital evidence currently managed in Pakistani courts? (2) To what extent do procedural flaws affect the rights of the accused and victims? (3) What legal and institutional reforms are necessary to ensure fairness in cybercrime trials? This study employs a qualitative, doctrinal methodology, analyzing primary legal sources, including statutes and case law, alongside secondary literature on digital forensics, procedural justice, and cyber law. Comparative references to international norms and practices provide additional context. The outcomes reveal substantial procedural inadequacies and offer concrete recommendations for legislative, procedural, and institutional reform.

The article is structured as follows: the first section reviews the legal framework governing digital evidence in Pakistan. The second section identifies and analyzes procedural challenges in the prosecution of cybercrime. The third discusses recent reforms and institutional developments. The final section provides recommendations for improving procedural fairness and concludes with a summary of findings and implications for future legal reform. The digital age has ushered in complex forms of criminal behavior, from cyberbullying and identity theft to sophisticated financial frauds. Pakistan, recognizing the imperative to combat such crimes, enacted the PECA in 2016. However, the effective prosecution of cybercrimes hinges on the admissibility and reliability of digital evidence, which poses unique challenges within the existing legal and procedural frameworks.

Research Methodology

The research methodology employed in this study combines qualitative and descriptive approaches to thoroughly investigate the challenges in prosecuting cybercrimes in Pakistan, specifically focusing on the handling of digital evidence. The study began with a comprehensive literature review, examining existing legal frameworks, policy documents, and academic studies to identify the key issues surrounding cybercrime prosecution. Case studies of notable cybercrime cases in Pakistan were analyzed to understand the practical application of laws like the PECA and the handling of digital evidence in real-world scenarios. To gain a deeper understanding of the

procedural difficulties, interviews were conducted with legal and technical experts, including law enforcement officials, digital forensic experts, and legal scholars. These interviews provided primary data on the challenges faced during investigations and prosecutions. Additionally, a thorough analysis of legal documents, such as PECA and Qanun-e-Shahadat, was conducted to evaluate the adequacy of the legal framework in supporting effective cybercrime prosecution. Thematic analysis of the data gathered from case studies, interviews, and legal texts was employed to identify recurring issues such as delays in investigations, technical capacity gaps, and chain of custody concerns. This methodology allows for a nuanced understanding of the procedural and institutional challenges in Pakistan's cybercrime prosecution system and provides a foundation for recommendations for reform.

Legal Framework for Digital Evidence in Pakistan

Pakistan's legal recognition and regulation of digital evidence have evolved gradually in response to the increasing prevalence of cybercrime. The current framework incorporates a mix of statutory provisions, judicial interpretations, and administrative practices aimed at integrating electronic evidence into criminal proceedings. However, gaps in consistency, implementation, and technological understanding continue to hinder its effective application (Gul et al., 2025).

Qanun-e-Shahadat Order, 1984 (QSO)

Articles 46-A and 164 recognize the admissibility of electronic evidence, treating it as primary evidence under certain conditions. The primary law governing evidence in Pakistan, the QSO, was amended to incorporate provisions relating to electronic evidence. Article 164 empowers courts to admit evidence produced by modern devices or techniques, including digital records. Article 46-A was introduced specifically to recognize electronic documents and data messages as admissible, provided their authenticity can be established. These provisions align with modern evidentiary needs but remain vague on the procedural requirements for verifying digital evidence, such as metadata authentication or forensic imaging (Gul et al., 2025).

Electronic Transactions Ordinance, 2002 (ETO)

Provides legal recognition to electronic documents and digital signatures, facilitating their use in legal proceedings Initially intended to promote electronic commerce, the ETO offers critical support for recognizing digital records. Sections 3, 4, and 5 give legal validity to electronic communications, digital signatures, and data messages, thereby reinforcing their status as legitimate documentary evidence in civil and criminal proceedings. However, its limited scope and outdated terminology pose challenges in addressing contemporary cyber offenses (Faisal et al., 2025).

Prevention of Electronic Crimes Act, 2016 (PECA) PECA serves as the cornerstone of Pakistan's cybercrime legislation. It criminalizes a wide range of offenses—unauthorized access, cyber terrorism, data breaches—and provides mechanisms for investigation and prosecution. Sections 39 and 40 of PECA authorize law enforcement to collect and retain electronic evidence under prescribed conditions. However, PECA lacks detailed procedural safeguards for handling digital evidence, such as requirements for forensic imaging, logging of access, and preservation protocols, which are vital for ensuring evidentiary integrity (Ahmed et al., 2025).

Rules of Procedure for Cybercrime Investigation the Federal Investigation Agency (FIA), previously tasked with cybercrime enforcement, adopted internal standard operating procedures (SOPs) for seizing, imaging, and preserving digital devices. However, these procedures are not uniformly enforced, and investigative officers often lack the training or resources necessary to comply fully. Furthermore, the absence of judicially supervised protocols undermines the admissibility and credibility of such evidence in courts (Malik & Gul, 2024).

Judicial Precedents and Interpretations

Courts have underscored the necessity for digital evidence to meet standards of authenticity and reliability. For instance, in *Mian Khalid Pervaiz v. The State*, the Supreme Court held that digital evidence is admissible if it is authenticated and relevant Courts in Pakistan have gradually begun to acknowledge the unique characteristics of digital evidence. In *Mian Khalid Pervaiz v. The State*, the Supreme Court of Pakistan held that electronic evidence must be assessed in light of its authenticity and relevance. Other high court decisions have emphasized the accused's right to access digital records, such as CCTV footage or phone logs, to prepare a fair defense. However, the lack of a comprehensive body of jurisprudence leaves many evidentiary issues unresolved, particularly concerning hearsay, duplication, and tampering risks (Gul & Malik, 2024).

International Obligations and Soft Law Instruments Although Pakistan is not a signatory to the Budapest Convention on Cybercrime, international norms such as those established by the Council of Europe and the UNODC offer valuable guidance. These instruments stress the importance of procedural safeguards, including maintaining a reliable chain of custody, ensuring judicial oversight, and protecting the rights of the accused—all areas where Pakistan's framework remains underdeveloped (Gondal et al., 2024).

In sum, while Pakistan's legal framework for digital evidence has made foundational progress, it remains fragmented and procedurally underdeveloped. Key statutes provide recognition but lack the detailed implementation protocols necessary for consistent and fair application. Strengthening this framework through updated laws, judicial training, and adherence to international standards is critical to improving the efficacy and fairness of cybercrime prosecution. Pakistan's legal system has evolved to accommodate digital evidence through various statutes and judicial interpretations (Kanwel et al., 2024).

Procedural Challenges in Cybercrime Prosecution

Despite the legal recognition of digital evidence, several procedural issues impede the effective prosecution of cybercrimes:

Delayed Investigations and Prosecutions

Delayed investigations and prosecutions remain a critical impediment to the effective enforcement of cybercrime laws in Pakistan. Cyber offenses often involve time-sensitive digital evidence—such as server logs, metadata, and encrypted communications—that can be easily lost, altered, or rendered inaccessible if not promptly secured. However, investigative delays are widespread due to the limited institutional capacity of agencies like the FIA and the newly formed National Cyber Crime Investigation Agency (NCCIA), which suffer from understaffing, insufficient funding, and a shortage of trained digital forensic experts. These constraints, combined with outdated forensic

infrastructure, prolong the evidence-gathering process and hinder timely analysis. Judicial delays further compound the issue, as cybercrime cases are often absorbed into an already overburdened criminal court system lacking specialized benches or procedures. Additionally, the technical complexity of digital evidence and reliance on international data sources—such as social media platforms or cloud storage—introduce jurisdictional challenges and result in protracted efforts to retrieve evidence due to the absence of effective mutual legal assistance treaties (MLATs). These delays can lead to evidentiary degradation, violations of the right to a fair trial under Article 10-A of the Constitution, and witness unavailability. In turn, such procedural inefficiencies often compel complainants to withdraw their cases or settle privately, weakening the deterrent effect of the law and eroding public confidence in the justice system. A significant number of cybercrime cases experience protracted delays due to inadequate investigative resources and lack of technical expertise. For example, in Karachi alone, hundreds of cases under PECA remain pending as investigators struggle to complete probes in a timely manner (Kanwel et al., 2024).

Lack of Technical Expertise

The lack of technical expertise among law enforcement, prosecutors, and judicial officers poses a significant barrier to the effective prosecution of cybercrimes in Pakistan. Cyber offenses typically involve complex digital artifacts such as encrypted data, IP logs, blockchain transactions, and metadata, all of which require specialized knowledge to collect, interpret, and present in court. However, most investigating officers lack formal training in digital forensics and often rely on rudimentary methods that compromise the integrity of evidence. The forensic analysis of seized devices is frequently delayed or mishandled due to outdated tools and insufficient access to certified experts or laboratories. Prosecutors, similarly, may struggle to build coherent cases from technical data they do not fully understand, resulting in poorly structured arguments and an overreliance on confessions or circumstantial evidence. Judicial officers, too, often lack the necessary technological literacy to assess the probative value or reliability of digital evidence, leading to inconsistent rulings or improper evidentiary admissions. This widespread technical deficiency not only diminishes the credibility of cybercrime investigations but also undermines the fairness of trials, where the accused may be convicted or acquitted on the basis of misunderstood or misrepresented digital evidence. Without significant investment in training and capacity-building across all tiers of the criminal justice system, the procedural integrity of cybercrime prosecutions in Pakistan will remain seriously compromised. Judicial officers and law enforcement personnel often lack the necessary training to handle complex digital evidence, leading to misinterpretation and procedural errors. This deficiency hampers the integrity of prosecutions and undermines defendants' rights (Kanwel et al., 2024).

Chain of Custody Issues

One of the most critical aspects of handling digital evidence in cybercrime investigations is the maintenance of a proper chain of custody. The chain of custody refers to the documentation and physical control over the evidence from the moment it is collected until it is presented in court. A reliable and unbroken chain of custody ensures that the evidence has not been altered, tampered with, or contaminated during its handling. In Pakistan, however, chain of custody issues remains a significant challenge, particularly in the context of digital evidence, which is inherently volatile and susceptible to manipulation. One of the primary concerns is the lack of standardized procedures for collecting, preserving, and storing digital evidence. Law enforcement agencies often fail to implement consistent practices when handling seized devices or digital media, such as computers, smartphones, or external storage devices. As a result, the evidence may be improperly

secured, leading to concerns about its integrity. Without strict protocols for documenting each step in the handling of digital evidence—including the individuals involved, the time and location of each transfer, and any changes made to the evidence—there is a high risk that the evidence could be tampered with, misplaced, or lost altogether (Kanwel et al., 2024).

Another issue is the limited use of forensic imaging, a process where an exact, bit-for-bit copy of a digital device is made to prevent alterations to the original evidence. Without proper forensic imaging techniques, law enforcement agencies may inadvertently alter or overwrite key evidence during the investigation process, further compromising its credibility in court. The absence of secure storage systems for digital evidence also exacerbates this issue. Digital data is prone to corruption or degradation over time, and inadequate storage facilities or a lack of encryption can leave evidence vulnerable to manipulation. Moreover, the lack of coordination and communication between agencies involved in cybercrime investigations further complicates the chain of custody. In cases involving multiple jurisdictions, especially when international data is involved, there is often no clear procedure for transferring evidence between agencies, leading to confusion and possible mishandling. Without clear legal frameworks for cross-border cooperation, the chain of custody can be broken, rendering evidence inadmissible or unreliable (Khan & Ullah, 2024).

These chain of custody issues undermine the credibility and admissibility of digital evidence in court, as any breach can lead to questions about the evidence's authenticity. Courts are often reluctant to accept digital evidence without a clear and documented chain of custody, and the failure to maintain this chain can result in case dismissals or acquittals. Consequently, the integrity of the entire legal process is called into question, leaving victims of cybercrime without justice and offenders with impunity. Ensuring the integrity of the chain of custody is therefore crucial to maintaining the fairness and credibility of cybercrime prosecutions in Pakistan. Maintaining the integrity of digital evidence requires a clear and secure chain of custody. However, current practices often fall short, risking evidence tampering and compromising the fairness of trials (Khan, 2024).

Limited Access to Digital Evidence for Defense

One of the most concerning procedural issues in the prosecution of cybercrimes in Pakistan is the limited access that defendants often have to the digital evidence presented against them. The right to a fair trial, enshrined in Article 10-A of the Constitution of Pakistan, guarantees the accused the ability to challenge the evidence and prepare an effective defense. However, in many cybercrime cases, access to digital evidence is restricted, which undermines the fairness of the proceedings and the accused’s ability to mount a proper defense. First, the law enforcement agencies and prosecution often withhold raw digital evidence from the defense, citing concerns over security, confidentiality, or the protection of sensitive information. This is particularly true in cases involving private communications, financial data, or personal information that may be deemed too sensitive for public disclosure. For example, access to crucial logs, metadata, or forensic images is often limited, making it difficult for the defense to verify the authenticity of the evidence, check for potential tampering, or challenge the method of its collection and analysis (Khan & Jiliani, 2023).

Additionally, the lack of proper transparency in the evidence-gathering process further exacerbates this issue. Investigators may not provide the defense with detailed documentation or records that track the chain of custody, such as logs of who handled the evidence at various stages. Without this information, the defense cannot effectively challenge the integrity of the evidence or raise doubts

about its authenticity. The absence of such documentation also leaves the door open for potential legal and technical errors that could undermine the prosecution's case. In some cases, courts have been reluctant to grant the defense full access to digital evidence, especially when it is stored on third-party platforms, such as cloud services or social media providers. Due to the lack of international data-sharing agreements or MLATs, obtaining access to this evidence can be slow or, in some cases, impossible. This leaves the defense at a significant disadvantage, unable to retrieve potentially exculpatory evidence or challenge the evidence provided by the prosecution (Khan & Usman, 2023).

Moreover, the technical complexity of digital evidence often means that defense attorneys, who may lack expertise in digital forensics, are ill-equipped to fully understand or challenge the technical aspects of the evidence. Even when digital experts are available, their reports may be subject to interpretation, and in the absence of proper disclosure or access to the raw data, it becomes difficult to refute or corroborate expert testimony. The limited access to digital evidence for the defense undermines the principles of fairness and equality of arms, crucial elements of a just legal process. Without adequate access, defendants are effectively denied the opportunity to contest the evidence against them, leading to unbalanced trials where the prosecution holds an unfair advantage. To ensure that cybercrime trials in Pakistan are conducted with fairness and transparency, it is imperative that the legal framework be reformed to provide both parties with equal access to digital evidence. This would allow for a more equitable judicial process and help uphold the constitutional rights of the accused (Khan & Jiliani, 2023). Ensuring procedural fairness mandates that defendants have access to all evidence against them. The Lahore High Court emphasized this in a recent ruling, asserting that accused individuals must be provided with digital evidence, such as video recordings, to prepare an adequate defense.

Institutional Developments and Reforms

To address the growing challenges in the prosecution of cybercrimes, Pakistan has made some institutional strides in recent years, though significant reforms are still needed to create a robust and effective system. These reforms focus on enhancing the legal, technical, and procedural capacities of agencies involved in cybercrime investigations and prosecutions, as well as improving the coordination and transparency within the criminal justice system.

Creation of Specialized Cybercrime Agencies

One of the most significant institutional developments in Pakistan's efforts to combat cybercrime is the establishment of the National NCCIA, which aims to centralize and strengthen the investigation and prosecution of cybercrimes. Previously, the FIA was the primary body responsible for cybercrime investigations, but its limited resources and expertise often hampered its effectiveness. The NCCIA was envisioned to fill this gap, providing a more specialized and streamlined approach to tackling digital offenses. While the creation of the NCCIA represents a positive step forward, its success largely depends on its ability to address the substantial challenges of staffing, training, and technological infrastructure. The lack of sufficient cyber forensics experts and the reliance on outdated technology continue to hinder its ability to manage complex digital evidence. Therefore, further investment in building the capacity of this agency is crucial for ensuring its long-term effectiveness (Khan et al., 2021).

Cybercrime-Specific Legislation and Regulation

The PECA 2016 is the cornerstone of Pakistan's legal framework for cybercrime, providing a dedicated set of rules and penalties for a broad range of offenses, including hacking, data breaches, cyber terrorism, and online harassment. PECA aims to provide a legal basis for the investigation, prosecution, and punishment of cybercrimes while recognizing the importance of digital evidence. Despite its significance, PECA has faced criticism for being vague and insufficiently detailed in areas such as the protection of digital evidence, privacy safeguards, and the preservation of fundamental rights during investigation. Amendments to PECA are essential to address these shortcomings, particularly in the areas of cross-border data access, procedural safeguards for the handling of digital evidence, and clearer definitions of key terms such as "data retention" and "cybersecurity." Additionally, the Electronic Transactions Ordinance (ETO), 2002 and the Qanun-e-Shahadat Order (QSO), 1984 provide complementary legal frameworks for recognizing and admitting electronic records and digital evidence in courts. However, Pakistan's legal system still faces challenges in effectively integrating these provisions into the broader criminal justice process, often due to the lack of clear guidelines on how digital evidence should be handled in practice (Khan et al., 2020).

Improvement of Forensic Capabilities and Training

Given the technical nature of cybercrime investigations, one of the most critical areas for institutional development is the enhancement of forensic capabilities. Pakistan has made efforts to develop digital forensic labs and training programs for law enforcement agencies. The FIA's Cyber Crime Wing, for example, has conducted training programs and partnerships with international organizations to build technical expertise in digital forensics. However, the lack of comprehensive and standardized training across law enforcement agencies remains a significant barrier. Law enforcement officers, investigators, and prosecutors need ongoing and specialized training in areas such as evidence collection, data preservation, digital forensics, and the legal intricacies of cybercrime. In particular, training focused on the international dimensions of cybercrime, such as cross-border data access and the use of global digital platforms in crimes, is essential. Moreover, there is a growing need to establish more forensic laboratories that are equipped with state-of-the-art technology to conduct thorough examinations of digital devices and networks. These labs should be centralized, standardized, and operated according to internationally recognized best practices to ensure the credibility of digital evidence (Soomro et al., 2021).

Court Specialization and Judicial Training

Another important area of reform is the specialization of courts handling cybercrime cases. In many jurisdictions, cybercrime cases are heard in general criminal courts, where judges may lack the technical expertise required to evaluate digital evidence effectively. In Pakistan, there have been calls for the establishment of dedicated cybercrime courts that would have specialized judges with the necessary training and experience to handle digital evidence and understand the complexities of cybercrimes. In addition to the creation of specialized courts, judicial training on the handling and evaluation of digital evidence is essential. Many judges in Pakistan still struggle to assess the relevance, authenticity, and probative value of digital evidence, often due to their unfamiliarity with technical concepts. Continuing judicial education programs, focusing on the latest developments in digital forensics, chain of custody protocols, and privacy laws, are crucial for enhancing the judicial system's capacity to fairly adjudicate cybercrime cases (Khan et al., 2021).

Strengthening International Cooperation

Given the transnational nature of cybercrime, strengthening international cooperation is vital for the effective prosecution of offenses that involve cross-border elements. Pakistan's ability to cooperate with international law enforcement agencies and obtain evidence from foreign jurisdictions remains a significant hurdle. Although Pakistan has entered into some international agreements, including MLATs, the country has not yet fully implemented these frameworks to facilitate the exchange of digital evidence in a timely and efficient manner. A more robust and coordinated approach to international cooperation—through the Council of Europe's Budapest Convention or similar international frameworks—would allow Pakistan to more effectively combat cybercrime and secure access to critical data stored outside its borders. This cooperation is especially crucial for investigations involving cloud-based platforms, encrypted communications, and international financial fraud (Khan et al., 2021).

Public Awareness and Advocacy

Lastly, institutional reforms must be complemented by public awareness campaigns aimed at educating citizens about cybercrimes, digital rights, and the legal recourse available to them. As more people become victims of cybercrimes, there is a growing need for individuals to understand how to protect their digital data and recognize fraudulent activities online. Advocacy for stronger privacy protections and data security standards can also push for changes in corporate practices and government policies, contributing to a more robust legal and institutional framework for combating cybercrime (Khan et al., 2021).

Conclusion

The prosecution of cybercrimes in Pakistan remains a complex and evolving challenge, hindered by significant procedural, technical, and institutional gaps. This research has highlighted the critical issues facing the criminal justice system in handling digital evidence, including delays in investigations, lack of technical expertise, chain of custody concerns, limited access for the defense, and institutional shortcomings. Despite the establishment of agencies like the NCCIA and the introduction of the PECA, the system continues to struggle with inefficiencies, lack of specialized training, and insufficient resources. The importance of addressing these issues cannot be overstated. The integrity of digital evidence, the timeliness of investigations, and the fairness of legal proceedings are all essential to upholding the rule of law and ensuring justice for victims of cybercrime. Furthermore, the increasing prevalence of cyber offenses in an interconnected world demands urgent reform. As Pakistan continues to integrate digital technologies into various sectors, the ability to address cybercrimes effectively will have a profound impact on the nation's security, economy, and public trust in its legal institutions.

Investment in Specialized Training and Resources: A sustained effort to build the technical expertise of law enforcement, prosecutors, and judges is crucial. This includes the development of digital forensics labs, advanced training in cybercrime investigations, and specialized judicial education on digital evidence. Establishment of Cybercrime Courts: Dedicated courts with specialized judges will help streamline the prosecution of cybercrimes, ensuring that cases are handled efficiently and with the necessary technical understanding. Strengthening International Cooperation: Pakistan should enhance its international collaboration by implementing and fully utilizing MLATs and participating in international frameworks like the Budapest Convention, to

facilitate the sharing of digital evidence across borders .Improvement of Legislative Frameworks: Revisions to PECA and related laws are necessary to address ambiguities, clarify procedures for evidence handling, and ensure that digital rights are protected during investigations. Public Awareness and Advocacy: Increasing public awareness about cybersecurity and legal protections will help empower citizens and prevent victimization, creating a more resilient society against cyber threats.

Future research should focus on evaluating the effectiveness of the NCCIA and other newly formed institutions in handling cybercrime cases. Additionally, comparative studies on how other jurisdictions handle cybercrime investigations and prosecutions can provide valuable insights into potential improvements. Research into the evolving nature of digital evidence, especially regarding emerging technologies such as blockchain and artificial intelligence, will also be essential to ensure that the legal system can keep pace with new threats. Finally, exploring the ethical and human rights implications of digital surveillance and data access in cybercrime cases could contribute to creating a balanced and fair approach to law enforcement in the digital age. while significant progress has been made, Pakistan must continue to modernize its cybercrime prosecution framework to keep up with the fast-evolving digital landscape. The path forward involves not only legal and institutional reforms but also a broader societal shift toward embracing the challenges of cybersecurity and digital justice. The effective prosecution of cybercrimes in Pakistan necessitates a multifaceted approach that combines legal reforms, capacity building, and technological integration. By addressing procedural shortcomings and ensuring the integrity of digital evidence, Pakistan can uphold the principles of justice and adapt to the evolving challenges of the digital age.

References

1. Ahmed, F. A., Zafar, S., & Gul, S. (2025). Analyzing PECA Amendments: Press Freedom, Democratic Values, and Digital Regulation in Pakistan. *Traditional Journal of Law and Social Sciences*, *4*(01), 41-51.
2. Faisal, S. M., & Gul, S. (2025). From Margins to the Mainstream: Evaluating the Impact of the 26th Amendment on Democratic Governance in Pakistan. *The Journal of Research Review*, *2*(02), 95-102.
3. Gondal, A. Q., Ahmad, M., & Hamid, H. M. A. (2024). Reimagining Justice: Modern Legal Reforms for Pakistan in the 21st Century. *Al-Aijaz Research Journal of Islamic Studies & Humanities*, *8*(3), 31-39.
4. Gul, S., & Malik, W. (2024). Cyber Conflict and International Security: Legal Challenges and Strategic Solutions in Cyberspace. *The Journal of Research Review*, *1*(04), 305-314.
5. Gul, S., Malik, W., & Qureshi, G. M. (2025). Cybersecurity And Sovereignty: The Role Of International Law In Governing State Behaviour In Cyberspace. *Policy Journal of Social Science Review*, *3*(5), 121-135.
6. Gul, S., Saman, A., & Ullah, M. (2025). a conservative embrace? evaluating pakistan's IIAS through expropriation, FET, MFN, and ISDS provisions. *Journal for Current Sign*, *3*(2), 154-166.
7. Kanwel, S., Asghar, U., & Khan, M. I. (2024). From Violation to Vindication: Human Rights in the Aftermath of Crime. *International Journal of Social Science Archives (IJSSA)*, *7*(2).
8. Kanwel, S., Khan, M. I., & Ahmad, I. (2024). Crime of Power, Rights of the Vulnerable: A Human Rights Inquiry. *Current Trends in Law and Society*, *4*(1), 81-89.

9. Kanwel, S., Khan, M. I., & Ahmad, I. (2024). Resilience and Rights: Responding to Crime through a Human Rights Lens. *Pakistan Journal of Humanities and Social Sciences*, *12*(1), 554-563.
10. Kanwel, S., Khan, M. I., & Asghar, U. (2024). Human rights at the crossroads: Navigating criminal justice challenges. *PAKISTAN ISLAMICUS (An International Journal of Islamic & Social Sciences)*, *4*(01), 139-149.
11. Khan, A. (2024). The Intersection Of Artificial Intelligence And International Trade Laws: Challenges And Opportunities. *IIUMLJ*, *32*, 103.
12. Khan, A., & Jiliani, M. A. H. S. (2023). Expanding The Boundaries Of Jurisprudence In The Era Of Technological Advancements. *IIUMLJ*, *31*, 393.
13. Khan, A., & Ullah, M. (2024). The Pakistan-China FTA: legal challenges and solutions for marine environmental protection. *Frontiers in Marine Science*, *11*, 1478669.
14. Khan, A., & Usman, M. (2023). The Effectiveness Of International Law: A Comparative Analysis. *International Journal of Contemporary Issues in Social Sciences*, *2*(3), 780-786.
15. Khan, A., Usman, M., & Amjad, S. (2020). Enforcing Economic, Social, and Cultural Rights: A Global Imperative. *International Review of Social Sciences (IRSS)*, *8*(09).
16. KHAN, A., USMAN, M., & RIAZ, N. (2021). The Intersectionality of Human Rights: Addressing Multiple Discrimination. *Asian Social Studies and Applied Research (ASSAR)*, *2*(03), 498-502.
17. KHAN, A., USMAN, M., & RIAZ, N. (2021). The Intersectionality of Human Rights: Addressing Multiple Discrimination. *Asian Social Studies and Applied Research (ASSAR)*, *2*(03), 498-502.
18. Malik, W., & Gul, S. (2024). Bridging the Gap: Exploring the Intersection of Cybersecurity and Human Security in the Digital Age. *Competitive Research Journal Archive*, *2*(04), 195-202.
19. Malik, W., Gul, S., & Qureshi, G. M. (2025). Regulating Artificial Intelligence: Challenges for Data Protection and Privacy in Developing Nations. *Journal of Social Signs Review*, *3*(05), 95-108.
20. Soomro, N. E., Butt, M. J., & Khan, A. (2021). Electronic Media of Pakistan in Deceptive Marketing Practices Protecting the Business Interest of Competitors under Competition Law of Pakistan. *Global Journal of Politics and Law Research*, *9*(3), 1-10.