Journal of Law & Social Studies (JLSS)
Volume 7, Issue 1, pp 12-25
www.advancelrf.org

Cyber Harassment and Online Violence Against Women: A Critical Analysis of Women Protection Law Regime in Pakistan

Dr. Imtiaz Ahmad Khan
(Corresponding Author)
Associate Professor / Chairperson Law, University of Sahiwal, Sahiwal
Email: imtiazahmad@uosahiwal.edu.pk

Samra Irshad
Visiting Lecturer at the University of Sahiwal, Sahiwal
Email: samrairshad07@gmail.com

H Shah Jalal Ud Din
Visiting Lecturer at the University of Sahiwal, Sahiwal
Email: jshah5584@gmail.com

Abstract
It is a reality that in contemporary times women are more vulnerable to cyber harassment and online violence. This research provides a recourse to explore cyber harassment laws and online violence against women in Pakistan with argumentation that women with advancement of technology need special protection. This piece of study is constricted to the extent of addressing online violence and cyber harassment and argues for the adoption and regulation of emerging online crimes against women such as cyber stalking, cyber bullying, fake ID, nude pictures/videos and deepfakes. This research culminates the gaps in the practical implementation of cyber laws in Pakistan and resorts to inquire that to what extent they provide protection for women against online violence and cyber harassment. The argument of this paper encircles around the hypothesis that women need special protection because they are more vulnerable in the digital era, however, Pakistani cyber laws remain less effective, outdated with reactive approach to provide special protection to women. To address this predicament, this piece of study delves deep to analyze the women protection laws and judicial approach in Pakistan. It also provides the best policies and practices throughout the globe to combat online violence coupled with recommendations for cyber laws in Pakistan to address the contemporary challenges of cyber harassment with critical perspective by following the qualitative approach.

Keywords: Cyber-harassment, online violence, women protection laws, crimes, special laws, electronic crimes, legal framework.

Introduction

Cyber-harassment crime against women remains to be the most highlighted crime in contemporary times with the emergence of modern technologies. Violence of any nature and form against women is unacceptable irrespective of the socio-economic, cultures and societal concerns. One can ponder the significance of this nuance by following the account of Ban Ki Moon, a former United Nation Secretary-General, enunciated in 2008 that.

> *"There is one universal truth, applicable to all countries, cultures and communities: violence against women is never acceptable, never excusable, and never tolerable"*

The outlook of this paper explains the legal framework of online violence and cyber harassment in Pakistan as it is crucial to elaborate the context and understanding of existing laws. Every state has its legal framework regarding each and every aspect of life because laws serve as the backbone of every state conducive to create a balance in society. Several laws exist in Pakistan pertinent to women protection; however, the important thing is to find out that to what extent these laws and their operationalization work in combating the crime against women. Cybercrime is a worldwide peculiarity as with the advancement of technology, cybercrime, and victimization of women render the significant danger to the security of a person as an entirety (Saleem et al., 2023). Before the Prevention of Electronic Crimes Act (PECA), 2016, which includes provisions to protect women online and a component to hold criminals accountable who use information technology as a tool for crime, there was no significant regulation in Pakistan to protect women online. The grave danger to the security of women overall is appropriately not covered by this Demonstration as the argument goes that women are entitled to special protection in modern times (Tubrazy, 2020).

This paper offers insights to the fact that crimes against women involving online space and social platforms remain uncovered in the existing legal framework of women protection laws. The argument of the following research constitutes the negation of the special protection to women requisite to protect them in contemporary times. The research is culminated into different sections; the first one renders the existing legal framework of women protection regime and judicial approach in Pakistan, the second section provides a recourse to the international best practices to protect women against crimes encompassing online space and social platforms. It provides a foundation of critical account to debunk the effectiveness and operationalization of women protection laws to protect women in contemporary times. The research overall provides the argumentation of special protection to women against cyber-harassment and online violence by resorting to the qualitative aspects of the study. In culmination the research provides recommendations for the policy makers to ponder on this predicament to consider the concern of special protection through the inclusion of new form of online crimes against women.

Existing Legal Framework of Online Violence and Cyber Harassment in Pakistan

This account provides the existing legal framework of women protection laws in culmination to find out the extent and reality perspective of laws addressing the online crimes against women. The first consideration resorts to the constitution of Pakistan, 1973;

Constitution of the Islamic Republic of Pakistan, 1973

Every person residing on Pakistani soil is entitled to fundamental rights under the 1973 constitution. According to Article 4 of the Constitution, every citizen is entitled to fair treatment under the law. This implies that any violation of a citizen's rights, whether committed by a governmental or private individual or organization, should be justified by a national law. Article 10-A, which guarantees citizens the right to due process and a fair trial, is another pertinent clause; this clause solely applies to criminal charges. The constitution regarded as the guardian of fundamental rights provides articles for the protection of child and women. Regarding personal security, Article 09 declares that no one shall be deprived of their life or liberty. The same as in Article 25, which states that nothing can stop the government from enacting special laws to protect women and children. Article 32 makes special provisions for women's representation in local government (Women Development Department, 2021). According to Article 34, the state must take the required actions to let women to participate in all facets of life and social activities (The Constitution of the Islamic Republic of Pakistan, 1973). Women have equal rights under the Constitution of Pakistan 1973. The Principles of Policy chapter emphasizes the idea that all citizens and individuals should be treated equally and with equal rights, regardless of their gender (Asif et al., 2023).

Pakistan Penal Code, 1860

The Pakistan Penal Code offers protection for women against specific offenses, including Section 354 of the PPC, which prohibits assault or use of force against women with the intention of offending their modesty. Sections 509 and 499 of the Pakistan Penal Code deal with harassment and defamation, respectively. Take the instance of Section 509 (Pakistan Penal Code, I860 (XLV of 1860), 1860) which states that when someone says or make any gesture with the intention to invade privacy of any women, communicates in a sexual way with the intention of causing annoyance, intimidation, commits such acts on the premises of a workplace either explicitly or implicitly affecting modesty of such women, shall be punished with imprisonment and fine. Although Pakistan Penal Code elaborates instances of the behavior, the nuance of cyber-harassment remained unclear and not mentioned specifically (Asif et al., 2023). According to the abovementioned sections from PPC it is evidently proven that PPC lacks the direct provisions regarding the protection for women against cyber harassment and online violence.

The Pakistan Telecommunication Act, 1996

Pakistan Telecommunication Act of 1996 founded Pakistan Telecommunication Authority (PTA) in 1997 that is the primary licensing and regulatory authority managing Pakistan's internet and telecommunication sector. It also serves to advocate policies and encourage the expansion of telecommunication and internet services (Zahoor & Razi, 2020). The PTA is fundamentally a governmental organization under the jurisdiction of the Ministry of Information Technology and Telecommunication (MOIT). Under the guidance of the government, the authority controls online activity in close collaboration with PTCL and the FIA (Haque et al., 2013). The primary objective of the PTA was to ensure competition in the telecom market. PTA releases elements of policing under various areas of life such as the citizen's protection most against online harm, Cell phone identification, Registration and blocking, and provide the Telecom Customer Protection Guidelines, 2009. Pakistan Telecommunication Act was the first attempt to ensure protection for women against online violence (Pakistan Telecommunication (Re-Organization) Act, 1996). However, the act fails to provide the requisite to ensure special protection to women in contemporary times. Online crimes like deepfakes, cyber bullying, and cyber stalking remain to be subservient concern of this act.

The Federal Investigation Agency Act, 1974

In response to increasing demands in the fields of pecuniary offenses, immigration and passports, smuggling, and offenses with national implications, the Pakistan government formed the Federal Investigation Agency (FIA) in January 1975. FIA is the primary law enforcement agency to investigate cybercrimes and its strategic responsibility is constricted to the investigation of specific offenses related to issues involving the federal government and most importantly to investigate crimes related to computers, the internet and the unauthorized use of information technology to harass someone (Niazi, 2022). The Act provides the FIA authority over seventy-two provisions of the Pakistan Penal Code, ranging from simple assault to murder, sedition, and corruption, to allow agency to carry out such investigations with the authority to file criminal litigations under extraterritorial jurisdiction. Members of FIA have the same authority to make arrests as police officers throughout Pakistan. The function of FIA is more important in the current scenario where the law and order is being used to combat cybercrimes in Pakistan (Ahmed, 2012). Contradistinction to these instances, in reality FIA lacks a broad mandate to address cyber-harassment and online violence against women. The agency remains involved in politically driven cases and encounter resource constraints coupled with procedural complexities.

Electronic Transactions Ordinance, (ETO) 2002

The Electronic Transactions Ordinance (ETO) of 2002 made it illegal to obtain information and data of someone without authorization. Even though it is not specifically considered a criminal statute but deals with specific offences (Electronic Transactions Ordinance, 2002). The ETO provisions theoretically regulate data privacy and regulation in the absence of formal data protection legislation.

These domains of data protection and regulation are considered by National Response Centre for Cyber-Crime (NR3C) to fight cyber bullying and other online violence against women (DRF, 2018). It does, however, make unauthorized access to information and data illegal rather than directly regulating data protection. It also calls for the creation of government body with capacity to certify electronic documents and to enact laws protecting users privacy (E. A. Khan, 2018). The NR3C relies on the ETO provisions to ensure the data protection and its regulation but in reality, the implementation of this law is subjected to limitations that makes its scope narrower to consider online crimes against women.

The Electronic Crimes Act, 2004

This act was passed with the Ministry of Information Technology's consultation, adhering to the provisions of the Electronic Transactions Ordinance of 2002. This statute established the various cyberspace-related offenses as cyber-crimes. The Electronic Crimes Act of 2004 first time defines cybercrime as a wide variety of unlawful actions, including spoofing, spamming, cyber stalking and unauthorized access. More serious offenses including electronic fraud, forgery, system damage, and cyber terrorism are also included. Cybercrime also includes the introduction of malicious code, the misuse of encryption and devices, and these activities. However, this act failed to establish any enforcement unit to regulate the cybercrimes (Saleem et al., 2023). The law remains more orientated to other cybercrimes like spoofing, spamming, cyber terrorism and fraud and fails to emphasize different forms of online violence against women specifically.

The Protection against Harassment of Women at the Workplace Act, 2010

The Protection against Harassment of women at Workplace Act passed in 2010, to protect women from harassment, abuse, and intimidation at work. It covers all employees, including regular, contractual, temporary, and daily wage workers, in both the public and private sectors. It renders a comprehensive meaning of harassment, including any unwanted sexual demands, and other verbal or sexual sort that establishes an unfriendly or hostile workplace environment. This Act explains conduct standards in a comprehensive way such as to deal with harassment; every organization is required to adopt an internal Code of Conduct. It explains Mechanism for Complaints and Appeals as Complaints can be filed in a clear manner according to the Act. Incidents can be reported by employees to the inquiry committee, which will investigate within a specified amount of time (Deeba, 2021). Decisions can be appealed to the manager or other relevant authorities by both complainants and accused parties. However, the scope of this act is constricted to workplace environments and fails to provide any redressal to the victims outside of workplace.

Prevention of Electronic Crimes Act, 2016 (PECA)

Globally, modern civilizations have changed as a result of extremely fast and limitless access to vast amounts of information via a variety of communication devices, including laptops, tablets, and smartphones (S. Khan et al., 2019). In 2016, the National Assembly enacted the Prevention of Electronic Crimes Act (hereinafter PECA) to provide a comprehensive legal framework to define various kinds of electronic crimes, mechanisms for investigation, prosecution and adjudication in relation to electronic crimes. The PECA, 2016, provides various kinds of cybercrimes and their punishment. The Act purveys that; an individual will be punished for three years or more or will be charged with a fine of 1,000,000 rupees or more whenever he is found guilty of cybercrime. The PECA provides relevance of different online crimes against women in modern times. Cyber harassment, particularly when someone records a video of someone else and posts it on various social media platforms without the victim's knowledge, constitutes online violence and is covered by section 24 D of the PECA (Tanveer, 2019).

However, the court looks at whether one's integrity is in question or not that makes the court approach restrictive in providing protection to the victims of online violence. According to a survey conducted in 2019, a study shows that cyber harassment and online violence turn out to be more

risky because, in the majority of the cases, the victim remains unaware of the harasser and what harm he could bring to the victim (Tanveer, 2019). The purpose of the PECA remains to safeguard people's rights and privacy while also providing legal procedures for considering and prosecuting offenses involving electronic and online activity. Before it was passed in 2016, ETO already imposed restrictions over the unauthorized use of information. An early formulation and implementation of a well-crafted cybercrime law would have been made in country like Pakistan, where digital literacy is relatively low (Haq & Zarkoon, 2023). However, the PECA lacks the competency to consider all the cyber-nature crimes against women and to protect the people proportional to the advancement of technology in Pakistan. For instance, the PECA 2016 fails to criminalize harassing others or deals with sharing of any offensive content on social media; rather, it simply provides punishments for unauthorized access and interference. The act provides general conception of cybercrimes and apply those generalizations to online crimes against women. Contradistinction to these realities, the situation and practices in advanced countries are different and proactive. Take the instance of EU, If the objectionable video clip is not removed within an hour, the platform that released it might face heavy sanctions (Iqbal, 2023).

Sections 3 and 4 of PECA thoroughly explains that whoever with unscrupulous intention acquires unapproved access to any data will be punished for a term extending to 90 days or with a fine which might reach out to 50,000 rupees or with both, and anyone who makes copies or communicates or causes to be sent any information with malicious purpose and without permission faces a maximum sentence of six months in prison, a fine of up to 100,000 rupees, or both.

Section 5 goes on to say that anyone who intentionally damages, disrupts, or destroys all or any portion of another person's information faces up to two years in prison, a fine of up to 500,000 rupees, or both. Section 10 provides that whoever takes steps to involve in any, of the offenses under Sections 6. 7, 8, or 9, where the danger is with the aim to pressurize, threaten the public or people in general or a part of general society or make a feeling of dread or insecurity in the public eye and advance inter-faith or ethnic hatred, shall be punished with imprisonment of fourteen years or a fine. Section 14 of PECA declares punishment for the person who obtains, sells, possesses, communicates or utilizes someone else's personal data without permission will be punished with a fine of up to 5,000.00 rupees, three years in jail, or both.

Section 20 straightforwardly addresses cyber harassment and online violence against women. It forbids the utilization of data and information to harass a woman, including cyber bullying, conveying obscene, vulgar, or sexually unequivocal material or making any idea or proposition of an obscene nature, which can frequently target women or their integrity. It likewise covers dangers made against a person or their relatives through electronic correspondence. Section 21 exaggerates the true meaning of Spoofing, while not directly centered around women, spoofing can be utilized to target women in cybercrimes. This section is used to penalize spoofing, where an individual proposes a computer to harass a woman and damage their actual identity, which can be utilized to execute different offenses, including those against women's modesty. Section 25 explains hate that can be coordinated towards women, and this section denies the scattering of information through any data framework with the idea of working up hatred against any individual or gathering of people.

The PECA, 2016 overall discusses the provisions that partially and theoretically protect certain rights that empower female online users. The law also encompasses the provision of electronic fraud involving any person resorted to establish a relation with female user to procure any wrongful gain. It provides protection from electronic fraud with the punishment of two year and fine or both. Furthermore, the law directly discusses the cyber-stalking with three year of punishment, offence against dignity of natural person with punishment that may extend to three year or fine of one million rupees, and offences against the modesty of natural person (Gul & Anjary, 2022).

Judicial Approach and Women Protection against Online Violence in Pakistan

The approach of courts remained overall progressive to provide protection to more vulnerable and online victimized women in society. The courts in Pakistan departed from the general rule to grant bail in offences with less than 10 years of imprisonment in order to deny any favor to the accused. In *Fakhar Zaman vs State*, 2023 the court applied the same approach to provide protection to the woman who was victimized by the accused through modern means. This case study included the offences of cyber stalking, harming the dignity and modesty of natural person in accordance with PECA sections 21 and 24, in which complainant was helpless due to her nude images and videos were being transmitted and displayed via WhatsApp to harm her reputation and privacy (Fakhar Zaman vs State, 2023 PCrLJ 496 Peshawar High Court).

In another case *Abdul Rehman vs State, 2022* sections 3, 4 and 21 of PECA 2016 regarding the cyber stalking and transmitting objectionable images of a women were observed by the honorable court. The court refused the plea of the accused that the offences claimed did not fall in the prohibitory clause of section 497 of CrPC. The court held that, commonly in the current case the privacy of a young woman has egregiously been acquainted with the complete dishonor of her family regardless of whether her marital life went to risk. The incident was reported by her father, subsequently, the concurrent viewpoint of the court in refusing bail to the accused was appropriate given the existing facts and circumstances of the case (Abdul Rehman vs State, 2022 SCMR 526 SC).

In some cases, courts granted bail on the ground of establishing further guilt of the accused. In *Muhammad Ajmal vs State, 2022* sections 20, 21, and 24 of PECA, as making questionable pictures and recordings of young ladies by intoxicating her and sharing similar over social media, the co-accused had proactively been allowed bail given a concessional explanation made by the victim herself. A device utilized for sharing frightful and objectionable recordings and videos of the victim was of co-accused. The accused was qualified for the concession for post-arrest bail and abandoned the request of consistency; moreover, the punishment for this offense under sections 20 and 21 of PECA is 05 years of imprisonment. So, there were adequate grounds to consider that the accused case was completely covered by section 497(2) CrPC, calling for additional investigation into his guilt (Muhammad Ajmal vs State, 2022 SCMR 274 SC).

The courts also distinguished the sharing of any general data or information and its scope under the PECA. In *Sheraz Khan v. State, 2022* section 50 General Clauses Act 1897, uploading general data or information on social media and sending messages through any mobile application does not constitute a violation of PECA until it is transmitted through unauthorized access for the purpose as described in PECA or targets a specific person in the case of cyber stalking, cyber bullying, spamming, or spoofing (Sheraz Khan vs State, 2022 PCrLJ LHC).

The Case law of *Meera Shafi vs Federation of Pakistan, 2022* revolved around allegations of harassment, possibly being connected with the workplace or institutional harassment including state substances. The court decision on Harassment in Meera Shafi claimed that people or organizations associated with the Federation of Pakistan harassed her in a professional or personal capacity. It was argued that the nature of the harassment was in violation of her constitutional rights in Pakistan. The court completely checked on the proof introduced by the two parties, including any documentary evidence, declarations, and records of correspondence. The court observed at the allegations in light of the relevant provisions of the Constitution, anti-harassment laws, and any applicable administrative regulations. It looked at whether the claims of harassment were dealt with fairly. This included determining whether the Federation's mechanisms for handling such complaints were utilized effectively. The Federation's mechanisms for handling complaints of harassment were found to be either inadequate or improperly implemented, preventing the petitioner from receiving the necessary protection and redress.

The court granted Meera Shafi relief, which may consist of formal apologies, directives for compensation, and other measures to address the harm caused by the harassment. The court gave the Federation instructions to improve its policies against harassment and make sure that complaint redresses mechanisms are used properly. The decision emphasized the role of the judiciary in protecting women's rights against harassment, particularly within state institutions. It brought to light the significance of having absolute procedures in place to deal with and avert harassment to guarantee a safe and secure environment for every woman. This decision sets a precedent for future cases and emphasizes the significance of promptly and effectively responding to allegations of harassment to safeguard women's rights and dignity (Meera Shafi vs Federation of Pakistan 2022 SCMR 1267 SC).

Policies and Best Practices from International Regime to Address OVAW

The advancement of technology coupled with the concern of more participation of women in digital space has exposed women to different kinds of violence. Technology on the one hand provides benefits of communication and interaction and on the other hand it has become a tool for perpetrating violence against women. This tech-enabled violence encompasses cyber-stalking, deep fakes, online harassment and non-consensual sharing of the intimate images (Chikwe et al., 2024). This account will render the best practices from international regime to address that how they have overcome the prevalent quandary.

Best Practices of India to Combat OVAW

In its publication "Crime in India," the National Crime Records Bureau (NCRB) gathers and disseminates statistical data on crimes annually. The data also provides the details pertinent to cyber-crimes and OVAW. The central government of India in recent times have taken comprehensive measures in consultation with all stakeholders to combat online VAW (Ministry of Women and Child Development, 2022). These measures include from taking legislative measures to introduce rigorous punishments to enhanced grievance redressal mechanisms. Uttar Pradesh is acting in this regard, particularly with regard to OVAW. To address instances of cyberstalking and cyberbullying, the Uttar Pradesh government has chosen to establish a "women cyber cell" at each of the state's cyber police stations. Cybercrimes pertaining to women would be handled by the women cyber cell. There were eighteen cyber police stations spread across the state's cities as of March 2021 (The Commonwealth, 2023).

The Information Technology (IT) Act, 2000 provides the stringent punishment regarding the sharing of any sexual abuse content. Section 67B of IT Act, 2000 deals with this menace. The Information Technology Rules, 2021 hold social media platforms accountable for the safety of intermediary users. These codes make sure the robust grievance mechanism. Internet service providers (ISP's) must communicate their terms and conditions to users, which must prohibit them from publishing any content that might be harmful, obscene, defamatory, infringe upon the privacy of others, injure minors in any way, or violate any other laws (Ministry of Women and Child Development, 2022).

The government of India also runs a program called Prevention of cybercrimes against Women (CCPW) by the support of Nirbhaya Fund. Through this program, measures are taken to increase public awareness of cybercrimes, issue alerts and advisories, train law enforcement officers, prosecutors, and judges, improve cyber-forensic facilities, and build capacity. Measures, like National Cyber Crime Reporting Portal (www.cybercrime.govt.in) and a toll-free number 1930, have been operationalized in recent times to provide assistance to lodge a complaint against OVAW. Indian government in recent times have organized training programs for law enforcement agencies (Ministry of Women and Child Development, 2022). Under the Cyber Crime Prevention against Women and Children program, more than 19,600 law enforcement officers, judges, and prosecutors received training on cybercrime awareness, investigation and forensics. A provision of the Information Technology (IT) Act, 2000 addresses the threat of fraudulent calls and messages made using the

internet. Cheating via personation is punishable by up to three years of imprisonment and a fine under Section 66D of the IT Act, 2000 (Chikwe et al., 2024).

Best Practices of US to Combat OVAW

Since the largest digital corporations and tech infrastructure are located in the United States, regulations pertaining to content control and transparency might have a significant impact on the industry both domestically and globally. This strategy resulted in the creation of the US internet regulatory framework, which has few content restrictions and is consistent with the First Amendment's guarantee of free speech. In general, the values of freedom and transparency have long guided internet governance in the United States. As a result, the USA emerged as the primary location for technical infrastructure, creating the greatest tech sector that includes multinational fiber optic networks and software and hardware tech enterprises (Carasa, 2022).

The US government alongside legislation pertinent to Violence against Women Act, 1994 has operationalized the task force to combat the new form of VAW on digital space The Task Force develops recommendations for the federal government, state governments, digital p latforms, schools, and other public and private institutions in order to prevent gender-based violence that is facilitated by technology. One of the recommendations is to emphasize the connection between online misogyny and radicalization to violence. This task force provides the assistance to the victims of online violence. Through the advancing the use of technology to support victims of crime initiative, the Department of Justice's (DOJ) Office for victims of cybercrime provides victim services groups with funding of totaling $3 million (Executive Office of the President, 2022). The US also has the secret service named as National Threat Assessment Center (NTAC) that examines the online threats and motives coupled with the prior communications and their presence of attackers at online space. US spends more on funding research of the victims of online violence and make decisions according to the reporting experience and hurdles faced by the victims.

Best Practices of Singapore to Combat OVAW

In Singapore, the Penal Code and Harassment Act, 2014 has been extended to include cyber-crimes recently. In February of 2019, the Criminal Law Reform Bill was presented to the parliament with the goal of amending the Penal Code to more effectively deal with acts of violence enabled by technology. This revised the Penal Code and was passed in May 2019. The Bill said that it was intended to,

> *"Amend the Penal Code and several other Acts in order to modernize criminal offenses, stay abreast of technology advancements and new trends in crime, improve protection for children and vulnerable victims, harmonize the criminal laws, and update the sentence guidelines"* (The Commonwealth, 2023).

The website "GOsafeonline" has been developed by the Cyber Security Agency of the Ministry of Communications and Information. This offers parental tools and advice on how to utilize social networks safely. In an effort to increase awareness of cybersecurity and personal data protection, the organization has also worked with the Singapore Personal Data Protection Commission to create student activity books. The Singapore Council of Women's Organizations established the Awareness, Connect, Take Precaution, or A.C.T Against Violence portal in November 2020. It offers tools to empower women to combat harassment and violence (The Commonwealth, 2023).

Pakistan's Response to International Conventions Protecting OVAW

Budapest Convention

The primary worldwide convention on cybercrime known as the Budapest convention was drafted by the Committee of Europe and was opened for signature in Budapest in 2001 and came into force in 2004. The convention is the primary International Treaty on crimes carried out through the Internet and other computer networks, managing copyright, pornography, hate crimes, and online harassment against women. The Budapest Convention has not been signed by Pakistan. Notwithstanding, Pakistan has been a member of the United Nations Office on Drugs and Crime (UNODC) beginning around 1981. The UNODC works to combat cybercrime and aid member states in improving their cybercrime prevention and response capabilities (Mahmood, 2022). Presently, Pakistan's PECA 2016 fails to make a move against guilty parties who are not situated in Pakistan. However, the FIA could ask the authorities in the United States and Europe to gather foreign evidence and assist in locating, tracing, and preventing cyber-attacks from cyberspace, if Pakistan ratified the convention.

The Convention on the Elimination of All Forms of Discrimination against Women

A comprehensive international treaty, CEDAW was ratified on December 18,1979, by the United Nations General Assembly (Aarbakke & Nielsen, 2017). CEDAW aims to end all forms of discrimination against women and promote gender equality. It is frequently referred to as an international bill of rights for women. CEDAW's preamble reaffirms belief in the dignity and worth of fundamental human rights. It acknowledges that widespread discrimination against women persists despite numerous international efforts and instruments.

The Convention is the primary international legal tool for protecting and defending women's rights since it acknowledges gender equality and forbids discrimination against women in all contexts, incl uding the public and private spheres (Ministry of Women and Child Development, 2022). 189 states have ratified CEDAW to this point except Pakistan. Pakistan has ratified CEDAW and is committed to eliminating discrimination against women; the country faces challenges in aligning certain provisions of the convention with its legal and cultural context. In Pakistan there is a need to make efforts and reforms to ensure the full realization of women's rights in Pakistan.

The Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women

In America, the Convention of Prevention, Punishment and Eradication of VAW is a crucial step to combat gender-based violence. It establishes a legal framework for the protection of women's rights and outlines comprehensive measures for the prevention, punishment, and elimination of violence against women. States Parties commit to addressing and eradicating all forms of VAW by ratifying the convention. This convention also not yet ratified by Pakistan (Lohaus & Gutterman, 2013). The Organization of American States (OAS) ratified this regional human rights agreement, which is primarily aimed at nations in the Americas. Pakistan, as an Asian nation, is not eligible to sign or ratify this particular convention because it is not a member of the OAS.

The problem is global and its severity demands for precise legislation and instructions for punishment. It has been acknowledged by a number of instruments internationally, notwithstanding the lack of an international legal framework that particularly regulates online violence. In order to address online and ICT-facilitated violence against women, Recommendation 35 of the Committee on the Elimination of All Forms of Discrimination Against Women (CEDAW) expands the definition of violence against women beyond the physical space to include "technology-mediated environments" (World Bank, 2023).

The recent awareness regarding the emergence of online crimes at international law through the conventions have made countries to adopt criminal laws addressing cyber-crimes. Out of 190 countries in the world, 53 have introduced criminal laws related to online harassment. These laws provide punishments frequently consist of incarceration, a monetary fine, or a mix of the two. According to Bulgarian legislation, internet harassment offenses that take place in the context of domestic abuse are punishable by a higher prison term. Cyber harassment in Nigeria is punishable by three to ten years in prison under the Cybercrimes Act (World Bank, 2023).

The recent conventions internationally provide the inference that there is a dire need of international consensus to treat these offences seriously by introducing harsh punishments. The enactment of laws internationally, though, not enough to provide prevention of the cyber-crimes. The prevention of crimes could only be possible through its effective implementation and that will be sufficed to render a message that cyber-crimes and online violence against women is unacceptable. The CEDAW convention is good enough that provides the international consensus pertinent to eliminating all type of discrimination against women. However, the convention regarding online violence against women is a requisite to alarm this issue that will make countries to adopt strict laws and punishments to prevent emerging cyber-crimes.

Conclusion and Recommendations

In the light of the expanding scope of cybercrimes, adopting appropriate supervisory legislative measures and efficient law enforcement mechanisms are requisite to address the VAW issues in Pakistan. In Pakistan there is PECA 2016 for regulatory approaches to address the rising incidence of online abuse. The Parliament in 2016 passed PECA with the intention of preventing cybercrimes. However, Pakistan lacks a distinct code of conduct for cyber bullying and other forms of OVAW. Its function is limited to filling gaps; it fails to offer a distinct legal framework or address the problems brought about by the usage of the Internet, particularly deep fakes, cyber stalking, and cyber bullying. According to the report, there is no one set of legislation that addresses online violence in Pakistan (Baloch, 2016). Instead, victims' rights are addressed by the police, prosecutors, and courts by looking into recently formed laws like the PECA or existing regulations that are sporadically found in traditional criminal statutes.

Although, it can be difficult to avoid online abuse, there are some ways we can reduce it to a greater extent. It will be achievable only with the cooperation between citizens, law enforcement and the government. Raising public knowledge of cyber harassment is the most effective strategy to avoid it. The effective execution of cyber laws and increasing conviction rate will prohibit the offenders to conduct crimes including online violence. The enforcement and execution of laws can significantly decrease the rate of cyber harassment. Society must play a part in the battle against online violence by deterring offenders and preventing prejudices that impede the victim from reporting the case. The nature of crime itself is constantly changing, which demands up gradation of laws (Ghosh, 2021). A good and effective law is also one that is responsive to the needs of its citizens. In the modern era, one can determine how responsive laws are by looking at how they have failed to address the issue of providing special protection to women, the most vulnerable part of society. The law enforcement agencies in Pakistan can improve their ability to combat cyber harassment cases by implementing the following guidelines;

- The Pakistan can make cyber-legal regime effective only through specific legislations to criminalize emerging form of crimes like deep-fakes and revenge porn. There is a need to extend the existing law of PECA, 2016 to incorporate deep-fakes and revenge porn to effectively counter this menace.
- The reporting mechanism of cyber-crimes in Pakistan is obsolete and partially non-operationalized. There is no effective online portal to lodge complaint regarding online

violence. There is an absence of smooth reporting mechanism and there is a need to render Online Portal pertinent to e-filing of cyber-crimes. To effectively assist women and young girls, the online complaint portal should be updated often and should start an inquiry by requesting identity verification.

- The prosecution and conviction rates regarding the cyber-crimes against women are very low. This encourages perpetrators to commit crimes with the intention that there is nothing that can stop us. There must be a halt to this and courts should apply progressive approach to punish the perpetrators.
- The victims of online violence should have access to justice. There are 2 cyber-courts in KPK, 4 in Punjab, 2 in Baluchistan and 27 in Sindh that reflects the lackluster concern by the government of Pakistan to address the issue sincerely. As the crimes are increasing with the advancement of technology, there is a need of more courts especially in Punjab, Sindh and in Baluchistan. This will ensure the access to justice for the victims of OVAW.
- There should be a mechanism to compensate victims of online violence. This will also ensure the concern of special protection to women especially when they will feel content regarding the operationalization of cyber-laws and compensation mechanism.
- The cybercrime wing lacks the jurisdiction to entertain cases that are being committed in foreign soil. However, they are permitted to do so under Section 1(4) of PECA. There is a need to designate at least one officer in each branch who has procured specialized training regarding cyber harassment laws and procedures.
- Another yet important recommendation for FIA is to collect Gender- disaggregated data of online harassment cases particularly of PECA sections 20, 21 and 24. This will catalyze the confidence and trust of people in cyber-law enforcement and help the government in shaping policy measures to address this menace effectively.
- A dedicated desk for cyber harassment should be established inside the cybercrime wing due to the gender sensitivity demanded of complainants/victims. Officers with specific training in gender sensitivity, online harassment, and counseling services should be assigned to this desk.
- Establishing communication links between cybercrime stations and police station is important to facilitate the transfer of cases and provide clarity regarding the registration, investigation and prosecution of cases. Because online and physical areas of crime overlap. Police departments have jurisdiction over cybercrime wings in major cities of Pakistan which demands the coordination of NR3C with other departments.
- A digital system with command of privacy and confidentiality for data protection and digital security that limits access to authorized personnel only is recommended. It has been noted that in order to disclose cyber harassment case details, many complainants need assurance of confidentiality. Rule 9 of the PECA Rules specifies standards for secrecy as well as protections when it comes to women and their personal photos and videos.
- Another yet admiring recommendation is there should must be training sessions for judges on cybercrime law, internet governance and OVAW. It has been observed that judges have a basic misunderstanding of the structure and nature of the internet crimes, which leads towards poor judgments and case laws.

Despite the law's intended protections, it doesn't seem to have provided women with the essential protection they need. This paper investigated the reasons behind the failure and ineffectiveness of cyber laws in Pakistan and offers some recommendations for how lawmakers might ensure women's rights in the quickly developing technological age. It seems that women are not receiving the necessary protection from the law, which is supposed to protect them. An investigation officer for cybercrimes needs to be tech-savvy and proficient with computer devices. Unregistered apps should be prohibited by law. Unregistered and self-made software is used by hackers and is the primary cause of cybercrimes (Bhatti et al., 2021).

The agencies that investigate cybercrimes are not at the tehsil level. Additionally, district-level cyber courts do not exist. Relieving the harmed parties is an extremely difficult and intricate process. For this reason, tehsil-level government should be developed, and FIA command should extend at each tehsil level. In contrast to other nations like the USA and UK, FIA inquiry is not appropriate for cyber harassment. Pakistan cyber laws have several flaws, and it becomes difficult to incorporate legislation as a result of these flaws. Another most important concern regarding OVAW in Pakistan is over burden judicial departments so that courts find it nearly hard to keep up with the volume of work although the approach of courts in Pakistan remained progressive in protecting women from online violence as compared to the crime reporting agencies such as FIA operating under PECA.

References

Abdul Rehman vs State, 2022 SCMR 526 SC

Aarbakke, M. H., & Nielsen, R. T. (2017). *Online Violence Against Women in the Nordic Countries Online Violence Against Women in the Nordic Countries*.

Ahmed, I. (2012). *The Federal Investigation Agency*.

Asif, R., Razzaq, M., & Khadam, N. (2023). Legal Analysis of Harassment Laws in Public Places: A Case Study of Pakistan. *Islamabad Law Review*, *7*(1). https://doi.org/10.1177/2158244014543786.6

Pakistan Telecommunication (Re-Organization) Act, (1996).

Baloch, H. (2016). Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016. *APC*.

Bhatti, D. S. H., Adnan, D. S. M., & Khaliq, A. (2021). View of Cybercrimes and Role of Law Enforcement Agencies_ A Critical Analysis. *Journal of Educational Management & Social Sciences*, *2*(1).

Carasa, L. L. (2022). *"Enhancing international cooperation to fight gender inequality: A comparative analysis of the effectiveness of internet regulations in tackling online violence against women in the EU and the USA"* (Issue June).

Chidinma Favour Chikwe, Eneh, N. E., & Akpuokwe, C. U. (2024). Conceptual framework for global protection against technology-enabled violence against women and girls. *International Journal of Science and Research Archive*, *11*(2), 279–287. https://doi.org/10.30574/ijsra.2024.11.2.0415

Code of Criminal Procedure, 1989

Pakistan Penal Code, I860 (XLV of 1860), (1860).

Deeba, M. F. (2021). Protection of Women against Sexual Harassment-Social Barricades and Implementation of Laws in Pakistan. *Journal of International Women's Studies*, *22*(4), 134–151.

DRF. (2018). *Online Violence Against Women in Pakistan*. https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/UNSR-Submission-by-DRF.pdf

Electronic Transactions Ordinance, (ETO) 2002

Executive Office of the President. (2022). *Establishment of the White House Task Force to Address Online Harassment and Abuse*. https://www.federalregister.gov/documents/2022/06/22/2022-13496/establishment-of-the-white-house-task-force-to-address-online-harassment-and-abuse

Electronic Transactions Ordinance, (2002). https://doi.org/10.1016/0016-0032(67)90624-2

Fakhar Zaman vs State, 2023 PCrLJ 496 Peshawar High Court

Ghosh, S. (2021). Pakistan ' s New Cyber Policy : Welcome , But Flaws Remain. *Bank Info Security*.

Gul, F., & Anjary, F. H. (2022). Online upsurge of women victims: Exploring the barriers to reporting and awareness of PECA 2016. *Journal of Mass Communication Department, Dept …*, *26*(1), 1–16. http://jmcd-uok.com/index.php/jmcd/article/view/217%0Ahttp://jmcd-uok.com/index.php/jmcd/article/download/217/99

Haq, I. U., & Zarkoon, S. M. (2023). Cyber Stalking: A Critical Analysis of Prevention of Electronic Crimes Act-2016 and Its Effectiveness in Combating Cyber Crimes, A Perspective from Pakistan. *Pakistan's Multidisciplinary Journal for Arts & Science*, *4*(3), 43–62.

Haque, J., Syed, F., & Ilyas, F. (2013). *PAKISTAN'S INTERNET LANDSCAPE A Report by Bytes for All , Pakistan* (Issue November).

Iqbal, M. (2023). The Prevention of Electronic Crimes Act (PECA) 2016 Understanding the Challenges in Pakistan. *Siazga Research Journal*, *2*(4), 273–282. https://doi.org/10.58341/srj.v2i4.35

Khan, E. A. (2018). The Prevention of Electronic Crimes Act 2016: An Analysis. *LUMS Journal of Law*, *5*(2), 1–25.

Khan, S., Tehrani, P. M., & Iftikhar, M. (2019). Impact of PECA-2016 Provisions on Freedom of Speech: A Case of Pakistan. *Journal of Management Info*, *6*(2), 7–11. https://doi.org/10.31580/jmi.v6i2.566

Lohaus, M., & Gutterman, E. (2013). International Efforts To Combat Corruption. *The Oxford Handbook of the Quality of Government*, *17*(6), 495–515. https://doi.org/10.1093/oxfordhb/9780198858218.013.24

Mahmood, F. (2022, November). Should Pakistan sign the Budapest Convention? *The Express Tribune*.

Meera Shafi vs Federation of Pakistan 2022 SCMR 1267 SC

Ministry of Women and Child Development, G. of I. (2022). Measures To Ensure Safety And Security Of Women And Children On Online Platforms. In *National Crime Records Bureau*. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1846133

Muhammad Ajmal vs State, 2022 SCMR 274 SC

Niazi, B. K. (2022). Exploring and Critically Analyzing Cybercrime Legislation and Digital Rights in Pakistan: Challenges and Prospects. *INDUS JOURNAL OF LAW & SOCIAL SCIENNCES*, *1*(1).

Pakistan Penal Code, 1860

Prevention of Electronic Crimes Act, 2016

Punjab Protection of Women against Violence Act, 2016

The Constitution of the Islamic Republic of Pakistan, Pub. L. No. 1 (1973).

Saleem, H., Jan, J., & Areej, A. (2023). Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges. *Society, Law and Policy Review*, *1*(1), 10–22.

Sheraz Khan vs State, 2022 PCrLJ LHC

Tanveer, S. (2019). *CYBERSPACE IS BECOMING UNSAFE FOR WOMEN IN PAKISTAN*. Institute of Business Administration, Pakistan.

The Commonwealth. (2023). *Addressing Online Violence Against Women and Girls in the Commonwealth Asia Region*. https://www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/download/1097/1095/9675?inline=1

The Constitution of Pakistan, 1973

The Federal Investigation Agency Act, 1974

The Pakistan Telecommunication Act, 1996

The Protection against Harassment of Women at the Workplace Act, 2010

Tubrazy, S. J. (2020). Cyber Crimes in Pakistan. In *studocu*.

Women Development Department, G. of T. P. (2021). *Women Rights*. https://doi.org/10.1007/978-3-319-95687-9_300175

World Bank. (2023). *Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws*.

Zahoor, R., & Razi, N. (2020). Cyber-Crimes and Cyber Laws of Pakistan: An Overview. In *Progressive Research Journal of Arts & Humanities (PRJAH)* (Vol. 2, Issue 2). https://doi.org/10.51872/prjah.vol2.iss2.43