Remittances Review
September 2024,
Volume: 9, No:S 4, pp.1907-1922
ISSN: 2059-6588(Print) | ISSN 2059-6596(Online)

Received : 31 August 2024, Accepted: 24 September 2024

STRENGTHENING LEGAL FRAMEWORKS TO COMBAT CYBERCRIME: A CRIMINAL JUSTICE PERSPECTIVE ON PAKISTAN'S LEGISLATIVE RESPONSE

**Amina Bari*

*Deputy Director (Legislation), Law and Parliamentary Affairs Department, Government of the Punjab, Pakistan

Correspondence Email ID: aminabari.dd@gmail.com

ABSTRACT

The exponential growth of digital technologies has transformed communication, commerce, and governance, but it has also given rise to complex forms of cybercrime that transcend national boundaries. Offenses such as hacking, identity theft, financial fraud, data breaches, cyber terrorism, and online harassment have become increasingly sophisticated, posing serious threats to individual privacy, economic stability, and national security. Pakistan, like many developing nations, faces significant challenges in effectively addressing these crimes due to legislative limitations, weak enforcement mechanisms, and inadequate institutional capacity. This study critically examines Pakistan's legal and criminal justice response to cybercrime, with a particular focus on the Prevention of Electronic Crimes Act (PECA) 2016. Using a qualitative doctrinal research approach, the study analyzes legislative texts, judicial decisions, and institutional reports to evaluate the scope, interpretation, and implementation of PECA. Comparative insights are drawn from international frameworks, including the Budapest Convention on Cybercrime and the Indian Information Technology Act (2000), to assess Pakistan's alignment with global best practices. Findings indicate that while PECA 2016 provides a foundational legal structure, it remains limited in addressing emerging threats such as artificial intelligence misuse, crypto currency fraud, and cross-border data crimes. Moreover, enforcement agencies such as the Federal Investigation Agency (FIA) Cybercrime Wing struggle with inadequate training, technical infrastructure, and coordination, while the judiciary lacks specialized expertise in digital forensics. The study concludes that effective cybercrime control in Pakistan requires legislative modernization, institutional strengthening, judicial specialization, and enhanced

international cooperation. It recommends targeted policy reforms, capacity-building programs, and public awareness initiatives to promote a safer digital ecosystem. By aligning Pakistan's cybercrime legislation with global standards, the country can ensure a more resilient, transparent, and accountable criminal justice system in the digital age.

Keywords: *Cybercrime, PECA 2016, Pakistan, criminal law, legal mechanisms, digital security, international cooperation.*

1. INTRODUCTION

In the contemporary digital age, technological advancement has transformed nearly every aspect of human interaction, from communication and commerce to governance and education. However, the same innovations that empower societies have simultaneously created vast and complex opportunities for criminal exploitation within cyberspace. Across the globe, cybercrime has evolved into one of the most pressing threats to national security, economic development, and individual privacy. In Pakistan, this challenge has become particularly severe due to the rapid digitalization of public and private sectors without corresponding legal and institutional preparedness. The increasing reliance on online systems for banking, e-commerce, and government services has expanded the attack surface for malicious actors who exploit weak cyber security frameworks and limited awareness among users (Zia ul Islam, Khan, & Zubair, 2019).

The Pakistani government recognized the growing threat of digital offenses and took legislative action through the Prevention of Electronic Crimes Act (PECA) 2016, which serves as the primary legal framework to regulate and penalize electronic crimes. The Act aims to safeguard individuals, institutions, and national data infrastructure from offenses such as hacking, identity theft, cyber stalking, defamation, and digital fraud. Despite its ambitious scope, however, PECA's enforcement has encountered significant challenges—including outdated procedural mechanisms, inadequate technical expertise, and overlapping institutional jurisdictions. These shortcomings have hindered the effective investigation, prosecution, and adjudication of cyber offenses, limiting the law's deterrent potential (Usman, 2017).

Moreover, Pakistan's cybercrime landscape exists within a broader international context, where technological borders are blurred, and crimes committed in one jurisdiction can instantly affect another. The absence of comprehensive international cooperation frameworks and limited

alignment with global conventions—such as the Budapest Convention on Cybercrime—further constrain Pakistan's ability to combat transnational digital offenses effectively. Consequently, the country faces mounting difficulties in balancing privacy rights, digital freedom, and state security within its legal system (Sharma & Alam, 2016).

This paper critically examines the strengths and weaknesses of Pakistan's legislative and institutional approach to combating cybercrime from a criminal justice perspective. It explores the existing legal mechanisms, evaluates enforcement strategies, and analyzes judicial interpretations under PECA 2016. Furthermore, it draws comparative insights from other jurisdictions to highlight best practices and identify reform priorities. Ultimately, this study seeks to determine how Pakistan's legal response can be modernized to address evolving cyber threats while upholding the principles of justice, accountability, and international cooperation (Talha Khan, 2015).

1.2. Objectives of the Study

The objectives of this study are outlined as follows:

1. To examine the effectiveness of Pakistan's existing legal framework—particularly the Prevention of Electronic Crimes Act (PECA) 2016—in addressing various forms of cybercrime.
2. To analyze the enforcement mechanisms and institutional capacity of key agencies, such as the Federal Investigation Agency (FIA) Cybercrime Wing, in investigating and prosecuting cyber offenses.
3. To compare Pakistan's legislative and judicial response to international standards, including the Budapest Convention on Cybercrime, and identify areas requiring harmonization.
4. To propose strategic recommendations for strengthening Pakistan's legal, institutional, and procedural mechanisms to enhance cybercrime prevention, investigation, and prosecution.

1.3 Research questions

1. How effective is the Prevention of Electronic Crimes Act (PECA) 2016 in addressing and preventing various forms of cybercrime in Pakistan?
2. What challenges do law enforcement and judicial institutions, particularly the FIA Cybercrime Wing, face in enforcing cybercrime laws and ensuring successful prosecution?

3. How does Pakistan's legislative and judicial framework for combating cybercrime compare with international standards such as the Budapest Convention?
4. What legal, institutional, and policy reforms can strengthen Pakistan's criminal justice system to effectively counter emerging cyber threats?

1.4 Significance of the Study

This study holds significant importance in understanding and improving Pakistan's legal and institutional response to the growing challenge of cybercrime. In an era where digital dependency is rapidly increasing, cyber threats pose grave risks to individuals, businesses, and national security. By critically examining the Prevention of Electronic Crimes Act (PECA) 2016 and related institutional mechanisms, the research provides valuable insights into the effectiveness and limitations of Pakistan's current cyber laws (Goodman & Brenner, 2002).

The findings of this study will assist policymakers in identifying legislative loopholes and developing more comprehensive cybercrime laws aligned with global standards such as the Budapest Convention. It will also help law enforcement agencies, particularly the FIA Cybercrime Wing, enhance their investigative capacity, coordination, and use of digital forensics. For the judiciary, the study offers guidance on interpreting and implementing cyber laws in line with international best practices. Moreover, academics and researchers will benefit from the comparative analysis, which contributes to the broader discourse on cyber law and digital governance in developing nations. Ultimately, this research aims to strengthen Pakistan's criminal justice framework to create a safer, more secure, and legally robust digital environment (Ingram, 2014).

2. LITERATURE REVIEW

2.1 Global Perspectives on Cybercrime and Legal Frameworks

Cybercrime has emerged as a major global security and governance concern, transcending national borders and traditional law enforcement boundaries. According to Wall (2017), cybercrime can be broadly categorized into three areas: offenses against individuals (such as identity theft and harassment), property crimes (including hacking and financial fraud), and crimes against the state (such as cyber terrorism). The global nature of these offenses

requires innovative legislative responses and multilateral cooperation. Brenner (2019) notes that traditional criminal justice systems are often ill-equipped to deal with digital evidence, anonymous offenders, and jurisdictional conflicts. International frameworks like the Budapest Convention on Cybercrime (2001) have therefore become essential models for harmonizing national laws and promoting cross-border collaboration. Countries that have adopted these frameworks have reported improved investigation procedures and legal coherence in combating digital crimes (Raza Khan, 2016).

2.2 Regional and Comparative Legal Approaches

Comparative studies reveal significant variations in the effectiveness of cybercrime laws across jurisdictions. In developed nations such as the United Kingdom, the United States, and Malaysia, regular legislative updates and digital capacity-building programs have enhanced the efficiency of cybercrime prosecution. Ahmad and Noor (2020) highlight Malaysia's Computer Crimes Act 1997 as a model of adaptability due to its periodic revisions in response to technological developments. Similarly, the UK's Computer Misuse Act 1990 has evolved through successive amendments that address hacking, malware dissemination, and online fraud. These countries emphasize continuous training of investigators, judicial digital literacy, and inter-agency collaboration—factors that Pakistan can adopt to strengthen its enforcement framework. Comparative evidence thus illustrates that cyber legislation must evolve in tandem with technology to remain effective (Kundi & Shah, 2009).

2.3 Pakistan's Legislative Framework: Progress and Challenges

In Pakistan, the enactment of the Prevention of Electronic Crimes Act (PECA) 2016 marked a landmark effort to address cyber threats within a formal legal structure. Zafar and Khalid (2021) regard PECA as a significant legislative milestone, as it defines a wide range of cyber offenses including unauthorized access, data theft, and online harassment. However, they also point out inconsistencies in implementation, lack of judicial expertise, and political interference in enforcement processes. The Federal Investigation Agency's (FIA) Cybercrime Wing—tasked with executing PECA—faces numerous operational challenges, including limited technical capacity and insufficient forensic infrastructure (Rashid & Khan, 2022). Additionally, issues such as delayed investigations, jurisdictional overlaps, and procedural ambiguities hinder

effective prosecution. Scholars argue that without strong institutional mechanisms and legal clarity, PECA remains only partially effective in curbing cyber offenses (Munir & Shabir, 2018).

2.4 Need for Legislative Modernization and International Cooperation

Recent research emphasizes that Pakistan's cyber laws must evolve to meet emerging technological realities such as artificial intelligence misuse, cryptocurrency fraud, and cross-border data theft. Hussain (2023) asserts that Pakistan's non-participation in the Budapest Convention restricts its ability to cooperate in international investigations and extraditions involving digital crime. Scholars advocate for harmonization of domestic laws with international standards to enhance mutual legal assistance and data-sharing protocols. Furthermore, capacity-building initiatives for law enforcement officers, prosecutors, and judges are deemed essential to bridge knowledge gaps. The integration of advanced digital forensics, institutional transparency, and international collaboration are repeatedly cited as key elements for reform (Naseer & Bhatti, 2022). Hence, a forward-looking and adaptive legal strategy is indispensable for strengthening Pakistan's criminal justice response to cybercrime (Mushtaque, Ahsan, Nadeem, & Umer, 2014).

3. METHODOLOGY

4.1 Research Design

This study adopts a qualitative doctrinal research approach, focusing on the systematic examination of laws, judicial interpretations, and institutional frameworks. The aim is to understand how Pakistan's legal system, particularly under the Prevention of Electronic Crimes Act (PECA) 2016, addresses cybercrime through existing legal provisions and enforcement mechanisms.

3.2 Data Sources

The research primarily utilizes primary and secondary sources. Primary sources include legislative documents, official government publications, and judicial decisions relevant to cybercrime. Secondary sources encompass academic journals, policy reviews, and expert commentaries, which provide critical insights and contextual understanding of Pakistan's cyber law enforcement environment.

3.3 Comparative Framework

To broaden the analytical scope, the study integrates comparative perspectives from international frameworks such as the Budapest Convention on Cybercrime and the Indian

Information Technology Act (2000). These comparisons help assess Pakistan's legal progress and identify best practices from jurisdictions with more mature cybercrime legislation and enforcement systems.

3.4 Analytical Procedure

The analysis centers on the textual interpretation and critical evaluation of PECA 2016, its procedural guidelines, and institutional reports. By synthesizing findings from legal documents and scholarly critiques, the study identifies existing gaps, evaluates institutional performance, and proposes evidence-based reforms aimed at aligning Pakistan's cybercrime response with international standards.

4. DATA ANALYSIS RESULTS (QUALITATIVE)

Table 1: Thematic Analysis of Pakistan's Cybercrime Legislation (PECA 2016)

Theme	Relevant Sections/Provisions (PECA 2016)	Key Findings	Identified Gaps
Definition and Scope of Cybercrime	Sections 3–10	Defines offenses like unauthorized access, data theft, and cyber terrorism.	Some emerging crimes (AI misuse, crypto fraud) remain unaddressed.
Enforcement Mechanisms	Sections 29–40	Grants FIA powers for investigation and prosecution.	Limited technical capacity and procedural delays reduce effectiveness.
Judicial Oversight	Section 44 and Rules 2018	Courts authorized to try cyber offenses.	Lack of judicial expertise in digital evidence handling.
Victim Protection and Privacy	Section 21–24	Provides remedies for online harassment and defamation.	Weak enforcement and limited awareness among victims.

Table 2: Comparative Analysis of Cybercrime Legislation (Pakistan vs. International Frameworks)

Aspect	Pakistan (PECA 2016)	Budapest Convention (2001)	Indian IT Act (2000, amended 2008)
Legal Scope	Covers cyber terrorism, data theft, and online harassment.	Provides standardized definitions and cross-border cooperation.	Focuses on hacking, fraud, and electronic signatures.
International Cooperation	Limited; not a signatory to Budapest Convention.	Enables global collaboration and evidence sharing.	Allows mutual assistance with signatory states.
Institutional Mechanisms	FIA Cybercrime Wing handles enforcement.	Encourages specialized agencies with international liaison.	Established CERT-IN for digital incident response.
Procedural Framework	Relies on court authorization and FIA guidelines.	Provides harmonized procedural standards.	Emphasizes electronic record admissibility.

Table 3: Institutional Performance and Implementation Challenges

Institution	Mandate/Role	Observed Strengths	Challenges Identified
Federal Investigation Agency (FIA) Cybercrime Wing	Investigation and enforcement of PECA 2016.	Active national presence; online complaint system.	Lack of trained personnel, limited digital forensics capacity.
Judiciary	Trial and adjudication of cybercrime cases.	Independent legal authority.	Inadequate judicial expertise and delay in case disposal.
Ministry of IT & Telecommunication	Policy formulation and digital regulation.	Promotes digital literacy and cybersecurity awareness.	Weak coordination with law enforcement agencies.
Public Awareness Initiatives	Cyber safety campaigns and reporting portals.	Growing social media awareness.	Low rural outreach and reporting hesitancy.

Table 4: Thematic Findings and Suggested Reforms

Theme	Findings from Analysis	Implications

Theme	Findings from Analysis	Implications
1. Legislative Scope and Coverage	PECA 2016 provides a foundational legal framework but does not fully address emerging digital crimes such as cryptocurrency fraud, AI-based offenses, and data brokerage.	Legislative lag leaves new forms of cybercrime unregulated and limits prosecutorial effectiveness.
2. Institutional and Investigative Capacity	The FIA Cybercrime Wing lacks adequate technical resources, digital forensics labs, and skilled investigators.	Operational inefficiency undermines enforcement and public trust.
3. Judicial Competence and Case Management	Judges and prosecutors have limited exposure to digital evidence and cyber law procedures.	Leads to delayed adjudication and inconsistent verdicts.
4. International Cooperation and Legal Harmonization	Pakistan is not a signatory to the Budapest Convention and lacks robust cross-border data-sharing protocols.	Limits international collaboration in transnational cyber investigations.
5. Public Awareness and Victim Protection	Low awareness of cyber laws and limited victim support services hinder reporting and prosecution.	Undermines deterrence and victim confidence.
6. Policy Coordination and Governance	Fragmented coordination among ministries, law enforcement agencies, and regulatory bodies.	Results in overlapping mandates and slow policy response.

5. FINDINGS AND DISCUSSION

5.1 Legislative Scope and Coverage

The analysis reveals that Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 provides a foundational framework to combat cybercrimes, yet its coverage remains limited in addressing emerging digital threats. While the Act effectively criminalizes offenses such as unauthorized access, data theft, and online harassment, it does not comprehensively address new-age crimes like cryptocurrency fraud, artificial intelligence misuse, and cross-border data breaches. Scholars including Zafar and Khalid (2021) have argued that this legislative gap leaves critical digital domains underregulated, thereby reducing the deterrence effect of the law. In contrast, countries such as Malaysia and the United Kingdom routinely update their cyber laws to reflect technological evolution. Therefore, Pakistan's cybercrime framework requires regular legislative review mechanisms and amendments to accommodate future digital realities (Kundi, Nawaz, Akhtar, & MPhil Student, 2014).

5.2 Institutional and Investigative Capacity

The Federal Investigation Agency (FIA) Cybercrime Wing is the principal enforcement body under PECA 2016. The study found that, despite its legal mandate, the agency struggles with limited technical infrastructure, shortage of trained personnel, and procedural delays in cybercrime investigation. Institutional inefficiency often results in delayed responses, weak evidence collection, and reduced conviction rates. Rashid and Khan (2022) emphasize that without adequate digital forensic laboratories and inter-agency coordination, the implementation of PECA remains inconsistent. Moreover, political and bureaucratic interference sometimes hinders independent investigations. Strengthening the FIA through capacity-building programs, improved coordination with telecom regulators, and dedicated funding is essential for effective enforcement (Sridharan, 2016).

5.3 Judicial Competence and Case Management

The judiciary's role in enforcing cybercrime laws is crucial yet underdeveloped. The study found that judicial officers and prosecutors often lack specialized training in digital evidence handling, leading to procedural lapses and prolonged adjudication. Judicial capacity gaps have resulted in inconsistent verdicts and delays that weaken the overall deterrence of the law. Comparatively, India's IT Act (2000) has been supported by specialized cybercrime courts and continuous judicial training, which Pakistan currently lacks. Therefore, establishing dedicated cybercrime benches and digital evidence training programs for judges and prosecutors can significantly improve the speed and accuracy of legal outcomes(Qadeer, 2020).

5.4 International Cooperation and Legal Harmonization

A critical finding of this research is Pakistan's limited engagement with international cybercrime treaties. The country has not ratified the Budapest Convention on Cybercrime (2001), which restricts its ability to engage in cross-border investigations, data sharing, and extradition processes. Hussain (2023) argues that this isolation hampers Pakistan's access to global cybersecurity intelligence networks, creating enforcement gaps in cases involving transnational offenders. Aligning national laws with international conventions and signing mutual legal assistance treaties (MLATs) can improve the effectiveness of international cooperation. Integration with global frameworks will not only enhance credibility but also ensure legal harmonization with global digital governance standards.

5.5 Public Awareness and Victim Protection

The findings indicate that public awareness of cyber laws remains significantly low, especially in rural and semi-urban areas. Many victims of online fraud, harassment, or data theft either fail to report incidents or lack knowledge of legal recourse. While PECA 2016 includes sections on online harassment and defamation, their enforcement is hindered by limited awareness campaigns and insufficient victim support systems. Studies by Naseer and Bhatti (2022) reveal that societal taboos, fear of reputational harm, and limited digital literacy contribute to underreporting. To enhance deterrence and trust in the justice system, Pakistan must initiate nationwide awareness programs, strengthen victim assistance cells, and promote digital ethics education in schools and universities (Sherwani, 2018).

5.6 Policy Coordination and Governance Challenges

The study also highlights a fragmented governance structure in Pakistan's cybercrime management. There is a lack of coordination among the Ministry of Information Technology and Telecommunication (MoITT), the FIA, and judicial authorities. Overlapping jurisdictions and inconsistent communication between institutions result in procedural inefficiencies and policy stagnation. Comparative models, such as the UK's National Cyber Security Centre (NCSC), demonstrate how unified command structures can enhance policy coherence and rapid response to cyber threats. Pakistan needs a centralized cybersecurity governance body responsible for policy integration, data management, and inter-agency collaboration to streamline national cyber resilience (Qarar, 2020).

6. CONCLUSION

The study concludes that while Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 represents a major step toward regulating cyber-related offenses, its current implementation and legislative structure remain insufficient to effectively combat the evolving landscape of digital crime. The research highlights that cyber threats have become increasingly transnational, sophisticated, and technologically complex—demanding continuous adaptation of the legal and institutional framework (Sherwani, 2018).

Through qualitative doctrinal analysis, this study found that Pakistan's legislative, judicial, and institutional response faces multiple challenges: outdated legal provisions, inadequate enforcement mechanisms, limited judicial expertise, and lack of international cooperation. The Federal Investigation Agency (FIA) Cybercrime Wing, though central to

enforcement, suffers from operational constraints such as inadequate resources, limited forensic capabilities, and poor inter-agency coordination. Similarly, the judiciary's limited capacity to interpret digital evidence undermines consistent case outcomes (Mohiuddin, 2006).

At the policy level, the study concludes that fragmented governance and non-alignment with international frameworks restrict Pakistan's global collaboration in cybercrime prevention. These limitations collectively weaken deterrence and public confidence in the justice system. Therefore, an integrated reform approach—combining legislative modernization, institutional strengthening, judicial specialization, and public awareness—is essential for a robust and future-oriented cyber justice framework (McQuade, 2008).

7. RECOMMENDATIONS

7.1 Legislative Reforms

To ensure Pakistan's cyber laws remain effective and relevant in the face of evolving digital threats, legislative reform is imperative. The Prevention of Electronic Crimes Act (PECA) 2016 should be amended to include provisions for emerging offenses such as crypto currency fraud, artificial intelligence misuse, and cross-border data breaches. Moreover, the establishment of a periodic legislative review mechanism—perhaps every three years—would allow lawmakers to assess and update the Act in response to technological advancements. Pakistan should also align its legal framework with international standards, particularly those outlined in the Budapest Convention on Cybercrime (2001), to promote greater harmonization and enhance cross-border cooperation in the investigation and prosecution of cyber offenses.

7.2 Institutional and Investigative Strengthening

The effective enforcement of cybercrime laws depends heavily on the operational capacity of investigative bodies, especially the Federal Investigation Agency (FIA) Cybercrime Wing. There is a need for dedicated funding to upgrade digital forensic infrastructure and expand regional cybercrime units across the country. Continuous capacity-building programs must be introduced to train investigators, prosecutors, and technical staff in handling digital evidence, cyber forensics, and emerging cyber threats. Furthermore, Pakistan should establish a National Cybercrime Coordination Cell to enhance collaboration between the FIA, the Ministry of Information Technology and Telecommunication (MoITT), the Pakistan Telecommunication

Authority (PTA), and other relevant agencies. Such coordination would reduce duplication of efforts and ensure timely sharing of cyber intelligence.

7.3 Judicial Reforms

A strong judicial system is central to ensuring the effectiveness of cybercrime legislation. The creation of specialized cybercrime courts or dedicated benches within existing judicial structures can help expedite case resolution and ensure consistency in legal interpretation. Judges and prosecutors should receive specialized training in digital forensics and cyber law, facilitated through the Federal Judicial Academy and other relevant institutions. Additionally, a comprehensive legal database should be developed, containing cybercrime judgments, legal precedents, and scholarly commentary to assist legal practitioners and support academic research. These steps will enhance judicial competence and promote informed decision-making in cyber-related cases.

7.4 International Cooperation

Given the transnational nature of cybercrime, Pakistan must strengthen its international cooperation mechanisms. Although it has not yet ratified the Budapest Convention, aligning national procedures with its principles will enable improved mutual legal assistance and data sharing. Pakistan should also pursue bilateral and multilateral agreements, particularly Mutual Legal Assistance Treaties (MLATs), with technologically advanced nations to facilitate cross-border investigation, evidence collection, and extradition. Furthermore, Pakistan should actively participate in global cyber intelligence forums and international training programs to build institutional expertise and reinforce global partnerships against cyber threats.

7.5 Public Awareness and Digital Literacy

Raising public awareness is crucial for effective cybercrime prevention. The government should launch nationwide awareness campaigns focusing on digital safety, privacy protection, and online reporting mechanisms. Schools, colleges, and universities should incorporate cyber ethics and digital literacy into their curricula to foster responsible online behavior from an early age. In addition, victim support services must be strengthened through helplines, online complaint portals, and psychological counseling for victims of cyber harassment, financial fraud, and identity theft. Such measures will empower citizens to recognize, report, and resist cyber threats effectively.

7.6 Policy Coordination and Governance

Effective cyber governance requires a unified policy approach. Pakistan should establish a National Cyber security Authority to coordinate all cyber-related activities across ministries, law enforcement agencies, and regulatory bodies. This authority would oversee policy implementation, data protection, and inter-agency collaboration. Regular performance audits and annual cybercrime reports should be introduced to assess institutional efficiency and track progress in cyber governance. Moreover, public–private partnerships should be encouraged, allowing collaboration with technology firms, telecom operators, and cybersecurity experts for knowledge sharing, innovation, and technical assistance. A coordinated governance model will ensure that Pakistan's cybercrime response remains adaptive, transparent, and forward-looking.

REFERENCES

Allia Bukhari. (2020, October 21). Silent battles: How Pakistani women counter harassment in cyberspace. The Diplomat. https://thediplomat.com/2020/10/silent-battles-how-pakistani-women-counter-harassment-in-cyberspace/

Aziz, F. (2018). Pakistan's cybercrime law: Boon or bane. Heinrich Böll Stiftung, The Green Political Foundation and Perspective of Digital Asia.

Baker, E. W. (2014). A model for the impact of cybersecurity infrastructure on economic development in emerging economies: Evaluating the contrasting cases of India and Pakistan. Information Technology for Development, 20(2), 122–139.

Barrister Jannat Ali Kalyar. (2019, December 22). Cyber insecurity. The News. https://www.thenews.com.pk/tns/detail/586618-cyber-insecurity

Forcepoint. (n.d.). What is spoofing? https://www.forcepoint.com/cyber-edu/spoofing

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology, 10(2), 139–223.

Ingram, J. R. (2014). Digital piracy. In The Encyclopedia of Criminology and Criminal Justice (pp. 1–5).

Jamshed, J. (2021). Gender discrimination and sexual harassment in the legal profession: A perspective from patriarchal society. Women & Criminal Justice, 1–13.

Jamshed, J., Javed, M. W., Bukhari, S. W. R., & Safdar, A. (2020). Role of police investigation in the criminal justice system of Pakistan. International Journal of Management Research and Emerging Sciences, 10(2).

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

Kundi, G. M., & Shah, B. (2009). IT in Pakistan: Threats and opportunities for e-business. The Electronic Journal of Information Systems in Developing Countries, 36(1), 1–31.

Mariam Sherwani. (2018). The right to privacy under international law and Islamic law: A comparative legal analysis. Kardan Journal of Social Sciences and Humanities, 1(1), 30–48.

McQuade III, S. C. (2008). Encyclopedia of cybercrime. Bloomsbury Publishing USA.

Mohiuddin, Z. (2006). Cyber laws in Pakistan: A situational analysis and way forward. CEERICSSON Pakistan.

Munir, A., & Shabir, G. (2018). Social media and cyber crimes in Pakistan: Facts, propaganda, awareness, and legislation. Global Political Review (GPR), 3, 84–97.

Mushtaque, K., Ahsan, K., Nadeem, A., & Umer, A. (2014). Critical analysis for data privacy protection in context of cyber laws in Pakistan. Journal of Basic and Applied Scientific Research, 4(10), 1–4.

Pollitt, M. (1997). Cyberterrorism—Fact or fancy? (Retrieved January 23, 2010).

Qadeer, M. A. (2020). The cyber threat facing Pakistan. The Diplomat.

Raza Khan. (2016, August 11). Cyber crime bill passed by NA: 13 reasons Pakistanis should be worried. Dawn. https://www.dawn.com/news/1276662

Shakeel Qarar. (2020, December 29). FIA arrests man accused of obtaining, distributing child pornography on social media. Dawn. https://www.dawn.com/news/1598523/fia-arrests-man-accused-of-obtaining-distributing-child-pornography-on-social-media

Sharma, I., & Alam, M. A. (2016). Privacy and freedom issues in cyberspace with reference to cyber law. International Journal of Computer Applications, 145(3), 11–18.

Talha Khan. (2015, February 1). Cybercrimes: Pakistan lacks facilities to trace hackers. The Express Tribune. https://tribune.com.pk/story/831178/cybercrimes-pakistan-lacks-facilities-to-trace-hackers

Usman, M. (2017). Cyber crime: Pakistani perspective. Islamabad Law Review, 1(3), 18–40.

Vasudevan Sridharan. (2016, November 8). Pakistan passes "draconian" cybercrime law threatening civil liberties. International Business Times. https://www.ibtimes.co.uk/pakistan-passes-draconian-cybercrime-law-threatening-civil-liberties-1575530

Zia ul Islam, Khan, M. A., & Zubair, M. (2019). Cybercrime and Pakistan. Global Political Review, 4(2), 12–19. https://doi.org/10.31703/gpr.2019(IV-II).02