JOURNAL OF POLITICAL STABILITY ARCHIVE

Online ISSN: 3006-5879 **Print ISSN:** 3006-5860
DOI: https://doi.org/10.63468/jpsa.3.4.54

Vol. 3 No. 4 (2025)
https://journalpsa.com.pk/index.php/JPSA/about

Recognized by: Higher Education Commission (HEC), Government of Pakistan

Cyber Harassment and Online Violence Against Women in Pakistan: Legal Gaps and Enforcement Challenges

Dr. Khurram Baig
Professor of Law, HOD, School of Law, Multan University of Science and Technology, Multan, Pakistan.
mkb5729@gmail.com

Hadi Ali Jafary*
Visiting Lecturer, University Gillani Law College, Bahauddin Zakariya University Multan, Pakistan.
hadialij@gmail.com

*Corresponding Author

ABSTRACT

Online violence and cyber harassment of women in Pakistan have turned out to be an urgent issue in the digital age. Although the internet connectivity and social media has resulted in a better avenue of communication, trade and participation of women in civic activities, it has also brought with it new vices of mistreating women such as cyberstalking, sharing of intimate photos without their consent, impersonation and target threats. The legal reaction, which is majorly organized by the Prevention of Electronic Crimes Act, 2016 (PECA), can be seen as the endeavor to mitigate these harms as part of the broader scope of cybercrime control. But there are large gaps, in the formulation of statutes and in institutional practice. Women have problems with reporting barriers, insufficient gender sensitive mechanisms and slow or ineffective investigation procedures. These are aggravated by the socio-cultural stigmas and lack of digital literacy which further deter victims to find solutions.

The paper interrogates these concerns by analyzing the Pakistani law using the doctrines, reviewing the enforcement practices and the comparison with the international human rights standards. It claims that both legal reform and structural changes in implementation, gender-responsive law enforcement training, better digital forensic capabilities and closer cooperation with online platforms are both necessary to address technology-enabled gender-based violence. Finally, the paper points to the necessity of a systematic, victim-focused solution to the problem of

ensuring that the digital legal framework of Pakistan is well-equipped to represent the rights of women and can be harmonized with international standards.
Keywords: Cyber harassment, online violence, women's rights, PECA 2016, digital justice, Pakistan

INTRODUCTION

Pakistan has witnessed the growth of digital technologies which has changed the way people communicate, do business and access information. The digital realm has become an important social and economic arena with more than 130 million users of the internet. However, this space has turned into a very aggressive place to women, who are disproportionately targeted with online harassment, abuse and gender-based violence. The concept of technology-facilitated gender-based violence (TFGBV) covers an extremely broad spectrum of malicious behavior, such as cyberstalking, non-consensual sharing of intimate images, sexual harassment, impersonation and threats of physical violence. Such behaviors do not only undermine the safety of women online but have enormous offline impacts such as tarnished image, emotional abuse and in the worst scenario, physical violence.

The laws to be used to solve such harms in Pakistan can mainly be found in the Prevention of Electronic Crimes Act, 2016 (PECA). The Act is a criminal act against different types of cyber misconduct including unauthorized access, cyberstalking and the transmission of offensive material. Nonetheless, PECA was not designed with the explicit aim of tackling gender-based harms and its provisions tend to be too broad or limited to capture the experience of women online. Critics complain that the Act is more inclined to keep the state security and censorship to ensure that those who violate harassment are not punished than to over-protect the freedom of speech (Yongmei & Afzal, 2023).

of the availability of statutory tools, there is still a weak enforcement. Peaceful implementation of PECA requires the Federal Investigation Agency (FIA) which is experiencing chronic resources shortage, technical constraints and a lack of gender-sensitive training (Amjad et al., 2021). In the FIA Cyber Crime Wing, most women who come forward with complaints cite the delays in the processes, rudeness and non-confidentiality, which compound their unwillingness to file complaints (Ali, 2025a). Consequently, the legal process itself may become yet another victimization sphere instead of protection.

The civil society groups, including the Digital Rights Foundation (DRF), have been critical in recording and addressing the issue of online harassment by providing helplines and enlightenment campaigns. Their results are consistent in that more women are reporting online abuse, and that there are systemic space failures in institutional response (Ali, 2025b). Simultaneously, the international human rights organizations also stress that online harassment should be viewed as a type of violence against women and states are obligated to act under the treaties like the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) (Paes & Geraldes, 2021a).

It is in this context that this paper explores the gaps in the law and enforcement issues in the area of cyber harassment and online violence on women in Pakistan. It uses a doctrinal interpretation of PECA and the associated legislations, alongside empirical evidence of the civil society reports and international standards. The research posits that the solution should not be simply statutory changes, but institutional changes, capacity building and a victim-focused approach that will make women safe, dignified and be able to access justice in the digital age.

Legal Framework in Pakistan

Cyber harassment and online violence against women in Pakistan are mainly legally regulated in accordance with the Prevention of Electronic Crimes Act, 2016 (PECA). PECA is the first act to be enacted in reaction to the unprecedented growth of the internet application and the increase of cyber offences, indicating the first attempt at legislating the digital world in the country. Its clauses deal with a wide scope of misconduct, such as access to data without permission, cyberstalking, hate speech and sharing of objectionable material. Although PECA has offered a legal basis to criminalize some types of online abuse, gender-based harms have been addressed inconsistently and, in most cases, insufficiently (Khan et al., n.d.-a).

Key Provisions of PECA Relevant to Women's Protection

PECA contains several clauses that touch upon the cases of acts that belong to the category of technology-facilitated gender-based violence directly or indirectly. Section 21 would also criminalize the offences against the modesty of the natural person, such as sending sexually explicit photos or videos without consent. Section 24 outlaws cyberstalking, and sets it in broad terms as attempts to contact or monitor a person repeatedly via electronics. Section 22 makes it illegal to spam and it happens to harass someone but the boundary of what is meant by harassment is not clearly delineated. Also, Section 25 deals with unauthorized access to identity information which has been referred to in instances of impersonation, fake social media accounts or doxxing (Sethi, 2025).

Regardless of such provisions, there are still major gaps in definitional and procedural aspects. In an example, the culturally charged and ambiguous nature of the word modesty means that it remains to the interpretations of the law enforcement and the court to undermine the law. On the same note, the cyberstalking as defined by Section 24 fails to fully encompass more recent forms of harassment, including organized online provocation, non-consensual deepfakes or consistent harassment using encrypted messaging services. The law is thus an indication of a lag in the drafting of the law and the technological progress.

Constitutional and Ancillary Legal Protections

In addition to PECA, it is possible to find protections in the constitutional and general criminal law in Pakistan. Article 14 of the Constitution safeguards the privacy of home and the dignity of man and Article 25 guarantees equality before the law and also outlaws discrimination on the basis of sex. These clauses give a constitutional context on safeguarding women against internet harassment (Razzaq, n.d.). Also, the list of the provisions of the Pakistan Penal Code (PPC), including the

Section 509 (insulting the modesty of a woman) and the Section 354 (assault or criminal force targeting a woman with intent to outrage her modesty), have sometimes been applied to the cases with online character. These provisions however, were initially developed within the physical space and do not suit well in the virtual space.

The interplay between PECA and existing criminal law has created both overlap and uncertainty. Some cases have been prosecuted under the PPC rather than PECA, reflecting confusion among law enforcement officials about the correct legal route. This lack of clarity contributes to delays and reduces the likelihood of effective remedies for victims.

Institutional Rules and Procedures

PECA is enforced by the Federal Investigation Agency (FIA) who maintain special Cyber Crime Wings in major cities. FIA can open complaints, examine crimes and coordinate and collaborate with technology sites to recover data or shut downs. Nevertheless, evidence collection and digital forensics processes have not been well developed. It is often reported that FIA investigators are under-equipped and get inadequate training to appropriately approach sensitive complaints, especially those related to women (Imam & Naz, 2024a). Furthermore, Pakistan's data retention rules are vague and service providers often resist cooperation, especially when servers are located abroad.

In 2024, Pakistan undertook major institutional reforms in its cybercrime enforcement framework through the establishment of the National Cyber Crime Investigation Agency (NCCIA), which has replaced the Federal Investigation Agency (FIA) Cyber Crime Wing as the primary investigative body under the Prevention of Electronic Crimes Act, 2016 (PECA). The NCCIA now operates under the Ministry of Interior with specialized divisions for digital forensics, data recovery and victim protection. The reform aims to address chronic institutional challenges that previously existed within the FIA, such as limited resources, lack of gender sensitivity and delays in complaint processing.

The NCCIA's mandate includes enhanced inter-agency coordination, a digital evidence management system and a dedicated gender and child protection cell, which seeks to ensure confidentiality and responsiveness in cases involving women victims of cyber harassment. While these reforms are promising, early evaluations suggest that challenges persist regarding public awareness, jurisdictional overlap with provincial police, and effective implementation of victim-friendly procedures.

The transition from FIA to NCCIA represents a significant policy shift toward specialized, technology-driven enforcement of PECA, and offers a renewed opportunity to institutionalize gender-sensitive mechanisms in Pakistan's digital justice system.

The other procedural constraint is that there are no gender sensitive protocols. Online harassment victims commonly complain that they feel intimidated or dismissed by the law enforcement. This is worsened by the fact that the FIA cybercrime units do not have female personnel. Despite these efforts by the FIA over

the past few years to increase its outreach and accessibility, there are still areas of weaknesses in maintaining victim-friendly procedures that avoid infringing confidentiality and dignity.

Critical Assessment of the Legal Framework

Although PECA can be seen as a step towards consideration of cyber offences, it still does not cover the realities of the experiences of women online. Its language is moralistic and it has a focus on modesty and not autonomy, dignity and consent. In addition, the enforcement structure of the Act overemphasizes state security aspects, blasphemy and sedition, and the grievance of women is therefore given a back seat. According to scholars and civil society organizations, the law does not act as a tool of empowerment but, more often, acts as a censorship tool, which weakens not only digital rights but also the safety of women (Naseer & Ashraf, 2022).

In short, the Pakistani legal environment offers partial yet piecemeal coverage of online violence. The provisions of PECA create offences that may be applied to technology-mediated gender-based violence, but ambiguities in definitions, procedural protections, and weak institutionalization and mechanisms play a major role in its ineffectiveness. The promise of equality and dignity in the constitution is still just a dream in this area unless statutory and enforcement reforms are made.

Enforcement Architecture & Practice

The enforcement of the Pakistani system of cybercrime is mainly in the hands of the Federal Investigation Agency (FIA), which was responsible under the Prevention of Electronic Crimes Act, 2016 (PECA) to investigate and bring charges on electronic criminal activities. Practically, though, the enforcement architecture has been criticized as being under-resource, gender-insensitive and uneven in terms of technology-facilitated gender-based violence (TFGBV).

The Role of the FIA Cyber Crime Wing

The FIA Cyber Crime Wing has regional offices in major cities and its jurisdiction is the offences mentioned under PECA. It registers complaints, undertakes digital forensics and brings cases to be prosecuted in special courts. In theory, such a central structure ought to facilitate enforcement and give it a specialized concentration on cyber offences. However, as victims and civil society organizations have complained, there are severe constraints in practice. As an example, investigators in many cases do not have the technical skills to access deleted information, follow anonymous identities or obtain admissible electronic data (Shahaab et al., 2021). The result is that many complaints either stall during investigation or collapse in court due to evidentiary weaknesses.

Moreover, the FIA has been accused of institutional culture insensitivity to gender. Women who make visits to the Cyber Crime Wing often complain of discriminative or even chauvinistic attitudes. In other instances victims have been discouraged to file complaints as a way of being ashamed of it and this is indicative of deep-rooted patriarchal beliefs in the law enforcement system (Henshaw, 2023). Such responses not only undermine women's trust in the system but also reinforce

social stigma around reporting online harassment.

3.2 The Role and Need of National Cyber Crime Investigation Agency (NCCIA)

The enforcement of Pakistan's cybercrime laws has undergone significant institutional reform with the establishment of the National Cyber Crime Investigation Agency (NCCIA) in 2024 (Ahmad et al., 2025). The NCCIA has replaced the Federal Investigation Agency's (FIA) Cyber Crime Wing as the principal authority responsible for implementing the Prevention of Electronic Crimes Act (PECA) 2016. Operating under the Ministry of Interior, the NCCIA's mandate encompasses investigation, digital forensics, data recovery, and coordination with technology companies and international organizations. The creation of this dedicated body was aimed at addressing the structural weaknesses that characterized the FIA's earlier enforcement model such as limited resources, delayed complaint processing, lack of technical expertise and inadequate gender-sensitive mechanisms. The NCCIA now features specialized divisions, including a Gender and Child Protection Cell, a Digital Forensics Laboratory, and a Victim Support and Confidentiality Unit, designed to enhance institutional responsiveness and accountability. Despite these positive reforms, initial reports indicate that practical challenges persist, including jurisdictional overlaps with provincial police, limited public awareness of the agency's functions, and the need for continuous capacity building (Jones, 2012). Nonetheless, the NCCIA represents a critical evolution in Pakistan's cyber enforcement architecture, signaling a policy shift toward a more specialized, technology-driven, and victim-centered approach.

Case Handling and Procedural Bottlenecks

Procedural inefficiencies further weaken enforcement. The victims must present written complaints, submit electronic evidence and most of the times attend in-person at FIA offices. Such demands may be overwhelming, especially to women in rural communities that may not be digitally literate or have access to safe transportation (Bansal et al., 2024a). Delay in investigation is typical after a complaint is reported as cybercrime units are overloaded with an increasing number of cases. The Digital Rights Foundation (DRF) reported a massive rise in complaints recorded on the Cyber Harassment Helpline in 2023, yet the number of FIA units has not expanded accordingly (Imam & Naz, 2024b).

Another recurring bottleneck is coordination with technology companies. Many of the platforms where abuse occurs, such as Facebook, Instagram or WhatsApp, operate under foreign jurisdictions. The FIA lacks binding agreements with these companies, which means requests for data or content takedowns often go unanswered or face long delays. This gap leaves victims exposed to ongoing harm, as abusive material remains online for extended periods.

Interaction with Special Courts and Judiciary

The cases examined within the framework of PECA are sent to special courts. Although the inception of these courts was supposed to hasten the process of litigating cybercrime offenses, in the real world, the speed of this process is still

sluggish. Judges are frequently not specially trained to handle digital evidence, and might make much use of technical interpretations by FIA investigators. This gives rise to inconsistencies in decisions and undermines the violence prevention effect of prosecutions. It has also been noticed by legal practitioners that courts give precedence to cases related to financial crimes or threats to the national security, making harassment cases secondary (Faisal et al., 2024a).

This is worsened by the absence of gender-sensitive judicial procedure to help victims. To provide an example, hearings might fail to ensure privacy of the victims especially when it comes to intimate pictures. Cross- examination is sometimes bordering on victim-blaming, which may also retraumatize complainants. Despite the fact that the judiciary has started to appreciate the gravity of TFGBV, structural changes are minimal.

Civil Society and Parallel Mechanisms

Civil society groups have entered to fill gaps that have been left by the weaknesses of the formal enforcement. Cyber Harassment Helpline is a legal advice and psychological counselling and technical support service offered by the DRF to the victims. The helpline has become a reliable channel especially to the women who fear approaching state institutions. Its statistics have remained among the few credible materials that record the magnitude and the character of online harassment in Pakistan. Nevertheless, as important as these initiatives are, they cannot replace a sound state-enforcement mechanism.

Correspondingly, a few provincial governments as well as university administrations have developed complaint cells or awareness initiatives but that is only that. Lack of coordination at the institutional level between such initiatives and the FIA dilutes the effectiveness of such initiatives.

Assessment of Enforcement Gaps

A paradox is present in the enforcement architecture. On one hand, Pakistan has a central agency whose statutory powers to fight cybercrime. Institutional weaknesses, scarcity of resources and social-cultural prejudices, on the other hand, make this mechanism ineffective to most women. The inability by the FIA to adopt gender-sensitive measures, the limited knowledge of the judiciary and lack of robust cooperation in the platform all contribute to the inaccessibility to justice. PECA cannot guarantee women safety against online violence unless the enforcement structures are restructured and are properly equipped to handle the task.

Patterns of Online Violence Against Women

Pakistani digital space reflects the real-life disparities of the country, where deeply rooted patriarchal values are controlling the manner in which women perceive and react to harassment. The spaces of the Internet have made women available in new ways, however, it has opened new possibilities of violence. The trends of web harassment show the scope of different actions, which border on relatively mild harassment to extreme violence with life-threatening effects. These trends are not single events but they are woven in the larger social and cultural framework that uphold gender stratification and limit women agency.

Cyberstalking and Persistent Surveillance

In Pakistan, cyberstalking is one of the most widespread types of online harassment of women. It is used to refer to unlawful and unintended efforts to contact, follow or trace an individual using electronic means. Side-effects often encountered by survivors include phone calls made anonymously, repeated text messages and unrelenting surveillance of their social media use (Ali, 2025c). In others, offenders use online resources to exploit accounts, obtain personal data or implant spying programs. The chronicity of cyberstalking can also lead women to deactivate their social media accounts, or limit the visibility of their online presence, which virtually silences them online.

Non-Consensual Image Sharing and Deepfakes

The other bright trend is the non-consensual spread of intimate photographs that is also referred to as revenge porn. The victims usually have their personal photos spread online without their authorization, either by former partners or some actors who only want to blackmail them (Bangali & Tiwari, 2024). This risk has been amplified by the emergence of the deepfake technology tool, with such fabricated explicit videos of women being increasingly used to threats of shame and silence. Although such material can be proven to be a hoax, its distribution may result in irreparable reputational damage in conservative social settings where female concepts of honour are still dominant.

Impersonation and Identity Theft

Another trend is impersonation via fraudulent accounts. To commit fraud on social media, the perpetrators fake social media accounts using the names and photographs of women, frequently with the purpose to post defamatory information, request improper interaction or ruin reputations (Faisal et al., 2024b). These do not only subject women to harassment by strangers but also destroy their reputation and confidence in the internet. Though PECA has made the illegal use of identity information punishable, its application is uneven and most cases have been dismissed on the basis of the lack of evidence.

Online Blackmail and Extortion

Blackmail is highly related to non-consentual image sharing. Most women states that they are forced to give money, sexual favors or further communication by the threat of leaked private content. The threats are especially strong in the context of the culture of Pakistan, where even the accusation of impropriety may have a destabilizing personal effect. There is suicidal evidence that associates online blackmail with suicidal cases, which highlights how the crimes are life-threatening (Bansal et al., 2024b). The severity of these cases highlights the inadequacy of current safeguards and the urgent need for rapid response mechanisms to prevent harm.

Coordinated Harassment and Online Hate Campaigns

Outside of individual offenders, women, particularly journalists, activists and politicians, are the victims of organized campaigns of harassment. In these campaigns, the groups of anonymous users tend to flood the social media with threats,

derogatory slurs and doctored images to the women. Such attacks are especially directed at female journalists who report on politics or religion, where, in addition to silencing them, they tend to deter other women to engage in the public discourse (ul Haq et al., 2024). The scale and organization of these campaigns make them difficult to counter, as they exploit the viral nature of social media platforms.

Offline Consequences of Online Violence

Although online harassment might seem to be an activity that happens in a cyber realm, its effects are very solid in the real world. Victims of harassment are usually socially ostracised, pressurised by their families or even beaten. Online abuse has in certain cases preceded honor based crimes. The fact that there is a thin line between online and offline violence is important to note in that technological-mediated harassment is not a different category; it is a continuation of structural gender-based violence.

Analysis of Patterns

These trends indicate that online violence against Pakistan women cannot be perceived as isolated acts of bad behavior only. Rather, they are an expression of a continuum of gendered violence that has cultural, social and technological influences. The survival of cyberstalking, impersonation and blackmail highlights the weakness of current protection, and the emergence of deepfakes and organized hate groups demonstrates how technological advancement frequently outsmarts legal and other institutions. The process of silencing and traumatizing women will only persist without the introduction of specific reforms that would allow women to gain the same level of presence in the world of digital lives.

Patterns of Online Violence Against Women

Women online violence in Pakistan appears in various and more complicated forms that reflect on the global harms of digital violence but which are defined by local socio-cultural realities. The most prevalent categories are: cyberstalking, non-consent sharing of intimate images, hate speech, doxxing, blackmail and creation of false social media accounts. Such actions are not isolated but are systematically aimed at muzzling women in the public arena, especially journalists, activists and women involved in political discussion (Khan et al., n.d.-b).

The gendered aspect of online violence in Pakistan is a distinct characteristic of the violence, in which the threats are frequently directed at sexual violence or family honor, thereby instead supporting a patriarchal society. According to the surveys taken by the digital rights organizations, women are disproportionately subjected to harassment that suggests that they are either immoral or sexually inappropriate, regardless, which is a manifestation of offline cultural stigmatization of female agency (*DRF-Annual-Report-2023*, n.d.). In addition, the fact that WhatsApp, Facebook, Tik Tok and Instagram are also used as a means of harassment is noteworthy since they are also crucial in the education, business and social empowerment of women, thus forming a paradox of status as sources of empowerment and disenfranchisement (Gallagher, 2023).

Technological sophistication only increases the magnitude of the problem.

False caller ID apps, hacked accounts and even artificial intelligent created faked photos are some of the tools that perpetrators have progressively utilized to harass and blackmail women. Such a shift in strategies indicates that online violence does not exist as an isolated threat anymore but as an intricate web of computer-related violence, which involves both technical and institutional capacity to effectively respond (Sector, 2024).

These patterns also reflect systemic silencing. Women who speak out against online harassment are often subjected to coordinated trolling campaigns aimed at delegitimizing their voices in civic and political debates. Such targeted harassment contributes to self-censorship, thereby undermining women's participation in public life and curtailing democratic discourse in Pakistan (Kumar et al., 2021).

Barriers to Reporting & Access to Remedy

Despite the presence of laws and special enforcement agencies on cybercrime in Pakistan, women still encounter many obstacles when reporting incidents of online violence and remedies. Such obstacles are structural, cultural, procedural and technological, a reflection of the law in theory and law in practice.

One of the main obstacles is that it is socially stigmatized and feared. Several women fear to complain due to the potential victim-blaming in families and communities associated with filing complaints. With the majority of online harassment being gendered, including the threats of sexualized violence or sharing intimate pictures, women are afraid of being blamed on inviting harassment instead of being safeguarded by the authorities (Khan et al., n.d.-c). This stigma not only discourages reporting but also forces women to endure abuse silently, often withdrawing from online spaces altogether.

Institutional insensitivity and inefficient procedures are another barrier of the first order. Despite the fact that the Federal Investigation Agency (FIA) is the main institution charged with the responsibility to work on the cases of cybercrime, women have continually complained about the attitude of the officers who have disrespected them, absence of gender-sensitive operations and bureaucratic procedures. The studies indicate that the victims are often questioned in invasive ways, disallowed to file complaints or pressurized to resolve issues outside the court of law, which weakens trust in the system (Saleem et al., 2022). Moreover, the lack of female officers and trained digital forensic experts further exacerbates the reluctance of victims to engage with state institutions.

The barrier is also technological illiteracy. A common problem is that many victims do not understand how to maintain digital evidence including screenshots, metadata or traces of IP address. In a number of instances, evidence is ruled out on account of ineffective documentation. Such ignorance is also enhanced by the slowness of law enforcement agencies to respond, which occasionally leads to the loss of the digital trails. Otherwise, the perpetrators will take advantage of anonymity and technological loopholes to escape responsibility (IMAM, 2024).

Hurdles are associated with the legal system as such. Electronic crimes are criminalized by the Prevention of Electronic Crimes Act (PECA) 2016, which is,

however, inconsistently applied. Such ambiguities of jurisdiction as whether an act is defamation, obscenity or cyberstalking, tend to postpone prosecution. Moreover, PECA remedies are highly localized in urban centers, and thus women in rural jurisdictions have a low access to reporting systems. Geographic inequality increases, therefore, inequality in the safeguarding of digital rights.

Another barrier is **fear of retaliation**. Women who pursue legal remedies frequently face further threats from perpetrators, including doxxing, smear campaigns or offline intimidation. In high-profile cases, coordinated trolling campaigns have emerged to delegitimize complainants, making the pursuit of justice emotionally and physically exhausting. Such retaliation reinforces the perception that the risks of reporting outweigh the potential benefits (Atli, 2021).

Lastly, the economical and time constraints restrain the actions of victims in seeking remedies. PECA litigation is usually lengthy, and, in addition, legal representation is costly as it involves numerous court appearances. Time, cost and possible publicity make the burden overwhelming to many women particularly, those living in the underprivileged socio-economic groups. Therefore, with the existence of laws, access to justice is not a right but a privilege of the few.

Overall, obstacles to reporting and receiving remedies in Pakistan are not merely legal but systemic. The legal framework will remain symbolic, but not substantive unless issues of cultural stigma, institutional inefficiency, technological illiteracy and socio-economic inequality are mitigated.

Comparative & International Standards

The fight of Pakistan against online violence against women cannot be construed in a vacuum; it has to be evaluated in the context and experience of comparisons as well as international human rights. An overview of other jurisdictions and international standards exposes what is good and what is lacking in the protection of the digital rights of women in Pakistan.

Another normative framework that offers a normative basis at the international level is the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), where states are obliged to eradicate gender-based violence both in the public and the domestic environment (Paes & Geraldes, 2021b). The Committee on CEDAW has elaborated that online harassment, cyberstalking and non-consent sharing of images against women should be considered as violence against women and thus states should take action by preventing, protecting and redressing these acts. Moreover, the United Nations Human Rights Council (UNHRC) has confirmed that human rights enjoyed offline should also be guaranteed online, especially the right to dignity, privacy and the lack of violence (Ncube, 2023). These international commitments frame the standards by which Pakistan's legal and institutional mechanisms are evaluated.

In contrast, the European Union provides strong illustrations of the regulatory actions that combine data protection, online safety and gender equality. The Digital Services Act (2022) compels the platforms to promptly delete the illegal content, conduct risk assessments and become more transparent with algorithms

(Kandov, 2024). Importantly, member states have embraced national approaches that also integrate legal changes with victim support, including cybercrime hotline and counseling centers. The legal framework of Pakistan does not have such a comprehensive approach where the current legislation focuses on penal punishment without similar investments in the support of victims or prevention.

The other educative example is the case of India, which has similar cultures and legal system with Pakistan. The Information Technology Act of India, which is accompanied by judicial interpretations, prohibits cyberstalking and online abuse and the civil society organization the Internet Democracy Project deals with digital literacy and advocacy (Miftha, 2024). Notwithstanding these drawbacks, India has demonstrated greater awareness of cyber harassment as a constitutional rights concern and accordingly has created more conspicuous judicial review than Pakistan. This comparative prism shows the necessity of having the judiciary in Pakistan take the initiative in interpreting constitutional guarantees according to the international law of human rights.

In addition to national legislation, soft law mechanisms like the Istanbul Convention of the Council of Europe (2011) which are not binding on Pakistan explain how extensive conventions can establish high benchmarks. The Convention binds the parties to criminalize online harassment, stalking and gendered hate speech and requiring preventive education and support to survivors (Jirovsky, 2022). Such extensive commitments are not reflected in Pakistan domestic law yet and as a result, there are weak points in both victim protection and institutional responsibility.

When Pakistan compares its framework to these global and comparative standards, one can conclude that there is a two-fold gap in it: a very narrow emphasis on punitive law making with no structural support mechanisms and a low level of incorporation of international human rights principles into domestic interpretation. In order to align to global best practices, it is important that Pakistan shifts towards a victim-based model which is the integration of legal punishments with preventive educations, platform responsibility and support of survivors.

Recommendations

The response to cyber harassment and Internet violence of women in Pakistan is a complex process that involves combining the law, institutional reinforcement, technology and cultural change. The existence of these evils goes to show that laws are not effective in every practice, on paper, but on performance, enforcement and an enabling environment where women feel safe in exercising their rights.

Legal Reforms and Clarity

The current legal framework must be revisited to ensure precise definitions of cyber harassment, cyberstalking, non-consensual sharing of images and gender-based online violence. Many women face difficulty when reporting incidents because legal provisions are vague or inconsistently applied. Expanding statutory definitions and explicitly recognizing gendered harms in cyberspace would reduce

ambiguity for both complainants and investigators. Additionally, penalties should be proportional and structured to deter offenders while protecting the due process rights of the accused.

Specialized Enforcement Mechanisms

Dedicated cybercrime units exist but often lack resources, training and gender sensitivity. Establishing specialized desks staffed with female officers and digital forensic experts would make the process more approachable for victims. Timely investigation of cases, use of modern digital tracing technologies and coordination between law enforcement agencies are critical. A specialized nationwide helpline or reporting portal exclusively for women could provide a safer entry point into the justice system.

Judicial Capacity Building

The judiciary plays a vital role in shaping legal interpretations and enforcing protections. Regular training of judges and prosecutors on cyber laws, digital evidence and gender-sensitive adjudication is essential. Courts should be encouraged to adopt expedited procedures for cyber harassment cases to minimize delays and secondary victimization.

Awareness and Digital Literacy

The only way to have legal protection is to have the awareness of the rights of victims. Women should be educated through public awareness campaigns on how to recognize cyber harassment, how to gather evidence and the legal redress available. Digital literacy programs that teach safe internet behavior and ways of resisting harassment can be incorporated into schools, universities and workplaces. The collaboration with social media, technology companies and civil society organizations can increase the scope of such campaigns.

Collaboration with Technology Companies

A big percentage of internet bullying takes place on international sites. There should be closer partnership between the government and technology companies in order to establish rapid reporting and takedown systems. Transparency and fairness in social media should be applied through community guidelines which are specific to women to ensure that they are not targeted by hate speech, trolling and image-based abuse. The gap between the victims and the international service providers could be bridged by the assistance of the local grievance officers in Pakistan.

Community Engagement and Cultural Change

There are other trends of gender inequality that are underlying in cyber harassment. Addressing the current problem needs a change in culture, which would question the attitude of patriarchy, victim-blaming and violence against women. Religious leaders, teachers and community groups can also have a significant contribution to changing the status quo and making men supporters of safe places on the internet. Long-term change can be achieved by campaigns that emphasize the dignity and agency of women instead of the victimhood of these women.

Protection of Privacy and Data Security

As online violence is usually accompanied by the misuse of personal data and

pictures, it is critical to provide data protection protective measures. Both state and non-state actors should be enforced by laws that require the protection of user data and avoid unauthorized access. Women should have access to effective means of managing their digital selves such as better consent controls and the right to request that harmful content be removed.

Multi-Stakeholder Approach

The magnitude of the problem cannot be solved by government action only. It is crucial that the state institutions, civil society, academia and other international partners collaborate. Victim support services and advocacy can be given through the Civil society organizations, whereas the academic institutions can produce research regarding the trends and policy effectiveness. Collaborations with international organizations can enable Pakistan to ensure that it uses the best practices and makes them relevant to the local realities.

Victim Support Services

In addition to punishment, the victims of internet bullying require psychosocial support. Institutionalization of counseling services, legal aid clinics and peer support networks should be done in order to enable women to emerge. Anonymity protection and provision of reporting flexibility would minimize the fear of stigma and retaliation.

Monitoring and Evaluation

Lastly, the system should have accountability mechanisms embedded in it. Transparency can be improved by regular assessment of the legislation on cybercrime, self-regulation of the enforcement authorities and publication of statistics on documented incidents. Follow-ups will also help to monitor the progress made so that reforms are not implemented but rather put into action.

CONCLUSION

Cyber harassment and Online violence against women in Pakistan are among the most burning issues of the digital era, not only in relation to the protection of individual rights, but also in matters of credibility of the state legal system. Although Pakistan has made legislative efforts and especially with the enactment of the Prevention of Electronic Crimes Act and other efforts, the continuation and development of online abuse highlights the lack of effectiveness of existing solutions. The level of law, though highly important in establishing a base, is still restricted in scope and implementation. Unenforced, institutional and cultural barriers remain to expose the survivors and leave them frequently suppressed.

The trends of online violence show that women are overly victimized as they are harassed, blackmailed, threatened, sharing non-consent images and character attacked. Such actions do not only suppress people but also support patriarchal traditions that negatively affect the presence of women in the public, professional and political life. The prevalence of digital abuse has brought about an atmosphere of fear making some women not participate freely on online platforms, thus restricting them in accessing opportunities in education, employment and expression.

On a more detailed examination of the enforcement practices one will find that institutions in charge of dealing with cybercrime are usually poorly resourced, undertrained and not gender sensitive. This has rendered the justice system to be inaccessible or useless to several females who seek redress. In addition to institutional weaknesses, social stigmatization and cultural values are other significant disincentives to reporting because women are more afraid of reputational loss and victim-blaming than the actual abuse.

Its comparative analysis with the international standards reveals that Pakistan is behind in terms of incorporating holistic rights-based approach. Global best practices focus on more than powerful laws and technological infrastructure; they also include gender-sensitive policing, survivor support systems and digital literacy. The inability of Pakistan to align its internal system with such international standards shows that there is a gap in relation to which there is an urgent necessity to close.

The solutions proposed above tend towards a multi-pronged approach: ensuring the efficacy of laws, the institutional capacity, raising awareness and empowering victims by providing remedies that are easy to access. It is also crucial to change social attitudes according to which harassment is a norm and women are not encouraged to defend their rights. Legal reforms will not be enough without considering these cultural barriers.

Altogether, the problem of cyber harassment and online violence against Pakistani women is not a legal problem only, but a larger struggle against gender equality, human dignity and the fulfillment of the basic rights in the cyberspace realm. With the ever growing technology, the role of the state in ensuring a safe and enabling environment to women is becoming imperative. Pakistan can only hope to achieve digital environments where women are not merely safe but also empowered to contribute freely, only by consistent reforms, strong enforcement and a change of social norms.

REFERENCES

Ahmad, W., Asghar, U., & Afzal, M. (2025). An analysis of the effectiveness of FIA cyber crime laws in preventing and investigating online fraud in Pakistan: Challenges and recommendations. Research Consortium Archive, 3(2), 836–852.

Akhtar, S., & Khan, M. L. (2021). Receiver operative characteristics analysis for validation of parental expressed emotions scale. Webology, 18(6).

Al Lawati, T., Rana, A. M., Sohail, A., & Ul Haq, A. (2024). Examining the impact of green supply chain management practices on organisation performance and how to create a sustainable GSCM. Environment and Social Psychology, 9(9).

Ali, A., Khan, M. L., & Atta, N. (2024). Role of parental neglect in shaping resilience among individuals with substance use disorder. Journal of Development and Social Sciences, 5(2), 186–198.

Ali, R. (2025). Silenced online: Women's experiences of digital harassment in

Pakistan. Women's Studies International Forum, 110, 103090.
Ambreen, F., Fatima, A., Khan, S., Anum, T., & Khilji, I. (2025). The competitive mind: Impact of competitiveness on mental health. Journal of Political Stability Archive, 3(4), 734–746.
Amjad, S., Qasim, S., Alvi, U. F., & Amjad, F. (2021). The portrayal of violence against women in Pakistani electronic media. Elementary Education Online, 20(4), 2719–2719.
Ashraf, S., Khan, M. L., & Mahmood, T. (2025). Social capital, interpersonal communication skills and psychological wellbeing among young adults. Indus Journal of Social Sciences, 3(1), 251–265.
Atli, A. (2021). Illiterate mothers and their daughters: "My daughter should be educated, not be like me." Family Relations, 70(5), 1485–1497.
Aurangzeb, M. M., & Uddin, S. S. (2025). The artificial intelligence (AI) era: Challenges and opportunities for Pakistan and the Global South. Journal for Current Sign, 3(2), 254–264.
Aurangzeb, M., Uddin, S. S., Farooq, A., & Ali, R. A. (2025). Offensive realism and the Pacific Ocean: Understanding geopolitical rivalries through Mearsheimer's lens. Policy Journal of Social Science Review, 3(1), 268–278.
Bangali, S., & Tiwari, A. (2024). Breaking barriers: The power of cyber feminism in combating revenge porn. In Law and emerging issues (pp. 151–164). Routledge.
Bansal, V., Rezwan, M., Iyer, M., Leasure, E., Roth, C., Pal, P., & Hinson, L. (2024). A scoping review of technology-facilitated gender-based violence in low- and middle-income countries across Asia. Trauma, Violence, & Abuse, 25(1), 463–475.
DRF-Annual-Report-2023. (n.d.).
Faisal, S. M., Khan, N. T., & Ahmad, I. (2024). Challenges in combating cybercrime: A comparative study of Pakistani and international legal frameworks. The Journal of Research Review, 1(04), 228–242.
Fatima, S., Khan, M. L., & Kousar, R. (2024). Emotional intelligence, religiosity and quality of life among university students. Journal of Social & Organizational Matters, 3(2), 455–471.
Firdos, S., Khan, M. L., & Atta, N. (2024). Intrinsic motivation, social emotional competence and job satisfaction among school teachers. International Research Journal of Social Sciences and Humanities, 3(2), 58–79.
Gallagher, M. (2023). Gendered disinformation and platform accountability. In The handbook of gender, communication, and women's human rights (pp. 53–69).
Gurganari, L., Dastageer, G., Mushtaq, R., Khwaja, S., Uddin, S., Baloch, M. I., & Hasni, S. (2022). Assessment of heavy metals in cyprinid fishes: Rivers of district Khuzdar, Balochistan, Pakistan. Brazilian Journal of Biology, 84, e256071.
Henshaw, A. (2023). Addressing the digital gender gap. In Digital frontiers in gender and security (pp. 42–62). Bristol University Press.

Hsu, W. K. K., Le, T. D. L., Le, T. N. N., & Huynh, N. T. (2025). An advanced risk matrix model for the navigational safety of passenger-cargo ferries. SAGE Open, 15(3), 21582440251382306.

Hsu, W. K., Huang, S. H., Le, T. N. N., Wahidah, U., Huynh, N. T., & Tai, H. H. (2025). Assessment of logistics operations for international short-sea express: A case study in Taiwan. Transportation Research Record.

Imam, D. (2024). Cyber bullying in Pakistan: The silent menace. Center for Governance Research Pakistan.

Imam, S. K., & Naz, T. (2024). Cyberbullying: Legal challenges and societal impacts in the digital age. Pakistan Social Sciences Review, 8(4), 392–407.

Jirovsky, M. (2022). Gender-based online hate speech against women: Emerging regulation in international human rights law and the consequences for democracy and gender equality.

Jones, T. (2012). The accountability of policing. In Handbook of policing (pp. 693–724). Willan.

Kandov, B. (2024). Regulatory approaches for algorithms on online platforms in the Digital Services Act. ELTE Law Journal, 127.

Khan, I. A., Irshad, S., & Din, H. (n.d.). Cyber harassment and online violence against women: A critical analysis of women protection law regime in Pakistan. Journal of Law & Social Studies, 7(1), 12–25.

Kumar, P., Gruzd, A., & Mai, P. (2021). Mapping out violence against women of influence on Twitter using the cyber–lifestyle routine activity theory. American Behavioral Scientist, 65(5), 689–711.

Masih, S., Khattak, M. N., & Khan, T. I. (2025). The association of leadership with nurses' turnover intention: A two-wave cross-sectional study. International Journal of Nursing Studies Advances, 100459. https://doi.org/10.1016/j.ijnsa.2025.100459

Naseer, S., & Ashraf, C. (2022). Gender-based violence in Pakistan's digital spaces. Feminist Legal Studies, 30(1), 29–50.

Ngo, T. T., Huynh, N. T., & Yang, C. C. (2026). A sequential approach to airport efficiency evaluation. Journal of Air Transport Management, 131, 102922.

Uddin, S. S. (2017). Existence of external forces in Afghanistan: Pakistan's security dilemma since 9/11. International Journal of Asian Social Science, 7(4), 311–319.

Yasmeen, K., Khan, M. L., & Imran, H. (2024). Exploring emotional intelligence, remote work dynamics, team collaboration, and adaptive leadership. Pakistan Social Sciences Review, 8(2), 969–979.

Zafar, T. A. S. K. E. E. N., Khan, M. L., Maqsood, Z. U. N. A. I. R. A., Aidoune, Y. A. S. M. I. N. A., & Gilani, S. I. D. R. A. (2023). Psychological well-being and death anxiety among Pakistani general population during COVID-19. Journal of Jilin University (Engineering and Technology Edition), 42(4).