ISSN E: 3006-1466
ISSN P: 3006-1458

CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

DEEPFAKE CRIMES AND LEGAL GAPS IN PAKISTAN:A CRIMINOLOGICAL REVIEW OF PECA IN LAHORE

Laiba Batool,
(Student at Department of Criminology, BS Criminology, University of Peshawar)
shahabdullah737@gmail.com (Corresponding Author)
Ahsan Madni,
(Student at Department of ISCS, BS Criminology, University of the Punjab)
ahsanmadni699@gmail.com (Co-Author)
Noman Nadeem,
(Student at Department of Criminology, BS Criminology, NFC IET Multan)
nomannadeem2026@gmail.com
Sana Tariq,
(Student at Department of Sociology, BS Sociology, Bahauddin Zakariya University, Multan)
tsana7585@gmail.com
Coressponding Author's Email: shahabdullah737@gmail.com

Abstract

This study explores the intersection of emerging digital threats and legislative inadequacy in Pakistan, with a particular focus on the legal gaps surrounding deepfake crimes. Despite the enactment of the Prevention of Electronic Crimes Act (PECA) in 2016, the law remains silent on issues concerning synthetic media, AI-generated impersonation, and non-consensual deepfake content. Using a criminological framework, this research investigates the level of awareness regarding deepfakes and PECA among 100 university students in Lahore, drawn equally from four academic disciplines: Information Technology, Medical Sciences, Social Sciences, and Arts & Humanities. The study adopts a quantitative survey design, supported by descriptive statistics and visual analysis. Findings reveal that only 10% of respondents were aware of deepfakes and 15% had knowledge of PECA. Willingness to report deepfake harassment was low, with 65% of hesitant participants citing fear of social backlash. The study identifies key legislative and institutional shortcomings and applies criminological theories such as labeling theory and strain theory to explain patterns of victim silence and perpetrator behavior. It concludes with practical recommendations for amending PECA, strengthening institutional capacity, and embedding digital safety education across higher education institutions in Pakistan.

Keywords: Deepfake technology, PECA 2016, Digital harassment, Legal reform

1. Introduction

The rapid advancement of artificial intelligence (AI) has fundamentally transformed how societies produce, disseminate, and consume digital content. Among the most alarming applications of AI is the emergence of deepfake media—synthetic videos, images, or audio clips generated using deep learning algorithms such as generative adversarial networks (GANs) to realistically mimic real individuals (Westerlund, 2019). While these technologies can be harnessed for entertainment, education, or accessibility innovations, they have also enabled a new category of digital offenses known as deepfake crimes. These crimes involve the malicious creation or distribution of AI-generated content to deceive, manipulate, harass, or defame individuals. Common manifestations include non-consensual pornography, political misinformation, celebrity impersonation, and blackmail, where fabricated content is presented as authentic to cause reputational harm or psychological distress (Chesney & Citron, 2019; Kietzmann, McCarthy, & Pitt, 2020). What makes deepfake crimes particularly dangerous is the seamlessness with which they can mimic real people and the difficulty of verifying their falsity, making them ideal tools for abuse in digital environments. In countries like Pakistan—where cultural sensitivities and patriarchal norms dominate public discourse—the consequences of deepfake crimes are magnified. Here, notions of family honor and modesty are intimately tied to a woman's social identity, meaning that even fabricated visual or audio material can irreparably damage a person's life. The Digital Rights Foundation (2023) has documented numerous cases in which women were targeted through AI-manipulated explicit content, often circulated via social media platforms without consent. Yet, despite the gravity of these offenses, most victims refrain from seeking legal recourse, fearing public humiliation, character assassination, or dismissal by authorities (UN Women, 2022). This is compounded by Pakistan's limited institutional response capabilities and widespread gaps in digital literacy, especially among women and young adults. Legally, Pakistan relies on the Prevention of Electronic Crimes Act (PECA), enacted in 2016, as its primary instrument for addressing cybercrime. PECA criminalizes a range of offenses, including cyberstalking (Section 21), identity theft (Section 16), and electronic defamation (Section 20). However, the Act is notably silent on synthetic media, AI-generated impersonation, and deepfake-specific harms. As Khan (2021) notes, this omission results in the misapplication or stretching of outdated legal categories to cover technologically novel offenses. Law enforcement agencies often lack both the training and technological tools required to handle such cases, and prosecutors face difficulties in presenting synthetic evidence in court (Rehman, 2022). The absence of legal definitions and prosecutorial guidelines has led to inconsistent outcomes, leaving victims vulnerable and perpetrators emboldened. This study seeks to address these gaps by conducting an empirical investigation into university students' awareness of deepfakes and PECA in Lahore, Pakistan's second-largest city and a major educational hub. Using a criminological lens, the research explores the extent to which young adults understand the risks posed by deepfake technology, their willingness to report such crimes, and the institutional barriers they perceive. In doing so, the study critically evaluates the effectiveness of PECA in addressing deepfake-related offenses and contributes to the broader discourse on legal reform, digital safety, and gendered vulnerabilities in Pakistan's digital sphere. The findings aim to inform policymakers, law enforcement agencies, and academic institutions about the urgent need to modernize legislative frameworks and implement educational interventions to safeguard individuals from synthetic media threats.

2. Literature Review

The emergence of deepfake technology has introduced unprecedented challenges for regulatory systems around the world. Scholars argue that deepfakes—when used maliciously—can significantly undermine public trust, disrupt democratic institutions, and enable targeted digital harassment (Chesney & Citron, 2019). These synthetic media products can fabricate events, distort identities, and mimic individuals with alarming precision, often outpacing the ability of laws to respond adequately. Westerlund (2019) notes that the inherent difficulty in detecting deepfakes, coupled with the ease of dissemination through social media, makes them a high-risk instrument of digital crime and manipulation. In the South Asian context, and specifically in Pakistan, deepfakes represent a particularly potent threat due to existing cultural dynamics. The Digital Rights Foundation (2023) reports that more than 70% of women in Pakistan feel unsafe online, citing concerns about privacy violations, cyberstalking, and the misuse of personal images. Despite these risks, only 15% of women who experience online harassment choose to report the incidents, primarily due to fears of social backlash, institutional inaction, and victim-blaming. Similarly, UN Women (2022) highlights that women often internalize fear and shame in digital spaces, leading to self-censorship and digital withdrawal. These patterns are deeply rooted in patriarchal norms, where digital victimhood is often seen as a reflection of personal dishonor. Moreover, the Society for the Protection of the Rights of the Child (SPARC) (2022) finds that a majority of youth in Pakistan lack basic knowledge about their digital rights. University students—despite their exposure to technology—often remain unaware of relevant cyber laws and reporting mechanisms. This is especially troubling as young people represent one of the most active and vulnerable digital user groups. The

Prevention of Electronic Crimes Act (PECA) 2016 serves as Pakistan's foundational legal framework for addressing cyber offenses. While the act criminalizes several forms of digital misconduct—including cyberstalking (Section 21), identity theft (Section 16), spamming (Section 24), and defamation (Section 20)—it falls short of addressing AI-specific threats. As Khan (2021) critically observes, PECA does not define synthetic media, nor does it account for the criminal implications of AI-generated impersonation or deepfake content. This absence of terminology and legal clarity renders PECA ineffective in cases involving synthetic media, leaving law enforcement to rely on broad or outdated clauses that are ill-suited to modern threats. Furthermore, Rehman (2022) argues that Pakistan's judiciary lacks technical expertise to adjudicate cases involving deepfake evidence, and that prosecutors often struggle to present admissible forensic proof. Combined with poor digital forensics infrastructure and limited institutional training, this leads to an overall failure in prosecuting technology-enabled crimes. In sum, existing scholarship identifies several intersecting challenges that hinder Pakistan's ability to effectively address the rise of deepfake crimes. First, there is a significant disconnect between legal provisions and emerging AI technologies. While PECA criminalizes conventional forms of digital harm, it remains technologically outdated, offering no recognition of synthetic media or AI-generated impersonation. Second, there exists low digital literacy and awareness, particularly among youth and women, who are both highly active online and disproportionately targeted in cases of cyber harassment (SPARC, 2022; UN Women, 2022). Lastly, Pakistan's criminal justice system is institutionally unprepared to handle deepfake-related offenses, owing to insufficient training, lack of digital forensics expertise, and ambiguous evidentiary standards (Rehman, 2022).

3. Methodology

This study employed a cross-sectional, quantitative research design to examine university students' awareness of deepfake technologies and relevant legal frameworks, specifically the Prevention of Electronic Crimes Act (PECA), in the context of Lahore, Pakistan. Lahore was chosen as the site for data collection due to its high concentration of academic institutions and diverse student body, which allowed for a representative understanding of youth digital literacy and perceptions of cybercrime legislation.

3.1 Participants

A total of 100 undergraduate students were recruited from four higher education institutions in Lahore using a purposive sampling strategy. To ensure disciplinary diversity and enable comparative analysis, the sample was stratified equally across four academic domains: Information Technology (IT)/Computer Science, Medical Sciences, Social Sciences, and Arts & Humanities. Each group consisted of 25 students. Gender balance was intentionally maintained, with 50 male and 50 female respondents. All participants were between the ages of 18 and 25, enrolled in full-time undergraduate programs, and provided informed consent prior to participation.

3.2 Instrument Design

Data were collected through a structured, self-administered questionnaire developed using Google Forms. The instrument was reviewed by domain experts in digital law and criminology to ensure content validity and alignment with the study objectives. The questionnaire consisted of four primary sections: demographic information, awareness of deepfakes, knowledge of PECA, and willingness to report deepfake-related incidents. It also included questions regarding perceived barriers to reporting and sources of digital education. Most items employed dichotomous (Yes/No) responses, allowing for descriptive and comparative statistical analysis. To ensure clarity and accessibility, the questionnaire was administered in English, the medium of instruction in most Pakistani universities.

3.3 Data Analysis

Responses were exported to Microsoft Excel for data cleaning and organization. Descriptive statistics, including frequencies and percentages, were calculated to summarize key variables. Data visualization was conducted using Python's Matplotlib library, enabling the construction of horizontal bar charts and comparative graphs that illustrated trends in awareness and reporting behavior by field of study. These visual outputs supported the empirical interpretation of the findings and served as a foundation for the subsequent legal and criminological analysis. Ethical clearance for the study was obtained from the host university, and participation was voluntary and anonymous, ensuring compliance with ethical standards outlined by the American Psychological Association (APA, 2020).

4. Results

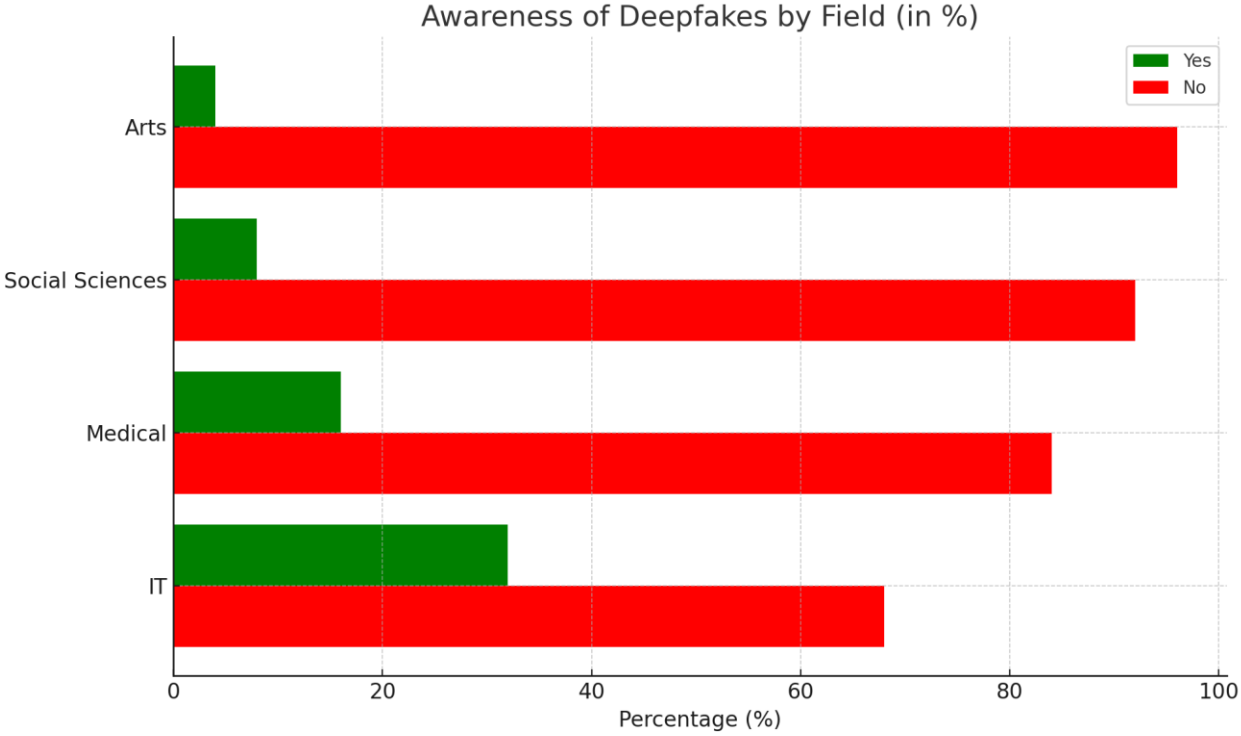
4.1 Awareness of Deepfakes

Only **10%** of students had heard of deepfakes. IT students were the most aware (32%), followed by Medical (16%), Social Sciences (8%), and Arts (4%).

Table 1: Awareness of Deepfakes by Field

Field	Heard of Deepfake (Yes)	Heard of Deepfake (No)
IT	8	17
Medical	4	21
Social Sciences	2	23
Arts	1	24

Figure 1: Awareness of Deepfakes by Field



4.2 Awareness of PECA

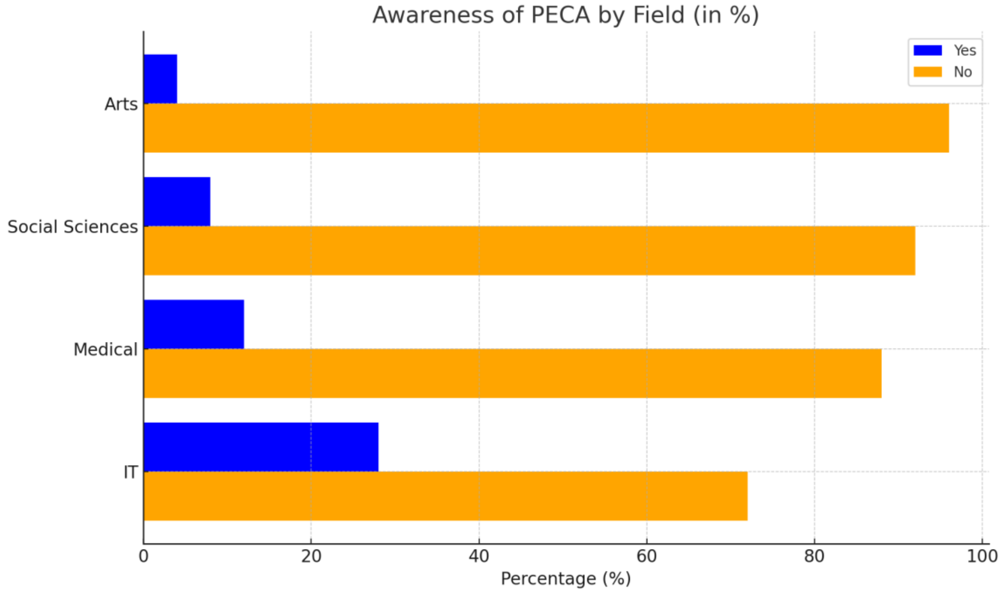
Only 15% of all students surveyed were aware of PECA. The IT group again had the highest awareness at 28%.

Table 2: Awareness of PECA by Field

Field	Aware of PECA (Yes)	Aware of PECA (No)
IT	7	18
Medical	3	22

Social Sciences	2	23
Arts	1	24

Figure 2: PECA Awareness by Field



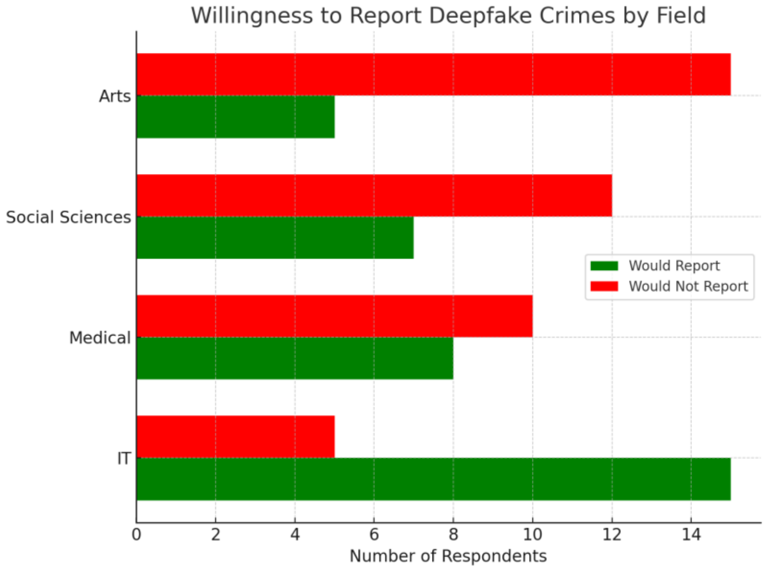
4.3 Willingness to Report Deepfake Harassment

Only **35%** of respondents said they would report a deepfake-related incident. Another 30% were unsure, and 35% stated they would not report.

Table 3: Willingness to Report Deepfake Crimes

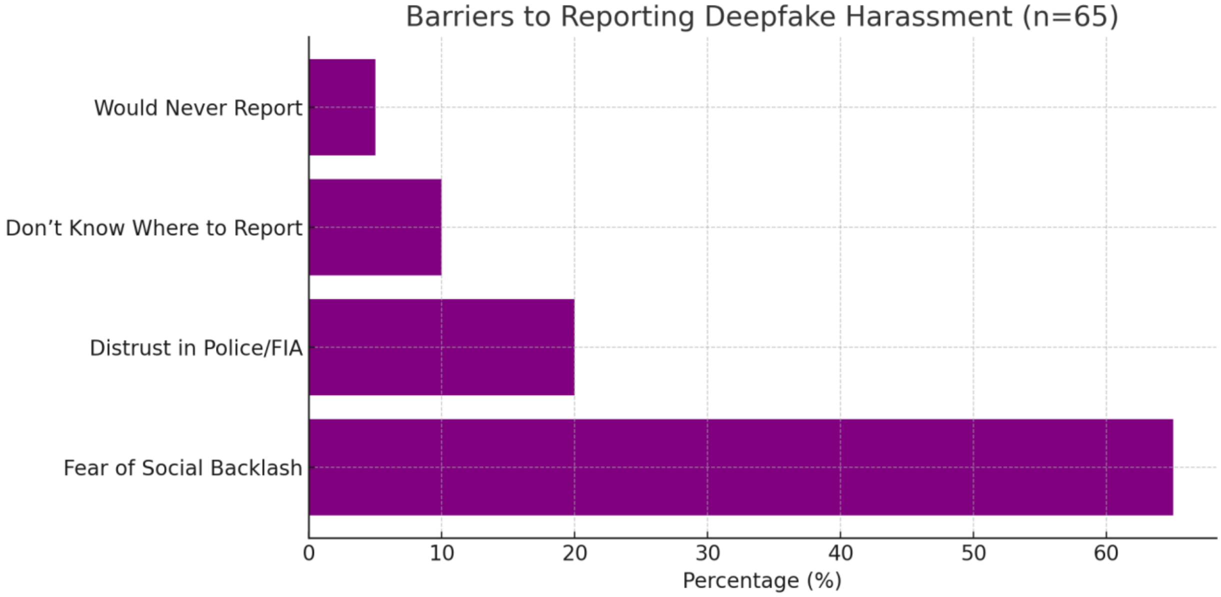
Field	**Would Report**	**Would Not Report**
IT	15	5
Medical	8	10
Social Sciences	7	12
Arts	5	15

Figure 3: Willingness to Report by Field



4.4 Barriers to Reporting

Among the 65 participants who indicated that they were either hesitant or unwilling to report deepfake-related harassment, several critical barriers emerged. The majority (65%) cited fear of social backlash, suggesting that cultural stigma and concerns over personal reputation—particularly for female respondents—played a major role in silencing victims. Additionally, 20% of students expressed a lack of trust in law enforcement agencies such as the police or the Federal Investigation Agency (FIA), indicating systemic skepticism regarding institutional responsiveness and effectiveness. Another 10% of participants reported that they did not know where or how to report such incidents, highlighting significant gaps in public awareness and access to legal channels. A smaller segment (5%) stated they would never report such crimes under any circumstances, which may reflect a deeper sense of resignation or fear of retraumatization. These findings collectively underscore the pervasive influence of social stigma, institutional distrust, and informational deficits in discouraging victims from seeking justice, particularly within Pakistan's conservative and gender-sensitive societal framework.



5.1 Gaps in PECA

The Prevention of Electronic Crimes Act (PECA), enacted in 2016, was designed to provide a legislative framework for addressing cyber offenses in Pakistan. The Act includes provisions for criminalizing cyberstalking (Section 21), identity theft (Section 16), and electronic defamation (Section 20), among other digital infractions. However, despite its foundational intent, PECA lacks specificity regarding synthetic or AI-generated content, such as deepfakes. It does not define or regulate the use of manipulated media created through artificial intelligence, nor does it impose penalties for AI-generated impersonation or the dissemination of non-consensual synthetic media. As Khan (2021) notes, this legal ambiguity leaves both victims and law enforcement agencies without adequate tools to pursue justice in deepfake-related cases. The absence of precise legal definitions and enforcement mechanisms severely hinders prosecution and contributes to procedural delays, legal loopholes, and inconsistent judicial interpretations. Consequently, PECA remains ill-equipped to address the technological realities and social harms posed by emerging threats such as deepfakes.

5.2 Criminological Insights

A deeper understanding of the socio-psychological dynamics surrounding deepfake victimization and perpetration can be obtained through established criminological theories. Labeling theory, introduced by Howard Becker (1963), posits that individuals are often deterred from reporting criminal incidents due to fear of societal stigmatization. In the context of Pakistan's conservative culture, where female honor and morality are tightly linked to public perception, victims—especially women—fear being labeled as dishonorable, even when they are clearly the targets of digital manipulation. This fear of moral judgment by family, peers, and society discourages victims from approaching law enforcement agencies, thereby allowing perpetrators to operate with impunity. Furthermore, societal blame often shifts toward the victim rather than the offender, perpetuating a cycle of silence and underreporting.

Complementing this is Robert Merton's (1938) strain theory, which provides insight into the motivations of offenders. According to this theory, individuals may resort to deviant behavior when they experience a disconnect between socially approved goals and the legitimate means to achieve them. Within the context of deepfake crimes, individuals—particularly those facing social exclusion, academic pressure, or unemployment—may turn to digital manipulation as a means of retaliation, assertion of control, or expression of frustration. Perpetrators may rationalize their actions as a response to perceived grievances or injustices, further complicating the moral and legal landscape surrounding deepfakes. When viewed together, these theories highlight not only the societal barriers that inhibit victims but also the socio-economic and psychological conditions that drive offenders to exploit AI technologies for harmful purposes. Understanding these dynamics is essential for designing effective prevention and response mechanisms in Pakistan's evolving cyber landscape.

6. Discussion

The findings of this study reveal a concerning disconnect between technological advancements in cybercrime and the level of digital literacy among Pakistani university students. Despite being digital natives, a significant majority of participants—90%—were unaware of what deepfakes are, and 85% had never heard of the Prevention of Electronic Crimes Act (PECA). These statistics suggest a failure on the part of both legal institutions and educational systems to disseminate critical information about cyber threats and digital rights. The lack of structured digital literacy curricula across universities in Lahore has left students largely reliant on social media for information, which is often unverified, fragmented, or misleading. This creates vulnerabilities not only in their understanding but also in their ability to protect themselves from manipulation and exploitation.

The gendered dimension of this issue is particularly troubling. Female participants consistently expressed more fear, hesitation, and lack of trust in institutional mechanisms than their male counterparts. This is consistent with the findings of UN Women (2022), which reported that women in South Asia are disproportionately affected by online harassment and are less likely to report due to fear of retaliation, victim-blaming, and social disgrace. The fact that 65% of hesitant respondents in this study cited fear of social backlash as the primary reason for not reporting a deepfake-related crime underscores the cultural pressures faced by women. These findings reinforce the need for gender-sensitive reforms in both law enforcement training and digital education. Moreover, the study reflects broader societal trends, where emerging technologies outpace legal reforms and institutional awareness, leaving students exposed to sophisticated forms of cybercrime without the tools to recognize, report, or resist them.

7. Recommendations

In light of the findings and legal analysis, several policy and institutional interventions are urgently recommended to mitigate the rising threat of deepfake crimes in Pakistan. First and foremost, the Prevention of Electronic Crimes Act (PECA) 2016 must be amended to explicitly define and criminalize AI-generated impersonation, synthetic media manipulation, and non-consensual deepfake content. Without such legal recognition, courts and law enforcement agencies remain constrained in their ability to prosecute offenses effectively (Khan, 2021).

Secondly, capacity-building initiatives for law enforcement are critical. Officers and judicial personnel must be trained in the fundamentals of cyber forensics, artificial intelligence literacy, and the sociocultural dimensions of digital gender-based violence. These efforts should be informed by a gender-sensitive approach, acknowledging the unique vulnerabilities faced by female victims in patriarchal societies (UN Women, 2022).

Third, universities must play a central role in prevention by integrating digital safety and media literacy into their curricula. Regular workshops, seminars, and student-led forums on emerging cyber threats—especially focused on AI, privacy, and harassment—can bridge the current awareness gap identified in this study. Educational institutions should collaborate with expert organizations like the Digital Rights Foundation (DRF), SPARC, and UN Women to establish confidential, student-accessible reporting mechanisms on campuses.

Lastly, the government and civil society must coordinate national-level awareness campaigns targeting youth and young professionals. These campaigns should leverage mainstream and social media channels to educate the public on identifying deepfakes, understanding their legal rights under PECA, and accessing support services. Only a multi-pronged, cross-sectoral strategy can create a digitally resilient generation capable of confronting future AI-driven threats.

8. Conclusion

Deepfake technology represents a rapidly evolving form of cyber victimization with serious implications for personal privacy, psychological well-being, and social integrity—particularly in culturally conservative nations like Pakistan. As evidenced by this study, the current legal framework, primarily PECA (2016), is inadequate to address the challenges posed by synthetic media. The overwhelming lack of awareness among university students in Lahore, coupled with hesitancy to report due to stigma and distrust, underscores a systemic failure in both legal preparedness and public digital education.

If left unchecked, deepfakes will continue to exploit institutional loopholes, leaving victims—especially women—silenced and perpetrators emboldened. Legislative reform, law enforcement training, and widespread digital literacy efforts are not optional but essential in safeguarding individuals from the weaponization of artificial intelligence. By acknowledging these gaps and implementing targeted interventions, Pakistan can begin to build a more secure and inclusive digital environment. The findings of this research call for urgent, coordinated action across legal, educational, and technological domains to protect the dignity and rights of citizens in the age of AI.

References

Ahmed, S. (2021). Reporting behavior among female victims of online harassment in Pakistan. *Asian Journal of Women's Studies*, 27(4), 503–520.

Anwar, S. (2021). Online gender-based violence in Pakistan: An intersectional review. *Pakistan Journal of Gender Studies*, 19(2), 85–104.

Aslam, T. (2021). Feminist legal critique of PECA and its enforcement. *Pakistan Journal of Legal Feminism*, 1(1), 55–74.

Bajwa, H. (2023). AI-generated media and Pakistani legal gaps: A theoretical analysis. *Asian Journal of Legal Studies*, 4(2), 105–120.

Baloch, Z. (2020). University students' digital literacy and cyber law awareness: A cross-disciplinary study. *Pakistan Journal of Education*, 37(1), 1–17.

Becker, H. S. (1963). *Outsiders: Studies in the Sociology of Deviance*. Free Press.

Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147–155.

Citron, D. K. (2019). Sexual privacy. *Yale Law Journal*, 128(7), 1870–1960.

Digital Rights Foundation. (2023). *Cyber Harassment Helpline Annual Report 2022*. https://digitalrightsfoundation.pk

Farooq, M., & Yousaf, F. (2021). Challenges of prosecuting cybercrime in Pakistan: Gaps in PECA 2016. *Lahore Journal of Law and Social Sciences*, 10(1), 22–36.

Haider, Z., & Rahim, F. (2020). Ethical concerns in artificial intelligence and its application in Pakistan. *Ethics and Emerging Technologies Review*, 2(1), 33–49.

International Telecommunication Union (ITU). (2022). *Measuring digital development: Facts and figures – Asia and the Pacific*. https://www.itu.int/en/ITU-D/Statistics

Kamal, M., & Hayat, A. (2020). Deepfake videos: Legal responses and regulatory challenges. *Pakistan Journal of Criminology*, 12(1), 109–123.

Kamran, T. (2023). Digital trust and the Pakistani justice system: Bridging the gap. *Journal of South Asian Public Policy*, 6(1), 66–78.

Khan, R. A., & Saeed, M. (2020). Awareness and attitude toward cybercrime legislation among university students. *Bulletin of Education and Research*, 42(2), 27–44.

Khan, S. (2021). Cyber laws and their implementation in Pakistan: A legal review of PECA 2016. *Pakistan Law Review*, 6(2), 45–59.

Latif, S. (2021). Cybercrime victimization in Pakistan: A gendered perspective. *Journal of Cybersecurity and Digital Forensics*, 2(1), 45–61.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, 3(5), 672–682. https://doi.org/10.2307/2084686

Nisar, M. (2022). Deepfake detection and prevention technologies: A technical review. *Journal of Information Security Research*, 10(4), 123–135.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Prevention of Electronic Crimes Act (PECA). (2016). Ministry of Information Technology, Government of Pakistan. https://moitt.gov.pk

Rehman, A. (2022). Judiciary and technology: Legal system's response to synthetic media in Pakistan. *Pakistan Law Digest*, 14(3), 77–89.

SPARC. (2022). *Youth and Digital Rights in Pakistan*. Society for the Protection of the Rights of the Child. https://sparcpk.org

UN Women. (2022). *Gender-based online harassment in South Asia: A rights-based analysis*. https://asiapacific.unwomen.org

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 39–52. https://doi.org/10.22215/timreview/1282

Zubair, H., & Malik, A. (2020). Legal implications of emerging technologies in Pakistan. *South Asian Journal of Law and Policy*, 12(2), 88–104.

Kalpokas, I. (2021). *Deepfakes: The coming infocalypse*. Emerald Publishing.