Zakariya Journal of Social Sciences (ZJSS)

ISSN Print: 2957-4897
ISSN Online: 2957-4900
Volume 5, Number 1, 2026, Pages 37 – 58
Journal Home Page
https://journals.airsd.org/index.php/zjss

An Empirical Analysis of Social Media-Driven Cyber Crimes against Women in Pakistan

Mehak[1] & Allah Bachayo[2]

[1]*MPhil Scholar, IMCS, University of Sindh, Jamshoro*
[2]*Department of Computer Science, Government College University Hyderabad, Pakistan*

ARTICLE INFO

Article History:

Received:	*January*	*08, 2026*
Revised:	*March*	*18, 2026*
Accepted:	*April*	*02, 2026*
Available Online:	*April*	*19, 2026*

Keywords:

Cyber Crimes, Social Media

ABSTRACT

The study examines the implications of social media on the psychological welfare of Pakistani women within a patriarchal framework, elucidating the cultural determinants and the significance of social capital. Social networking sites have recently risen to the top of everyone's priority list. Social networking sites are used to exchange any information. In recent times, it is clear that crimes against women are on the rise in all areas where cybercrime is rampant. However, it can be a very frustrating experience for a woman. In this research, a study was conducted to examine cybercrimes that occur against women. How does a cybercrime affect a woman? I am also planning to provide information on measures to curb the rising cybercrime against women in Pakistan. We will learn about the impact of cybercrime on the lives of women victims. This study discusses various cybercrimes, such as cyber defamation, email phishing, bitcoin fraud, data theft, and social media scams. Cybercrimes against women have been discussed for many years. The use of social media has increased as more systems have gone online, such as online education, virtual meetings, and work-from-home, which has led to cybercrime.

Corresponding Author's Email: *allah.bachayo@gcuh.edu.pk*

Introduction

The rapid growth of social media platforms has radically changed the ways people communicate, share information, and socialize around the world. Facebook, Twitter (X), Instagram, WhatsApp, and TikTok are some of the entities that are now integrated into day-to-day life in Pakistan, and therefore, open up new possibilities in education, the labor market, political mobilization, and social interactions. However, alongside these advantages, the use of digital platforms has spawned a range of cybercrimes at a disproportionately higher level among women. Social media-driven cybercrimes such as cyberstalking, online harassment, impersonation, blackmail, cyber threats, and unauthorized distribution of images

have become topical social and legal issues in the Pakistani environment. Females in Pakistan live in a highly patriarchal society, in which gender norms, cultural expectations, and power imbalance often limit their agency in real life as well as online. Instead of being used as a means of empowerment only, digital spaces tend to reflect gender-based violence in the offline world. Women are habitually harassed, intimidated, and have reputational damage, which leads to psychological trauma, social isolation, and a fear of becoming involved in online discussions. The lack of reporting of cybercrimes is also contributing to such issues as the fear of being socially stigmatized, the desire to blame the victim, the lack of awareness, and the distrust of the legal and institutional order.

The paper provides empirical research on cybercrimes against women on social media in Pakistan. It aims to examine the rates, types, and consequences of these crimes, as well as women's willingness to report cases and their trust in the law. The study will employ a quantitative research methodology, supported by a pilot study, to generate evidence to inform scholarly cognition, policy formulation, and the development of preventive and intervention strategies.

Literature Review

The second article is about social media and women in Pakistan. Social media has been well known as a two-sided tool for women in Pakistan. On the one hand, digital platforms empower people by providing access to information, economic opportunities, and channels for self-expression. Alternatively, women are also subjected to new types of surveillance, control, and abuse on these same platforms. Research has proved that the visibility of women online is often negatively targeted with patriarchal attitudes, hence strengthening the traditional gender roles and restricting their contributions to the public debate.

Cybercrimes Against Women

Types of cybercrimes against women are very diverse, with some behaviors being cyberstalking, cyberbullying, online threats, impersonation, blackmail, and non-consent sharing of pictures. Anonymity, easy access, and lax enforcement mechanisms are some of the factors that tend to promote these offenses. It has been shown that women tend to be targeted and harassed more often than men when it comes to online harassment, especially in situations where one is visible publicly, in the workplace, or in activism. The systematic review and critical analysis of the available national and international literature indicate that, although increased academic interest in the problem of cyber harassment and online violence against women exists, there are still some important gaps in the literature. Such gaps are the reasons this research is necessary and will add novel empirical and theoretical insights to the Pakistani context.

1. Absence of Combined Empirical Evaluation

A major gap in current research is the inability to integrate empirical studies that more effectively link social media-facilitated cybercrimes, women's lived experiences, and institutional actions within a single analytical framework. Numerous articles aim either to document trends in online harassment or to comment on legal provisions such as the Prevention of Electronic Crimes Act 2016 (PECA). Nevertheless, limited empirical research has examined the interactions among these domains, platform-based harm-based decision-making, and institutional processes, as well as the impact of these experiences on women's trust in legal protection (Qureshi, Abbasi, and Shahzad 2020; Khan, Irshad, and UD Din 2025). It is this discontinuity that constrains the explanatory ability of the current work.

2. The lack of Empirical Evidence of Reporting Behaviour and Barriers

Though under-reporting cyber harassment is also well-established as a problem, there exists little empirical research on the matter in Pakistan, which explores reporting behavior and the variables that deter women from receiving formal assistance. The above is frequently stated in the existing literature, and stigma, concerns about reputational damage, and institutional distrust are seldom quantified or assessed in terms of their psychological impact, the socio-cultural pressure on women, and their perceptions of enforcement effectiveness (Baig & Jafary, 2025). Consequently, the disparity between victimization prevalence and the outcome of formal justice is poorly comprehended.

3. Minimal Assessment of Legal and Enforcement Effectiveness Practice

The other critical gap concerns assessing legal effectiveness beyond doctrinal analysis. Although researchers emphasize the difficulties in implementing PECA and in enforcement agencies, few studies allow analysis of the impact of reporting and investigation procedures, victim support strategies, and case development on women's experiences and outcomes. This empirical fact is victim-centered, and it is challenging to conclude whether legal protections serve as effective deterrents, exist only on paper, or do not exist (Khan, Irshad, and UD Din 2025).

4. Inadequate Investigations of Platform-Specific and Technology-Driven Dynamics

The literature on Pakistan that addresses social media tends to generalize the concept without considering how specific features of the platform (including anonymity, forwarding, group messaging, public commenting, and content persistence) produce distinct forms of abuse. Platform affordances and algorithmic amplification are the focus of many international studies, but such research is scarce in the Pakistani context. This is a weakness that minimizes the knowledge about the ways of various platforms being used to perpetrate various forms of cybercrimes against women and constrains the formulation of platform-specific prevention measures.

5. Minimal Empirical Research of Digital Literacy as a Protection Factor

Despite recent literature identifying digital literacy as a potential preventive and empowerment-based approach, empirical testing has not examined its relationship to reduced vulnerability, enhanced reporting behavior, or improved engagement with legal protections. A majority of studies do not treat digital literacy as an empirical variable, but rather as a recommendation (Anjum, Barkat, and Shaikh 2026). This loophole limits the ability to develop evidence-based interventions to integrate education and institutional reform.

6. Requirement to have Context-Sensitive, Gender-Focused Research

Lastly, there is a wider gap in the context-specific study that is capable of explaining all socio-cultural contexts of Pakistan, such as honor-based stigma, patriarchal discourse, and gendered expectations, which define the online lives of women. Although these aspects are recognized, they are frequently discussed in abstract terms and are not empirically incorporated into analytical models (Aslam, Malik, and Khan 2023). In short, the available literature does not provide a synthesis of empirical, gender-sensitive research linking cybercrimes against women associated with social media to reporting behavior, the effectiveness of law and enforcement, platform dynamics, and digital literacy in Pakistan. The present study fills these gaps by offering an in-depth empirical analysis of patterns, risk factors, and institutional responses, thereby providing evidence-based knowledge for research, policy, and practice.

Problem Statement

Although social media is growing fast, and legal provisions have been introduced to protect women against cybercrimes, social media-based cybercrimes against women in Pakistan have been on the rise in magnitude, intensity, and effects. The education, employment, and civic engagement of women has become accessible through the use of platforms like Facebook, Instagram, WhatsApp, and X, but also platforms where women have disproportionately become victims of harassment, cyberstalking, impersonation, image-based abuse, threats, and blackmail of their reputation. These harms are not random or insignificant accidents, but an indication of gendered forms of power that are deeply rooted and are repeated and intensified using digital technologies (Aslam, Malik & Khan 2023).

Despite the enactment of the Prevention of Electronic Crimes Act 2016 (PECA) to combat offenses on online platforms, there remains a significant disparity between the legal provisions in place and the reality for women regarding safety and justice on the Internet. As empirical research suggests, women remain victims of incidents repeatedly, and a very low percentage of this victimization is reported and dealt with via the mechanisms of enforcement (Qureshi, Abbasi, & Shahzad, 2020). This implies that official status has not been directly converted into either protection or deterrence.

Sustenance of Gendered Cyber Harassment

The gendered characteristic of cyber-crimes against women is also one of the main aspects of the problem. Online harassment in Pakistan is also aimed at women and their dignity, morality, and reputation; these aspects have serious social implications in a patriarchal nation. Harassment in the form of images and impersonation is especially harmful since it aims to capitalize on the honor-related stigma and can cause social repercussions far beyond the online sphere. The available literature confirms that these harms tend to force women into self-censorship, social media abandonment, or abstinence from online opportunities, thereby negatively affecting women's access to education, employment, and social participation (Aslam, Malik, and Khan 2023; Qureshi, Abbasi, and Shahzad 2020).

Barriers and Constraints to Reporting. The second aspect of the issue is reporting and institutional response. Women who are the victims of cyber harassment are often hindered by the fear of stigmatization, fear of confidentiality, distrust of the enforcement agencies, and the complexity of the procedures. The enforcement-emphasized research demonstrates that institutional responses to PECA tend to be sluggish, insufficiently gender-conscious, and of limited capacity, which deters victims and undermines the law's crime-stopping effect (Baig & Jafary, 2025). This has led to widespread under-reporting, and the official figures reflect only a small percentage of actual victimization. Insufficient Knowledge of Effectiveness and Prevention. Another issue is the lack of combined empirical knowledge about the practical workings of social media-based cybercrimes and the effectiveness of current mitigation strategies. Much of the existing literature either documents patterns of victimization or critiques legal institutions, without providing empirical evidence of correlations among platform dynamics, women's experiences, reporting behavior, and enforcement effects. In addition, as digital literacy is emerging as a potential preventive measure, empirical evidence regarding its role in addressing women's vulnerability, their coping mechanisms, and their use of reporting mechanisms remains scarce (Anjum, Barkat, and Shaikh 2026).

Statement of the Research Problem

Hence, the main issue, which the present research will resolve, is the lack of an integrated and empirical insight into the social media-induced cyber-crimes against women in Pakistan

that can help to understand how such crimes occur on social media, why women are vulnerable and do not report them, and how effective the existing legal and enforcement frameworks are in practice. In the absence of it, policy and legal change will stay reactive, disjointed, and inadequate to empower women in their rights and safety in a fast-changing digital landscape in Pakistan.

Conceptual / Theoretical Framework

The paper takes a combined conceptual and theoretical approach to understand how cybercrimes conducted by social media against women in Pakistan take place, why women are vulnerable, and the role of legal and institutional reactions in creating the result. The phenomenon is multi-layered, as it involves various aspects of technology, gender norms, victims' decision-making, and institutional efficiency, which is why no single theory can be applied. Thus, the framework is a mixture of three complementary lenses:

1. A socio-ecological (multi-level) lens in which to contextualize cybercrime,

2. A gendered communication/patriarchy perspective to describe the influence of gender power relations on online abuse, and

3. A routine activity/opportunity lens to tell how platform affordances make cyber victimization possible.

The fourth supporting lens is legal effectiveness and procedural justice, which is used to measure the effective performance of PECA and enforcement procedures.

Socio-Ecological Lens (Multi-Level Context)

A socio-ecological approach describes cyber harassment as the result of interacting forces at multiple levels: individual, relational, community, institutional, and societal. The lens can be applied since cyber harassment in Pakistan does not occur in the virtual realm alone, but rather in a way that is informed by the offline culture, family restrictions, institutional limitations, and gender disparity.

Levels in this study

- Individual level: female digital literacy, safety skills on the Internet, privacy behaviors, coping, and awareness of reporting systems (Anjum, Barkat, and Shaikh 2026).
- Interpersonal level: the availability of women by offenders to social networks, peer groups, relationship settings, and blackmail relationships (Qureshi, Abbasi & Shahzad 2020).
- Community/platform level: social media characteristics (anonymity, forwarding, viral sharing, group chats, screenshot culture) that make things more visible and damage diffusion.
- Institutional level: reporting, FIA processes, capacity of cybercrime wing, gender sensitive, time lag in case investigation, and progression of cases (Baig & Jafary, 2025).
- The level of society: patriarchal traditions, honor-related stigma, victim-blaming, and the discourse in the society that conditions not only the patterns of harassment but also the reporting behavior (Aslam, Malik & Khan 2023).

Why it is important: The lens will enable the study to connect women's individual experiences to structural factors and institutional limitations, making it well-suited to

explaining why legal safeguards alone might not translate into safety in practice (Khan, Irshad, and Ud Din 2025).

Patriarchal Communication Lens and Gendered Power

This lens describes cyber harassment as a case of gender-based violence that is based on patriarchal power dynamics. The nature of online harassment is never randomly chosen: it frequently attacks the dignity of women, their reputation, as well as their mobility, particularly in situations where the visibility of women is a social issue. The model presumes that the digital space reproduces offline gender hierarchies in language, norms, and public judgment.

The main concepts used in this research are:

Gendered targeting: women tend to be attacked with moral policing, sexualized abuse, and reputation threats that play on honor-based stigma.

Silencing effect: harassment limits women's participation and expression, resulting in withdrawal/self-censorship (Aslam, Malik & Khan 2023).

Normalization processes: cultural narratives and victim-blaming may demoralize reporting and support impunity.

Connection to the literature on Pakistan: Research in Pakistan points to the existence of online harassment as a patriarchal practice and gendered patterns of discourse, especially in the form of abusive language, trolling, and threats that are used to embarrass women (Aslam, Malik, and Khan 2023). It is also a legal critique that women require special protection because digital harms intersect with the vulnerabilities of social life that women already possess (Khan, Irshad, and Ud Din 2025).

Routine Activity / Opportunity Lens (Platform-Enabled Crime)

The paper relies on an opportunity-based logic (commonly used in criminology) to describe how cybercrimes occur on social media. To put it simply, the three conditions, in combination with one another, increased the risk of cyber harassment:

1. motivated offender,
2. suitable target, and
3. lack of competent guardianship.

The way that the study modifies it to social media.

Motivated offender: perpetrators: perpetrators are motivated by revenge, coercion, exploitation, misogyny, or money- are common in victimization research (Qureshi, Abbasi & Shahzad 2020).

Appropriate target: women with a digital presence and social exposure can be approached; vulnerability can be heightened by weak privacy protections or by social factors that prohibit women from seeking help (Anjum, Barkat, and Shaikh 2026).

Weak guardianship: minimal platform control, poor reporting mechanisms, delayed responses from enforcers, and low deterrence due to underreporting and lateness (Baig & Jafary, 2025).

Opportunity structures of platform affordances

In this work, characteristics such as anonymity, fake accounts, forwarding, screenshotting, group broadcasting, and rapid sharing are considered opportunity structures that increase harm and reduce the cost of offense.

Legal Effectiveness and Procedural Justice Lens (Evaluating Response)

The framework also has a legal effectiveness lens, as the study assesses PECA and enforcement effectiveness. This is where the word effective is used in such a way that the presence of laws is not enough, but whether women are experiencing:

- available and transparent reporting lines,
- dignified and secretive treatment,
- timely investigations,
- fair outcomes, and
- meaningful deterrence.

Pakistan-oriented scholarship claims that PECA is significant but is typically applied reactively and in skewed ways, and that institutional constraints undermine women's protection (Khan, Irshad, and Ud Din 2025; Baig & Jafary, 2025). As such, this lens will direct the research in evaluating the gap between the law on paper and law in practice.

Combined Ideational Model in This Thesis

Key Constructs (Variables)

A. cyber-crimes (Dependent construct) instigated by social media

harassment, cyberstalking, impersonation, threatening, picture-based abuse, blackmail, defamation.

A. Prejudice against Chinese women (Risk factors)

Affordances of the platform (anonymity, forwarding, virality, fake IDs, persistent content)

Socio-cultural variables (patriarchal norms, honor stigma, victim-blaming) (Aslam, Malik, and Khan 2023)

Digital literacy/safety capacity (privacy settings, scam awareness, reporting knowledge) (Anjum, Barkat & Shaikh 2026)

C. Mediators/mechanisms

fear of being seen as a bad person, self-censorship, withdrawal, psychological distress.

reporting obstacles (fears of confidentiality, complexity of the procedure, institutional trust)

D. Moderators

age, education, urban/rural, heavy/light use of social media, platform.

E. Institutional response (Outcome-related construct)

effectiveness in enforcing, responsiveness, gender sensitive management, case proceeding (Baig & Jafary, 2025).

Proposed Research Model

The research model suggested is aimed at studying the connection between social media-related constructs of cybercrime and their effects on women in Pakistan. This model comprises independent variables representing various categories of cybercrime, one mediating psychological construct, and outcome variables concerning reporting behavior and institutional trust.

Impersonation and Blackmail

The types of cybercrimes that degrade women in a particularly unhealthy way include impersonation and blackmail. Fraudulent profiles, falsified identities, and doctored photographs are commonly used to intimidate women or bully them into silence. The blackmail capitalizes on cultural sensitivity to honor and modesty, which exposes women to psychological control and minimizes the likelihood of turning to the law.

Unlawful Transmission of Pictures

The unconsented distribution of photographs, traditionally also known as revenge pornography or image-based abuse, has become a problem of high acuity in Pakistan. This kind of behavior is taken advantage of to humiliate, dominate, or mete out punishment on women, which leads to serious emotional and social consequences. Victims face obstacles to justice despite the existence of law because of fear of exposure and institutional support.

Readiness to Report and Trust in the Legal Support

Some research reports low cybercrime incidences against women in Pakistan. Some factors that may lead to reluctance include a lack of awareness of legal rights, distrust of law enforcement agencies, lengthy legal processes, and societal stigma. Reliance on the defeasibility apparatus is central to whether victims will seek redress. In situations where confidence is low, cybercrimes go unreported, and offenders operate at will.

Research Gap

In spite of the useful findings offered by the existing literature on the topic of online harassment and gender-based violence, there is an absence of empirical, construct-based quantitative studies that also allow the investigation of multiple aspects of cybercrimes occurring through social media against women in Pakistan. This paper fills that gap by proposing a holistic model that considers the various types of cybercrime, their psychological effects, and reporting behavior. The current chapter, therefore, seeks to (a) identify the key themes in both national and global studies on online violence against women (OVAW) and cyber harassment; (b) illustrate how Pakistan-specific scholarship elucidates the pattern of cyber victimization, barriers to reporting, and judicial performance; and (c) reason why an integrated empirical study is needed where the harms of social media, lived experiences by women, and judicial performance can be connected, as opposed to viewing them as distinct phenomena. The conceptual framework of Chapter 3 is also established in the chapter, as recurring constructs such as emotional distress, trust in legal/support systems, digital literacy, platform affordances, and socio-cultural stigma are identified.

Theoretical Background

The paper is anchored on the theories explaining the causes of cybercrimes perpetrated by women through social media, their maintenance, and why the faulty application of legal protection is a common phenomenon. Its theoretical foundation integrates gender-based

violence theories, multi-level social theories, opportunity-based theories of crime, and protection/empowerment theories.

Online violence as gender based violence

Cyber harassment and online violence against women (OVAW) are better characterized as a form of gender-based violence, as unequal gender power relations predetermine it, and as it is often used to make women more visible, speechless, and have less control over their own lives. Online harassment behaviors in Pakistan are predominantly gendered, including threats, shaming, impersonation, and image-based harassment that are aimed at attacking dignity and reputation and lead to women retaliating by withdrawing from online activity (Aslam, Malik & Khan 2023; Qureshi, Abbasi and Shahzad 2020). This view takes care of the fact that online abuse does not exist in isolation from the offline society; on the contrary, it reproduces and reinforces the ideas of the existing patriarchal norms (Khan, Irshad, & Ud , 2025).

Altogether, the proposed research synthesizes: (1) gender-based violence theory to discuss the gendered aspect of hurt, (2) socio-ecological theory to discuss the presence of multi-level risk factors, (3) routine activity theory to discuss the presence of opportunity and weak guardianship depending on platform, (4) legal effectiveness theory to discuss the implementation gaps in PECA enforcing, and (5) digital literacy as a protective empowerment factor. Collectively, these lenses directly contribute to the thesis's focus on the pattern of cyber harassment, reporting conditions, and the practical effectiveness of the legal and enforcement response in Pakistan (Qureshi, Abbasi & Shahzad 2020; Aslam, Malik & Khan 2023; Khan, Irshad & Ud 2025; Baig & Jaf).

Surveillance of Applicable National and International Research

Online violence against women in international evidence

Online violence against women (OVAW) is a gendered harm that is always identified by international scholarship as a significant barrier to women enjoying a safe involvement in digital life. In all contexts, typical manifestations are cyberstalking, impersonation, sexualized harassment, threats, coordinated trolling, and non-consensual image dissemination. Researchers note that social media aggravates these harms through anonymity, the rapid reproduction of content, algorithmic visibility, and weak oversight when institutions or social structures respond slowly. Because of this, women are usually repeatedly victimized as opposed to being victimized once, and abuse spreads through various platforms and networks. Based on studies, it is found that OVAW does not just exist online; it often carries over into offline life by disrupting education, employment, conflict in the family, and even fear of physical violence, which strengthens the sense of self-censorship and withdrawal of women.

Global results of impacts and barriers to reporting

Globally, it has been shown that there are strong psychological and social effects, such as anxiety and stress, fear, and decreased well-being, particularly when the harassment is long-lasting or image-based. The victims can limit their privacy, leave their accounts, or forgo online opportunities altogether. The theme of under-reporting is a significant concern in the global arena: most of the victims fail to report because of stigma, the fear of not being believed, lack of confidence in the results, or fear of breaching their privacy and safety. Studies focusing on reporting behaviour show that institutional trust, victim-focused

practices, confidentiality, and speed of response are key related factors in the decision of women to access formal assistance.

The national victimization studies of Pakistan: trends

Pakistan-related empirical research offers context-specific evidence indicating that socio-cultural norms and gendered power relations influence cyber harassment. Studies on victimization of women indicate that women are targeted disproportionately by using social media and communication technologies, with picture-based abuse, impersonation, blackmail, and reputational attacks emerging time and again as prominent trends (Qureshi, Abbasi, and Shahzad, 2020). This is also demonstrated in this work, where victimization is commonly associated with such dynamics as honor and social stigma, which amplify the psychological damage and prevent the women from reporting or further pursuing online interactions. Moreover, socio-communication studies believe that the patriarchal discourse and the misogynistic language of the Internet allow the normalization of harassment and promote the culture of victim-blaming, which conditions the normalization of the abuse situation and limits the voice of women in the digital space (Aslam, Malik, & Khan, 2023).

Pakistan legal and enforcement literature (PECA, implementation)

The study of law in the nation pays close attention to the Prevention of Electronic Crimes Act 2016 (PECA) and the role of law enforcement institutions, including the FIA. Although PECA includes offenses related to the safety of women online (e.g., harassment, cyberstalking, misuse of identities, offenses against dignity/modesty), implementation gaps and shortcomings in reactive legal responses are evident (Khan, Irshad, and Ud Din 2025). The barriers emphasized in enforcement-oriented research include procedural complexity, inadequate investigative capabilities, delays, and inadequate gender-sensitive mechanisms that erode victims' confidence and undermine deterrence (Baig & Jafary, 2025). Taken together, these analyses imply that legal acknowledgment alone is insufficient; the quality of reporting channels, institutional sensitivity, and victim-oriented assistance have a potent influence on real-world protection.

Preventing and empowering: digital literacy in Pakistan

Digital literacy has recently been understood in the newly born Pakistan-oriented scholarship as a protective mechanism enabled by empowerment. Digital literacy can ensure safer online behavior (e.g., use of privacy settings, awareness of risks), enhance evidence preservation, and possibly guide women in more effectively navigating reporting systems. Researchers, however, state that digital literacy must be coupled with institutional change and effective enforcement to achieve meaningful harm reduction (Anjum, Barkat, and Shaikh 2026).

Analysis of the work that has been done

Discontinuity between Social, Legal, and Institutional Research

One of the greatest weaknesses of the current work is that it is typically divided along disciplinary lines. Numerous research records the experiences of cyber harassment that women undergo, as well as frequent patterns in impersonation, image-based abuse, and blackmail (Qureshi, Abbasi, and Shahzad 2020), but fail to relate them to the legal proceedings and the results of institutional processes. By comparison, legal scholarship often involves the study of laws like PECA 2016 in a doctrinal manner, not necessarily synthesizing victim experiences, barriers to reporting of abuse of children, or the realities of enforcement (Khan, Irshad & Ud Din 2025). Such segregation restricts the comprehension of the entire process of victimization to justice, which yields a partial understanding of how

cybercrimes against women are actually practiced and the responses, effective or ineffective, in practice.

Excessive dependence on Descriptive Results and Inadequate Explanatory Population

A large part of the literature is descriptive, as it aims to enumerate examples of online harms and their overall effects. Although this matter is significant, it often fails to provide a deeper explanation of why this or that harm persists and how social media characteristics (e.g., anonymity, sharing, forwarding, public commenting) affect perpetrators' strategies and victims' vulnerability. Pakistan-oriented studies have emphasized the role of patriarchal discourse and gendered communication on the Internet in causing online harassment (Aslam, Malik, & Khan, 2023). However, the implications have not always been converted into strong accounts of how socio-cultural forces are translated into platform processes and reporting effects. In the absence of this explanatory richness, studies will tend to recycle superficial descriptions rather than acquire knowledge that provides a clear directive for the intervention to be taken.

Limitations and Data Gaps Methodologically

The reliance on small samples, secondary sources, media coverage, or official case documentation is a recurring weakness. This is a big challenge since cyber harassment is highly under-reported owing to stigma, fear of tarnished reputation, and blame on the victim. There is empirical evidence that a small percentage of cases are registered and prosecuted, i.e., there could be an icy part under the water, based on official records (Qureshi, Abbasi, and Shahzad 2020). Procedural complexity and institutional delays are barriers to enforcement-oriented work, although less research empirically measures their impact on reporting rates or case trajectories (Baig & Jafary, 2025). This poses a significant evidence gap between estimates of the prevalence of victimization and other findings captured by only a few processes.

Poor Empirical Testing of PECA and Effectiveness of Enforcement

Although PECA 2016 is the core of Pakistan's response to cybercrime, available research tends to criticize it without systematically measuring its outcomes. The specialists believe that it is necessary to provide women with exclusive protection in the digital age and that the existing legislation is reactive and not responsive enough to new evils (Khan, Irshad, & Ud Din, 2025). Likewise, some weaknesses identified by enforcement studies include slow investigations, inadequate gender-sensitive mechanisms, and institutional inability (Baig & Jafary, 2025). Nevertheless, very little of the literature offers a comprehensive empirical evaluation of efficacy, including how women feel about reporting, how cases move toward a result, which aspects predetermine the outcome, and how trust and deterrence depend on enforcement practices. This loophole undermines the usefulness of the policy of current critiques.

Under-Theory of Pakistani Platform-Specific Dynamics

Research on the international level is growing to affirm that platform affordances and algorithmic systems can intensify harassment by making abusive content more visible and enabling its easy copying and replication. During the process aimed at the Pakistani audience, social media is frequently discussed in an overgeneralized way with no differentiation between the ways various platforms (Facebook, WhatsApp, Instagram, X) can facilitate different types of abuse. This is important because private messaging apps can facilitate coercion and blackmail, whereas trolling and reputational attacks are possible on public

platforms. In the absence of platform-specific analysis, research will be unable to describe patterns and prescribe platform-specific prevention efforts fully.

Digital Literacy and Prevention: Potential and Not Yet Developed

Recent research recognizes digital literacy as a protective factor that can empower women to control their privacy settings, become more aware of hazards, save evidence, and report them to authorities more efficiently (Anjum, Barkat, and Shaikh, 2026). Nevertheless, this literature is not extensive in a testable way. Most of the literature discusses digital literacy as a suggestion, but not the correlation between literacy levels and patterns of victimization, reporting behavior, or positive outcomes. This means that prevention-oriented studies are not yet robust enough to demonstrate the best outcomes, the best beneficiaries, and the best conditions.

All in all, the existing work has some good foundations but is very disjointed, descriptive, and limited in terms of methods. The most notable is the absence of systematic empirical studies that relate victimization patterns, socio-cultural dynamics, platform characteristics, reporting obstacles, and effectiveness of legal enforcement into a single evidence base. This is why in Pakistan the empirical study is required, which will be able to map the patterns of the social media-driven cyber-crimes against women and determine the level of effectiveness of PECA 2016 and the institutional mechanisms in relation to protecting women and ensuring justice in practice (Qureshi, Abbasi and Shahzad 2020; Aslam, Malik and Khan 2023; Khan, Irshad and Ud Din 2025; Baig and Jafary, 2025; Anjum, Barkat and Shaikh.

Identification of research gap

The systematic review and critical analysis of the available national and international literature indicate that, although increased academic interest in the problem of cyber harassment and online violence against women exists, there are still some important gaps in the literature. Such gaps are the reasons this research is necessary and why it will add novel empirical and theoretical contributions to the Pakistani context.

1. Absence of Combined Empirical Evaluation

A major gap in current research is the inability to integrate empirical studies that more effectively link social media-facilitated cybercrimes, women's lived experiences, and institutional actions within a single analytical framework. Numerous articles aim either to record trends in online harassment or to comment on legal provisions such as the Prevention of Electronic Crimes Act 2016 (PECA). Nevertheless, limited empirical research has examined the interactions among these domains, platform-based harms, decision-making, and institutional processes, as well as the impact of these experiences on women's trust in legal protection (Qureshi, Abbasi, and Shahzad 2020; Khan, Irshad, and Ud Din 2025). It is this discontinuity that constrains the explanatory ability of the current work.

2. The lack of Empirical Evidence of Reporting Behavior and Barriers

Though under-reporting cyber harassment is also well-established as a problem, there exists little empirical research on the matter in Pakistan, which explores reporting behavior and the variables that deter women from receiving formal assistance. The above is frequently stated in the existing literature. Stigma, concerns about reputational damage, and institutional distrust are seldom quantified or assessed in terms of their psychological impact, the socio-cultural pressure on women, and women's perception of enforcement effectiveness (Baig & Jafary, 2025). Consequently, the disparity between victimization prevalence and the outcome of formal justice is poorly comprehended.

3. Minimal Assessment of Legal and Enforcement Effectiveness Practice

The other critical gap concerns the assessment of legal effectiveness outside doctrinal analysis. Although researchers emphasize the difficulties in the implementation process in PECA and within enforcement agencies, few studies enable analysis of the impact of reporting and investigation procedures, victim support strategies, and case development on women's experiences and outcomes. This empirical fact is victim-centered, and it is challenging to conclude whether legal protections serve as effective deterrents, exist only on paper, or do not exist (Khan, Irshad, and Ud Din 2025).

4. Inadequate Investigations of Platform-Specific and Technology-Driven Dynamics

The literature on Pakistan that addresses social media tends to generalize the concept, without considering how particular features of the platform (including anonymity, forwarding, group messaging, public commenting, and content persistence) produce particular abuses. Platform affordances and algorithmic amplification are the focus of many international studies, but such research is scarce in the Pakistani context. This is a weakness that minimizes the knowledge about the ways of various platforms being used to perpetrate various forms of cybercrimes against women and constrains the formulation of platform-specific prevention measures.

5. Minimal Empirical Research of Digital Literacy as a Protection Factor

Despite recent literature identifying digital literacy as a potential preventive and empowerment-based approach, empirical testing has not examined the relationship between digital literacy levels and reduced vulnerability, enhanced reporting behavior, or improved engagement with legal protections. A majority of studies do not treat digital literacy as an empirical variable but rather as a recommendation (Anjum, Barkat, and Shaikh 2026). This loophole limits the ability to develop evidence-based interventions to integrate education and institutional reform.

6. Requirement to have Context-Sensitive, Gender-Focused Research

Lastly, there is a wider gap in the context-specific study that is capable of explaining all socio-cultural contexts of Pakistan, such as honor-based stigma, patriarchal discourse, and gendered expectations, which define the online lives of women. Although these aspects are recognized, they are frequently discussed in abstract terms and are not empirically incorporated into analytical models (Aslam, Malik, and Khan 2023).

In short, the available literature does not provide a synthesis of empirical, gender-sensitive research that links cybercrimes associated with social media against women to reporting behavior, the effectiveness of law and enforcement, platform dynamics, and digital literacy in Pakistan. The present study fills these gaps by offering an in-depth empirical analysis of patterns, risk factors, and institutional responses, thereby providing evidence-based knowledge for research, policy, and practice.

Problem Statement

Although social media is growing fast, and legal provisions have been introduced to protect women against cybercrimes, social media-based cybercrimes against women in Pakistan have been on the rise in magnitude, intensity, and effects. The education, employment, and civic engagement of women has become accessible through the use of platforms like Facebook, Instagram, WhatsApp, and X, but also platforms where women have disproportionately become victims of harassment, cyberstalking, impersonation, image-based abuse, threats, and

blackmail of their reputation. These harms are not random or insignificant accidents, but an indication of gendered forms of power that are deeply rooted and are repeated and intensified using digital technologies (Aslam, Malik & Khan 2023).

Despite the enactment of the Prevention of Electronic Crimes Act 2016 (PECA) to combat offenses on online platforms, there remains a significant disparity between the legal provisions in place and the reality for women regarding safety and justice on the Internet. As empirical research suggests, women remain victims of incidents repeatedly, and a very low percentage of this victimization is reported and dealt with via the mechanisms of enforcement (Qureshi, Abbasi, & Shahzad, 2020). This implies that official status has not been directly converted into either protection or deterrence.

Sustenance of Gendered Cyber Harassment

The gendered characteristic of cyber-crimes against women is also one of the main aspects of the problem. Online harassment in Pakistan is also aimed at women and their dignity, morality, and reputation; these aspects have serious social implications in a patriarchal nation. Harassment in the form of images and impersonation is especially harmful since it aims to capitalize on the honor-related stigma and can cause social repercussions far beyond the online sphere. The available literature confirms that these harms tend to force women into self-censorship, social media abandonment, or abstinence from online opportunities, thereby negatively affecting women's access to education, employment, and social participation (Aslam, Malik, and Khan 2023; Qureshi, Abbasi, and Shahzad 2020).

Barriers and Constraints to Reporting

The second aspect of the issue is reporting and institutional response. Women who are the victims of cyber harassment are often hindered by the fear of stigmatization, fear of confidentiality, distrust of the enforcement agencies, and the complexity of the procedures. The enforcement-emphasized research demonstrates that institutional responses to PECA tend to be sluggish, insufficiently gender-conscious, and of limited capacity, which has a deterrent effect on victims and undermines the law's crime-stopping effect (Baig & Jafary, 2025). This has led to widespread under-reporting, and the official figures reflect only a small percentage of actual victimization.

Insufficient Knowledge of Effectiveness and Prevention

Another issue is the lack of integrated empirical knowledge about the practical workings of social media-based cybercrimes and the effectiveness of current mitigation strategies. Much of the existing literature either documents patterns of victimization or critiques legal institutions, without providing empirical evidence of correlations among platform dynamics, women's experiences, reporting behavior, and enforcement effects. In addition, as digital literacy is emerging as a potential preventive measure, empirical evidence regarding its role in addressing women's vulnerability, their coping mechanisms, and their use of reporting mechanisms remains scarce (Anjum, Barkat, and Shaikh 2026).

Statement of the Research Problem

Hence, the main issue, which the present research will resolve, is the lack of an integrated and empirical insight into the social media-induced cyber-crimes against women in Pakistan that can help to understand how such crimes occur on social media, why women are vulnerable and do not report them, and how effective the existing legal and enforcement frameworks are in practice. In the absence of it, policy and legal change will stay reactive,

disjointed, and inadequate to empower women in their rights and safety in a fast-changing digital landscape in Pakistan.

Conceptual / Theoretical Framework

The paper takes a combined conceptual and theoretical approach to understand how cybercrimes conducted by social media against women in Pakistan take place, why women are vulnerable, and the role of legal and institutional reactions in creating the result. The phenomenon is multi-layered, as it involves various aspects of technology, gender norms, victims' decision-making, and institutional efficiency, which is why no single theory can be applied. Thus, the framework is a mixture of three complementary lenses:

1. a socio-ecological (multi-level) lens in which to contextualize cybercrime,

2. a gendered communication/patriarchy perspective to describe the influence of gender power relations on online abuse, and

3. A routine activity/opportunity lens to tell how platform affordances make cyber victimization possible.

The fourth supporting lens is legal effectiveness and procedural justice, which is used to measure the effective performance of PECA and its enforcement procedures.

Socio-Ecological Lens (Multi-Level Context)

A socio-ecological approach describes cyber harassment as resulting from interacting forces across multiple levels: individual, relational, community, institutional, and societal. The lens can be applied since cyber harassment in Pakistan does not occur in the virtual realm alone, but rather in a way that is informed by the offline culture, family restrictions, institutional limitations, and gender disparity.

Levels in this study

- Individual level: female digital literacy, safety skills on the Internet, privacy behaviors, coping, and awareness of reporting systems (Anjum, Barkat, and Shaikh 2026).
- Interpersonal level: the availability of women by offenders to social networks, peer groups, relationship settings, and blackmail relationships (Qureshi, Abbasi & Shahzad 2020).
- Community/platform level: social media characteristics (anonymity, forwarding, viral sharing, group chats, screenshot culture) that make things more visible and damage diffusion.
- Institutional level: reporting, FIA processes, capacity of cybercrime wing, gender sensitive, time lag in case investigation, and progression of cases (Baig & Jafary, 2025).
- The level of society: patriarchal traditions, honor-related stigma, victim-blaming, and the discourse in the society that conditions not only the patterns of harassment but also the reporting behavior (Aslam, Malik & Khan 2023).

Why it is important: The lens will enable the study to relate women's individual experiences to structural factors and institutional limitations, making it suitable for explaining why legal safeguards alone might not translate into safety in practice (Khan, Irshad, and Ud Din 2025).

Patriarchal Communication Lens and Gendered Power

This lens describes cyber harassment as a case of gender-based violence that is based on patriarchal power dynamics. The nature of online harassment is never randomly chosen: it frequently attacks the dignity of women, their reputation, as well as their mobility, particularly in situations where the visibility of women is a social issue. The model presumes that the digital space reproduces offline gender hierarchies in language, norms, and public judgment.

The main concepts used in this research are:

Gendered targeting: women tend to be attacked with moral policing, sexualised abuse, and reputation threats that play on honor-based stigma.

Silencing effect: harassment plays a role in limiting women's participation and expression, resulting in withdrawal/self-censorship (Aslam, Malik & Khan 2023).

Normalization processes: cultural narratives and victim-blaming may demoralize reporting and support impunity.

Connection to the literature on Pakistan: Research in Pakistan points to the existence of online harassment as a patriarchal practice and gendered patterns of discourse, especially in the form of abusive language, trolling, and threats that are used to embarrass women (Aslam, Malik, and Khan 2023). It is also a legal critique that women require special protection because digital harms intersect with the vulnerabilities of social life that women already possess (Khan, Irshad, and Ud Din 2025).

Routine Activity / Opportunity Lens (Platform-Enabled Crime)

The paper relies on an opportunity-based logic (commonly used in criminology) to describe how cybercrimes occur on social media. To put it simply, the three conditions, in combination with one another, increased the risk of cyber harassment:

1. motivated offender,
2. suitable target, and
3. lack of competent guardianship.

The way that the study modifies it to social media

Motivated offender: perpetrators: perpetrators are motivated by revenge, coercion, exploitation, misogyny, or money is common in victimization research (Qureshi, Abbasi & Shahzad 2020).

Appropriate target: women with a digital presence and social exposure can be approached; vulnerability can be heightened by weak privacy protections or by social factors that prohibit women from seeking help (Anjum, Barkat, and Shaikh 2026).

Weak guardianship: minimal platform control, poor reporting mechanisms, delayed responses from enforcers, and low deterrence due to underreporting and lateness (Baig & Jafary, 2025).

Opportunity structures of platform affordances.

In this work, characteristics such as anonymity, fake accounts, forwarding, screenshotting, group broadcasting, and rapid sharing are considered opportunity structures that increase harm and reduce the cost of offense.

Legal Effectiveness and Procedural Justice Lens (Evaluating Response)

The framework also has a legal effectiveness lens, as it assesses PECA and enforcement effectiveness. This is where the word effective is used in such a way that the presence of laws is not enough, but whether women are experiencing:

- available and transparent reporting lines,
- dignified and secretive treatment,
- timely investigations,
- fair outcomes, and
- meaningful deterrence.

Pakistan-oriented scholarship claims that PECA is significant but is often applied reactively and in skewed ways, and that institutional constraints undermine women's protection (Khan, Irshad, and Ud Din 2025; Baig & Jafary, 2025). As such, this lens will direct the research in evaluating the gap between the law on paper and law in practice.

Combined Ideational Model in This Study

Key Constructs (Variables)

A. cyber-crimes (Dependent construct) instigated by social media

harassment, cyberstalking, impersonation, threatening, picture-based abuse, blackmail, defamation.

A. Prejudice against Chinese women (Risk factors)

Affordances of the platform (anonymity, forwarding, virality, fake IDs, persistent content)

Socio-cultural variables (patriarchal norms, honor stigma, victim-blaming) (Aslam, Malik, and Khan 2023)

Digital literacy/safety capacity (privacy settings, scam awareness, reporting knowledge) (Anjum, Barkat & Shaikh 2026)

C. Mediators/mechanisms

Fear of being seen as a bad person, self-censorship, withdrawal, psychological distress.

Reporting obstacles (fears of confidentiality, complexity of the procedure, institutional trust)

D. Moderators

Age, education, urban/rural, heavy/light use of social media, platform.

E. Institutional response (Outcome-related construct)

effectiveness in enforcing, responsiveness, gender sensitive management, case proceeding (Baig & Jafary, 2025).

Proposed Research Model

The research model suggested is aimed at studying the connection between social media-related constructs of cybercrime and their effects on women in Pakistan. This model comprises independent variables representing various categories of cybercrime, one mediating psychological construct, and outcome variables concerning reporting behavior and institutional trust.

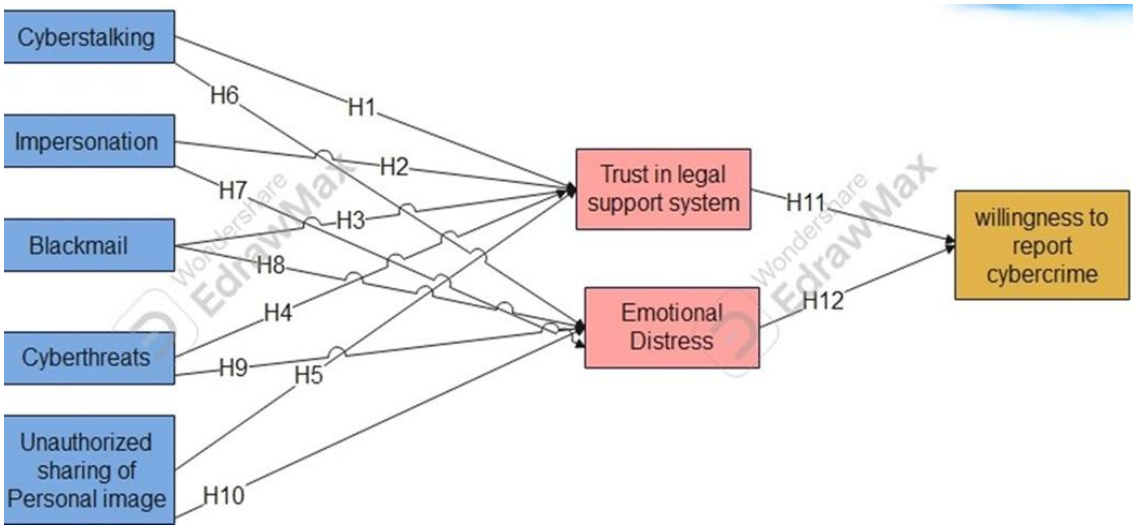


Figure No. 1: Proposed model of an empirical analysis of social media-driven cybercrimes against women in Pakistan

Independent Variables

Blackmail: Digital content or personal information used to threaten or coerce women into compliance or silence. Impersonation: It is an action performed by fabricating or stealing identities to cause harm to reputation or bullying women via the Internet.

Cyberthreats: These include direct or indirect threats of harm posted via social media. Cyberstalking: is defined as continuous, unwanted surveillance or communication via the Internet that causes fear or distress. Unauthorized Sharing of Images: Involves the intentional sharing of personal images/videos without the consent of the subject(s) with a view to shaming or controlling women.

Mediating Variable

Emotional Distress: This is the psychological consequences of cybercrimes; anxiety, fear, stress, and depression suffered by women due to cyber abuse.

Dependent Variables

Willingness to Report: This term refers to the victim's intention to report cybercrime incidents to authorities or other reporting sites. Trust Legal Support System: Refers to how much confidence women have in the legal institutions, law authorities, and cybercrime laws to deliver justice and protection.

Research Hypotheses

H1: There is a strong positive correlation between blackmail as an experience in social media and emotional distress in women in Pakistan.

H2: Emotional distress among Pakistani women is positively related to impersonation on social media.

H3: There is a significant positive correlation between cyberthreats on social media and emotional distress among Pakistani women.

H4: There is a strong positive correlation between cyberstalking on social media and emotional distress in Pakistani women.

H5: There exists a very strong positive correlation between unauthorized sharing of pictures among Pakistani women and emotional distress.

H6: There is a close negative relationship between emotional distress and willingness to report cybercrimes.

H7: Trust in the legal support system is significantly negatively correlated with emotional distress.

H8: There is a considerable positive linear relationship between trust in the legal support system and willingness to report cybercrimes.

Pilot Study

Purpose of the Pilot Study

The pilot study was conducted to evaluate the consistency and comprehensiveness of the research instrument prior to large-scale data collection. It was designed to test the internal consistency of the measurement constructs and to ensure that the questionnaire items were clear and applicable to the Pakistani context.

Sample and Data Collection

Some female social media users in Pakistan took part in a pilot survey. Purposive sampling was used to select respondents with prior exposure to social media platforms. The structured questionnaire was used to collect data using a Likert scale.

Reliability Analysis

Cronbach's Alpha was used to assess the internal consistency of each construct. The findings revealed that all constructs had high reliability, with alpha coefficients ranging from good to excellent. Constructs of blackmail, emotional distress, willingness to report, impersonation, cyberthreats, and trust in the legal system were found to be very reliable, and unauthorized image sharing and cyberstalking were found to be quite reliable.

Pilot Results Implications.

The findings of the pilot study demonstrate that the measurement tool is valid and suitable for large-scale data collection. A few word changes were made based on respondent reviews to enhance clarity. The main study will use the validated instrument to test the proposed hypotheses and research model. The overall Cronbach's alpha of the instrument was 0.881, indicating high internal consistency.

Table 1: Construct-wise Reliability

Construct	No. of Items	Cronbach's Alpha	Reliability Result
Cyberstalking	6	0.805	Good
Impersonation	5	0.891	Excellent
Blackmail	6	0.920	Excellent
Cyberthreats	6	0.886	Excellent
Trust in Legal Support System	6	0.880	Excellent
Unauthorized Sharing of Personal Images	6	0.866	Good
Emotional Distress	6	0.902	Excellent

Step 1: Data Collection

First, we have Cronbach's alpha values for each construct, which represent the internal consistency and reliability for each set of items. These values are listed as follows:

Step 2: Formula for Calculating Total Reliability

The total Cronbach's alpha is calculated by taking the mean of the individual Cronbach's alpha values. This means adding up the individual alpha values and dividing by the number of constructs.

Step 3: Calculation

Sum of Cronbach's alpha values:

0.805 + 0.891 + 0.920+ 0.886 + 0.880+ 0.866 + 0.902 + 0.899 = 7.649

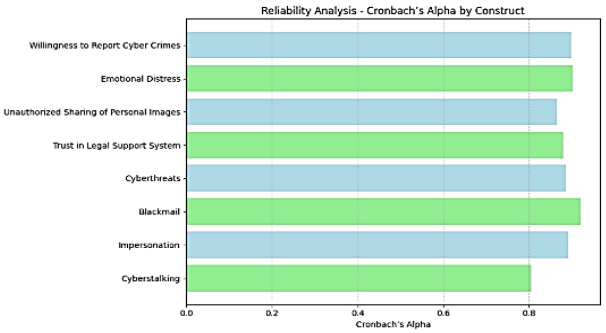
Number of constructs = 8

Total Cronbach's Alpha $= \frac{7.649}{8} = 0.881125$

Step 4: Conclusion

The total Cronbach's alpha is approximately 0.881, indicating high overall reliability of the measurement instrument and suggesting that the items within the constructs consistently measure the same underlying construct.

Figure No. 2: Reliability Analysis - Cronbach's Alpha by Construct



Here is the reliability analysis figure showing Cronbach's Alpha values for each construct. The graph visually represents the reliability of different constructs, ranging from "Good" to "Excellent," based on the values provided.

References

1. Aarbakke, MH & Nielsen, RT (2017). Online violence against women in the Nordic countries, Nordic Council of Ministers, Copenhagen.
2. Abbasi, S (2017). 'The unsocial media: Is online abuse silencing women in Pakistan?', Geo News, viewed 12 March 2025, https://www.geo.tv.
3. Ahmed, I (2012). The Federal Investigation Agency, Government of Pakistan, Islamabad.
4. Anderson, CA & Anderson, KB (2008). 'Violent video game effects on aggressive thoughts, feelings, physiology, and behavior', Journal of Experimental Social Psychology, vol. 44, no. 3, pp. 739–753.

5. Anjum, R, Barkat, A., & Shaikh, RK (2026). 'Vulnerability to Empowerment: Digital Literacy as A Shield for Women Against Cyber Harassment', Zenodo (CERN European Organization for Nuclear Research), European Organization for Nuclear Research, https://www.assajournal.com/index.php/36/article/view/1309
6. Asif, R, Razzaq, M., & Khadam, N 2023, 'Legal analysis of harassment laws in public places: A case study of Pakistan', Islamabad Law Review, vol. 7, no. 1, pp. 1–18.
7. Aslam, SB, Malik, MA & Khan, MA (2023). 'Gender and Cyber Communication: A Systematic Literature Review of Challenges Faced by Women in Pakistan', Global Language Review, vol. VIII, Humanity Only - HO, no. I, pp. 174–183, https://www.glrjournal.com/article/gender-and-cyber-communication-a-systematic-literature-review-of-challenges-faced-by-women-in-pakistan
8. Baig, K & Hadi Ali Jafary, (2025). 'Cyber Harassment and Online Violence Against Women in Pakistan: Legal Gaps and Enforcement Challenges', Journal of Political Stability Archive, vol. 3, no. 4, pp. 900–916, https://www.journalpsa.com.pk/index.php/JPSA/article/view/389
9. Baloch, H (2016). Internet rights and legislation in Pakistan: A critique on Cyber Crime Bill 2016, APC, Islamabad.
10. Bhatti, DSH, Adnan, DSM & Khaliq, A (2021). 'Cybercrimes and role of law enforcement agencies: A critical analysis', Journal of Educational Management & Social Sciences, vol. 2, no. 1, pp. 44–59.
11. Burnay, J, Bushman, B. & Larøi, F (2019). 'Effects of violent and sexualized video games on online sexual harassment', Computers in Human Behavior, vol. 99, pp. 219–227.
12. Carasa, LL (2022). Enhancing international cooperation to fight gender inequality: Internet regulation and online violence against women, MA thesis, University of Bologna.
13. Chikwe, CF, Eneh, NE & Akpuokwe, CU (2024). 'Conceptual framework for global protection against technology-enabled violence against women', International Journal of Science and Research Archive, vol. 11, no. 2, pp. 279–287.
14. Deeba, F (2021). 'Harassment at workplace and women's protection laws in Pakistan', Pakistan Journal of Gender Studies, vol. 22, pp. 45–62.
15. Digital Rights Foundation (DRF) 2018, Cyber harassment helpline annual report, DRF, Lahore.
16. Executive Office of the President 2022, National action plan to combat online gender-based violence, The White House, Washington DC.
17. Ferrara, K, Brunner, H & Whittemore, G (1991). 'Interactive written discourse as an emergent register', Written Communication, vol. 8, no. 1, pp. 8–34.
18. Ghosh, S (2021). 'Cyber violence and gender justice: Emerging legal challenges', International Journal of Law and Technology, vol. 15, no. 2, pp. 121–139.
19. Gul, S & Anjary, A (2022). 'Cyber stalking and offences against dignity under PECA 2016', Pakistan Law Review, vol. 6, no. 2, pp. 55–74.
20. Haq, R & Zarkoon, M (2023). 'Cyber laws in Pakistan: Evolution, effectiveness and reform needs', Asian Journal of Comparative Law, vol. 18, no. 1, pp. 89–108.
21. Haque, M, Khan, A & Iqbal, S (2013). 'Telecommunication regulation in Pakistan', Journal of Asian Public Policy, vol. 6, no. 3, pp. 255–270.
22. Iqbal, S (2023). 'Platform accountability and content regulation in EU digital law', European Journal of Law and Technology, vol. 14, no. 1, pp. 1–20.
23. Jamil, S (2006). Cyber-crime and legal framework, Oxford University Press, Karachi.

24. Khan, DrIA, Irshad, S & Ud Din, HSJ (2025). 'Cyber Harassment and Online Violence Against Women:A Critical Analysis of Women Protection Law Regime in Pakistan', Journal of Law & Social Studies, vol. 7, Advance Legal Research Foundation, no. 1, pp. 12–25. http://advancelrf.org/wp-content/uploads/2025/04/Vol-7-No.-1-2.pdf
25. Khan, S, Rehman, A & Ahmed, Z (2019). 'Cybercrime legislation and enforcement challenges', Pakistan Journal of Criminology, vol. 11, no. 3, pp. 23–40.
26. Kwetishe Joro, M et al. (2014). 'Gender issues and ICT for development', Information Technologies & International Development, vol. 10, no. 4, pp. 17–32.
27. Lakoff, R (1975). Language and woman's place, Harper & Row, New York.
28. Lohaus, M & Gutterman, E (2013). 'Violence against women and international law', Human Rights Quarterly, vol. 35, no. 1, pp. 1–28.
29. Mahmood, S (2022). 'Cybercrime governance and international cooperation', Journal of International Security Studies, vol. 9, no. 2, pp. 101–120.
30. Ministry of Women and Child Development 2022, Handbook on cyber violence against women, Government of India, New Delhi.
31. Mohsin, M (2016). 'The cyber harassment of women in Pakistan', The Diplomat, viewed 14 March 2025.
32. Navneet, K 2018, Cybercrime and digital victimization, Sage Publications, New Delhi.
33. Niazi, A 2022, Role of FIA in combating cybercrime in Pakistan, National Defence University Press, Islamabad.
34. Nurse, JRC 2018, 'Cybercrime and society', Computer Law & Security Review, vol. 34, no. 5, pp. 1121–1134.
35. Okoli, C & Schabram, K 2010, 'A guide to conducting a systematic literature review', Sprouts Working Papers, vol. 10, no. 26, pp. 1–50.
36. Pakistan Penal Code 1860, Government of Pakistan.
37. Pakistan Telecommunication (Re-Organization) Act 1996, Government of Pakistan.
38. Qureshi, SF, Abbasi, M & Shahzad, M 2020, 'Cyber Harassment and Women of Pakistan: Analysis of Female Victimization', Journal of Business and Social Review in Emerging Economies, vol. 6, no. 2, pp. 503–510, https://www.publishing.globalcsrc.org/ojs/index.php/jbsee/article/view/1150
39. Raza, A et al. 2019, 'ICT interventions for women empowerment in Pakistan', Human–Computer Interaction for Development, vol. 5, no. 1, pp. 33–49.
40. Saleem, A, Yousaf, Z & Khan, R 2023, 'Cybercrime victimization and legal response in Pakistan', Pakistan Journal of Social Sciences, vol. 43, no. 2, pp. 201–218.
41. Tannen, D 1990, You just don't understand: Women and men in conversation, Ballantine Books, New York.
42. Ubair, M 2020, 'Digital victimization and cyber abuse among women', Journal of Gender Studies, vol. 29, no. 4, pp. 456–470.
43. United Nations 2018, Report of the Special Rapporteur on violence against women, UN General Assembly, New York.
44. World Bank 2023, Technology-facilitated gender-based violence: Global evidence and policy responses, World Bank Publications, Washington DC.