



ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL

Available Online: <https://assajournal.com>  
Vol. 05 No. 02. April-June 2026. Page# 2727-2740  
Print ISSN: [3006-2497](https://doi.org/10.5281/zenodo.21245942) Online ISSN: [3006-2500](https://doi.org/10.5281/zenodo.21245942)  
Platform & Workflow by: [Open Journal Systems](https://doi.org/10.5281/zenodo.21245942)  
<https://doi.org/10.5281/zenodo.21245942>



**Regulating Digital Hate Speech: A Linguistic Analysis of Online Abuse Against Women and Its Policy Implications in Pakistan**

**Hafeez ul Rehman**

Lecturer (English) Education Department Government of Sindh

[hafeez9696rehman@gmail.com](mailto:hafeez9696rehman@gmail.com)

**Waliullah Dahri**

Lecturer (English) Sindh Agriculture University Tandojam

[waliullahdahri@gmail.com](mailto:waliullahdahri@gmail.com) ORCID: <https://orcid.org/0009-0005-2479-2326>

**Kashif Shaikh**

Instructor (English) IBA Community College Jacobabad

**Abstract**

*Social media has become an important place for public discussion in Pakistan, but it has also become a common place for abuse aimed at women. This study is a qualitative investigation of how language is used to harass and silence women on Pakistani social media, and whether current law protects women from this kind of abuse. The study is based on a close reading of public posts and comments collected from four major platforms used in Pakistan: TikTok, Facebook, X, and Instagram. It looks for repeated patterns in how online abuse against women is written, including shame based insults, sexual insults, attacks on a woman's character, group harassment by many accounts at once, and switching between Urdu and English to make insults stronger or harder to detect. The findings show that this abuse is not random rudeness. It follows clear patterns and works to control women and push them out of public life, both online and offline. The study also reviews the main law on this issue in Pakistan, the Prevention of Electronic Crimes Act (PECA) of 2016 and its 2025 Amendment. It finds that although the law does list some relevant offences, unclear definitions, weak enforcement, low conviction rates, and the 2025 Amendment's focus on false information and state institutions have left most everyday online abuse against women unaddressed. In some cases, the law has even been used against women who spoke publicly about their own harassment. The study ends with suggestions for reform, including a clearer legal definition of gender based online harassment, better trained investigation units, easier and safer ways to report abuse, stronger rules for social media platforms, and more public education on digital safety.*

**Keywords:** *online gender based violence, digital hate speech, cyber harassment, PECA, discourse analysis, Pakistan, social media, women*

## 1. Introduction

Over the past decade, more people in Pakistan have gained access to the internet and smartphones. Social media platforms such as Facebook, X (formerly Twitter), Instagram, and TikTok are now central to political debate, work, entertainment, and personal expression. For many Pakistani women, this growth has created useful chances for education, business, journalism, and public involvement. At the same time, reports from civil society groups such as the Digital Rights Foundation (DRF) and Media Matters for Democracy show that women who are visible online in Pakistan often face heavy, targeted abuse. This ranges from sexual insults and threats of rape to organised smear campaigns, the sharing of private information without consent, and edited or non-consensual images.

This abuse does not use random language. It draws on specific cultural ideas about honour, shame, and moral behaviour that are common in Pakistani society, and it often spreads through switching between Urdu, English, and regional languages, through images and memes, and through groups of accounts acting together. Understanding exactly how this abuse is built in language is an important first step toward writing laws and policies that can address it. However, much of the existing legal and policy writing on cyber harassment in Pakistan does not look closely at how the abuse is actually worded. This study aims to fill that gap by closely analysing real posts and comments on major social media platforms, and by reviewing how well Pakistan's cyber crime laws work in practice.

### 1.1 Background and Rationale

Pakistan ranks poorly on international measures of internet freedom and online safety for women. Independent monitors such as Freedom House have repeatedly described the country's online environment as limited for both political speech and personal safety (Freedom House, 2025). Since 2016, the main law covering online conduct has been the Prevention of Electronic Crimes Act (PECA), which makes offences such as cyberstalking and the unauthorised sharing of a person's images illegal, and which was significantly changed in January 2025 (Government of Pakistan, 2016, 2025). PECA was partly explained, when first passed, as a tool to protect women and children from online harm. However, rights groups have long argued that its unclear wording, and its use for other political goals, most recently the policing of "fake news" and harm to the reputation of state institutions under the 2025 Amendment, have made it a blunt tool (Human Rights Watch, 2025; International Federation of Journalists, 2025). It does little to address the specific, repeated forms of gendered online abuse, and in some documented cases it has been used against the very women who report such abuse (Amnesty International, 2025). A focus on language is important here because harassment is, above all, an act of communication. The exact words, tone, images, and methods used to insult, threaten, or silence women online shape both the harm caused and how hard it is to turn that harm into a clear legal offence. Legal definitions built around narrow acts such as "stalking" or "defamation" may fail to cover harassment that works through hints, group mockery, or the strategic use of jokes and memes. A qualitative study of real posts and comments is therefore well suited to showing the actual texture of the problem, which numbers alone cannot show.

### 1.2 Objectives

1. To study how women are abused and harassed through language on social media in Pakistan.

2. To assess whether current laws adequately deal with online abuse against women.
3. To suggest policy improvements based on the findings of the study.

### **1.3 Research Questions**

1. How is language used to harass women on social media in Pakistan?
2. Do current laws and policies provide sufficient protection against online abuse of women?
3. What policy changes can help prevent and address online abuse against women in Pakistan?

### **1.4 Significance of the Study**

This study adds to three related fields: language study and discourse analysis, gender studies, and technology policy. From a language point of view, it offers a clear list of the ways online abuse against women is worded in the Pakistani context, based directly on real posts and comments, adding to growing international research on the language of technology facilitated gender based violence. For policymakers, it offers evidence based directly on the language of abuse itself, rather than on abstract legal categories, to help write clearer and more workable laws. For civil society groups and platform safety teams, it points to the specific cultural language patterns that automated moderation systems, which are usually trained mostly on English language data, are likely to miss in mixed Urdu and English content. Finally, by looking closely at the 2025 PECA Amendment, the study speaks directly to an ongoing and unresolved policy debate in Pakistan about how to balance stopping online harm with protecting free speech.

### **1.5 Scope and Limitations**

This study is qualitative and descriptive rather than statistically representative. It focuses only on public posts and comments in Urdu and English found on four platforms widely used in Pakistan: TikTok, Facebook, X, and Instagram. Private messages, closed groups, and non-public content are not part of this study. Its findings describe common patterns rather than exact figures for how often each type of abuse occurs. Regional languages such as Sindhi, Pashto, Punjabi, and Balochi are mentioned where they appear in the data, but they are not studied in the same depth as Urdu and English, and this is noted as an area for future research. For ethical reasons, no exact abusive text taken from real accounts is shown in this report. The examples given are anonymised and reworded so that no identifiable person or exact wording is repeated, though they are based on patterns documented in the collected posts and comments and supported by existing published research and helpline reports.

## **2. Literature Review**

### **2.1 Language, Discourse, and Online Abuse**

Critical discourse analysis, developed by scholars such as Fairclough (1995) and Van Dijk (1993), treats language not simply as a neutral way of passing on information, but as a place where social power is built, repeated, and challenged. Van Dijk's (1993) work on discourse and racism developed methods for tracing how bias becomes built into everyday word choices, such as which words are chosen, how pronouns are used, and how ideas are framed. These methods have since been used to study online hatred toward women and other hate speech. From this view, abusive language aimed at women online is not simply a matter of individual rudeness. It works to reassert unequal treatment between men and women, to police women's presence in

public spaces, including online spaces, and to discourage women who go against accepted ideas of proper female behaviour.

Citron's (2014) legal writing on "cyber civil rights" reframed online harassment of women as an equality problem rather than as a simple personal conflict. She argued that the repeated, networked nature of online abuse causes harms, including damage to reputation, mental health, income, and career, that older harassment or defamation laws were not built to address (Citron, 2014). This reframing is directly useful for the Pakistani context, where much of the existing legal system, including parts of the Pakistan Penal Code on defamation and "modesty," was written before the internet existed and was not designed with networked, anonymous, and coordinated harassment in mind.

## **2.2 Technology Facilitated Gender Based Violence (TFGBV)**

International groups such as UN Women and the Association for Progressive Communications use the term technology facilitated gender based violence to describe a wide range of online behaviour, from unwanted sexual comments to image based abuse, the sharing of private information, and organised harassment campaigns (Sexual Violence Research Initiative [SVRI] et al., 2024). This type of abuse affects women and gender diverse people more than others, and it is often linked to, rather than separate from, offline violence (SVRI et al., 2024). Research comparing different countries consistently finds that abuse aimed at women combines general hostility with content aimed specifically at their gender, such as sexual insults, threats of sexual violence, attacks on appearance and morality, and attempts to expose or invent sexual wrongdoing in order to damage a woman's reputation within her family and community. Studies and helpline data from Pakistan, including the Digital Rights Foundation's long running Hamara Internet (Our Internet) programme and its Cyber Harassment Helpline, support this pattern (Digital Rights Foundation, n.d.). They also show that harassment is often used as a tool to silence women journalists, human rights defenders, and politically active women simply because they are publicly visible.

## **2.3 Gendered Online Abuse in the Pakistani Context**

Research and reporting focused on Pakistan point to several repeated features of online abuse against women. First, words related to honour and shame, such as *izzat* (honour), *sharam* (shame), and *gairat* (family honour), are often used online to threaten women with social or family consequences for being visible on the internet. This effectively brings offline social control methods into digital spaces. Second, accusations about a woman's moral character, including calling her "characterless" or "vulgar," are used to undermine her right to speak, especially if she is a journalist, activist, or public figure who criticises state institutions or supports women's rights. Third, harassment is often organised rather than done by one person alone, with networks of accounts, sometimes linked to political parties or ideological groups, joining together to target one woman at the same time. Fourth, switching between Urdu and English, along with the use of Roman Urdu (Urdu written in Latin letters), is used both to make insults stronger, since some insults carry more force in Urdu than their closest English equivalent, and to avoid detection by English language moderation systems, which are less able to identify abusive Urdu or Roman Urdu text.

Reports from Reporters Without Borders and the Committee to Protect Journalists have documented that women journalists in Pakistan often face a mix of professional attacks, such as

being called "lifafa" journalists, meaning bribed or bought, and gendered sexual harassment, which often increases when they cover politically sensitive topics (Committee to Protect Journalists, 2025; Reporters Without Borders, 2025). This double target, attacking both a woman's professional credibility and her sexual respectability at the same time, is treated in this study as a repeated pattern rather than as a coincidence.

#### **2.4 The Legal and Policy Landscape**

PECA 2016 was Pakistan's first full cyber crime law (Government of Pakistan, 2016). It made several offences illegal, including unauthorised interception of communications, cyberstalking under Section 24, electronic forgery, and cyber terrorism, and it gave the Federal Investigation Agency's Cyber Crime Wing the main responsibility for investigating these offences (Government of Pakistan, 2016). From early on, women's rights groups welcomed the Act's clear naming of cyberstalking and image based offences, while also criticising its unclear definitions, weak support systems for victims, and the FIA's limited resources and limited sensitivity to gender issues when handling complaints (Digital Rights Foundation, 2016).

In January 2025, Parliament passed the Prevention of Electronic Crimes (Amendment) Act, 2025 (Government of Pakistan, 2025). Independent legal reviews and human rights groups, including Human Rights Watch and the National Commission for Human Rights (NCHR), describe the amendment as focused mostly on stopping "fake or false" information and protecting the reputation of state institutions such as the judiciary, the armed forces, and parliament, with penalties of up to three years in prison (Human Rights Watch, 2025; National Commission for Human Rights, 2026). The amendment replaced the FIA's Cyber Crime Wing with a new National Cyber Crime Investigation Agency (NCCIA) and created new regulatory bodies, most notably a content regulation authority, referred to in different sources as the Social Media Protection and Regulatory Authority or the Digital Rights Protection Authority, with the power to order the removal of "unlawful" or "offensive" content, and in some accounts a Social Media Protection Tribunal to handle disputes (Government of Pakistan, 2025; Human Rights Watch, 2025).

Importantly for this study, several independent reviews agree that the 2025 Amendment does little to strengthen protection specifically against gendered online harassment, and may in some ways make things worse for women who speak publicly about harassment (International IDEA, 2025). Reporting from International IDEA and related sources notes that DRF helpline data show women make up most harassment complainants, yet the same sources describe how the broad and unclear "fake or false information" offence has been used, and could continue to be used, against women, including women journalists, who publicly describe their experiences of harassment (International IDEA, 2025; Digital Rights Foundation, n.d.). This puts them at risk of being charged with "spreading false information" instead of being protected. This gap between the law's stated purpose and its real world use is a central problem examined by Research Question 2 of this study.

#### **2.5 Research Gap**

Existing Pakistani research and advocacy writing tend to fall into two separate groups. One group offers legal and policy analysis of PECA without paying close attention to the actual language of the harassment being regulated. The other group offers sociological or journalistic accounts of online abuse against women, describing how common it is and its effect on wellbeing, without closely analysing how it is structured in language or connecting that structure back to gaps in the

law's wording. This study aims to close that gap. It uses discourse analysis methods to describe how the abuse is built in the language of real posts and comments, and then compares the resulting patterns directly against the specific offences, definitions, and enforcement systems in PECA 2016 and the 2025 Amendment, in order to show precisely where legal wording fails to match the real linguistic patterns of gendered online abuse.

### **3. Research Methodology**

#### **3.1 Research Design**

This study uses a qualitative, interpretive research design based on critical discourse analysis of social media posts and comments. A qualitative approach fits this study because the research questions are about meaning and process, that is, how abusive language is built and how it functions, rather than about the statistical rate of particular behaviours. The study is exploratory and works toward building theory. It uses Fairclough's three-part model of discourse, which looks at text, discourse practice, and social practice, to move from close reading of language toward broader claims about the social role of online abuse against women and its link to law and policy. The analysis is based entirely on publicly visible posts and comments; no interviews or surveys were conducted for this study.

#### **3.2 Data Sources and Sampling**

The data for this study is a purposefully built collection of publicly visible, gender directed abusive posts and comments taken from four major platforms used in Pakistan: TikTok, Facebook, X, and Instagram. The focus was on posts and comment threads involving Pakistani women journalists, human rights defenders, entertainers, and ordinary users who experienced visible group harassment. Purposeful and snowball sampling were used to find relevant posts and threads, starting with cases already documented by DRF, Media Matters for Democracy, and international press freedom groups, and expanding by following hashtags, reply chains, and comment sections on relevant posts.

Sampling covered a range of content types across the four platforms, including X posts and reply threads, Facebook post comments, Instagram comment sections, and TikTok video comments. As is standard in qualitative research, sampling continued until the point of saturation, meaning until new posts and comments stopped producing new patterns.

#### **3.3 Data Collection Procedures**

Data were collected through careful, ethically supervised review of publicly available posts and comment threads on the four platforms. No private messages, closed groups, or non-public content were accessed. For each platform, posts and comments were copied into a secure working file along with basic contextual information, such as the type of post that triggered the responses and the approximate number and timing of abusive replies, without recording any information that could identify the individuals involved. This contextual information supported the analysis of patterns such as coordinated group harassment, described in Section 4.5.

#### **3.4 Data Analysis**

The collected posts and comments were studied using critical discourse analysis, looking at word choice, such as sexual or dehumanising language, communication strategies such as threats, hints, and sarcasm, switching between Urdu and English, and how text worked together with images, emojis, or memes. Content was grouped into codes describing recurring linguistic strategies, and these codes were then organised into broader categories through repeated

review of the data. The resulting categories were then compared against the specific offences, definitions, and institutions set out in PECA 2016 and the 2025 Amendment, to see how well they matched and where gaps existed.

### **3.5 Ethical Considerations**

This study followed accepted ethical guidelines for internet research and research on gender based violence. All examples shown in this report are anonymised and reworded rather than copied word for word, to avoid spreading harmful content again, to protect the identity of both the women targeted and the people who posted the abuse, and to avoid causing further distress to anyone who may recognise the situation described. Usernames, profile pictures, and any other identifying details were removed from the working data during collection. No content from private accounts, closed groups, or direct messages was accessed or used at any stage of this study.

### **3.6 Trustworthiness and Rigour**

The study's findings were checked for trustworthiness through repeated review of the coded data, a clear record of how coding categories were built and revised, and comparison of patterns across all four platforms to check that findings were not specific to just one platform. Where possible, a second reviewer checked a sample of coded posts against the category definitions to confirm consistency. The researcher also stayed aware, throughout the study, of how their own language background and familiarity with these platforms could shape what is noticed and how it is understood in this kind of language based research.

## **4. Findings: The Linguistic Construction of Online Abuse Against Women**

Analysis of posts and comments collected from TikTok, Facebook, X, and Instagram showed five repeated, and often overlapping, patterns through which women are abused and harassed online in Pakistan. These are described below using anonymised, reworded examples. No exact harassing text from real accounts is repeated here.

### **4.1 Honour- and Shame-Based Shaming**

The most culturally specific pattern found was the use of honour and shame language, such as *izzat* (honour), *sharam/besharmi* (shame/shamelessness), and *gairat* (family honour), to present a woman's ordinary post, photo, or opinion as a failure of family or community honour. Comments of this kind, found across all four platforms, suggested that a woman's family should be ashamed of her, or that her father or brothers should "control" her, in response to something as simple as posting a photo or sharing an opinion. In language terms, this pattern shifts attention away from what a woman actually posted, and toward her, and her family's, moral standing. It also suggests that male relatives should be the ones to control her behaviour. This repeats offline patterns of male authority within what is meant to be a public, individual space online.

### **4.2 Sexualised Insults and Threats**

A second major pattern involves openly sexual language: insults that reduce a woman's worth to her sexual behaviour or availability, and direct or indirect threats of sexual violence. This pattern appeared most often in the comment sections of posts by women journalists and activists, frequently appearing soon after a post containing political commentary that had nothing to do with gender. In practice, this kind of language works to force silence rather than simply to offend. Threats are often timed to follow a specific post, presenting sexual violence as the expected result of the woman continuing to post publicly.

### **4.3 Character Assassination and Moral Delegitimisation**

A related but separate pattern involves comments that attack a woman's general moral character, calling her "vulgar," "immodest," "westernised," or dishonest, in order to undermine her professional or political posts rather than to respond to what she actually said. This was especially common in comments on posts by women journalists and politicians, where replies claimed the woman was "characterless" or being paid ("lifafa") whenever she posted critical commentary. A smaller number of comments used religious language, such as accusing a woman of lacking faith or moral values, as one version of this same character based attack. Across all these variations, the underlying pattern is the same: a personal moral attack is used in place of a real response to what the woman actually posted, shifting attention from her work to her character.

### **4.4 Coordinated Pile-On Harassment**

Rather than single hostile comments, much of the harassment found in this study was organised: groups of accounts, sometimes traceable to known political or ideological networks, posting similar or identical abusive comments within a short period of time under one triggering post. In language terms, these coordinated attacks were marked by repeated set phrases and shared hashtags, suggesting planning rather than a spontaneous reaction. This pattern was found on all four platforms, though it was most visible on X, where reply threads made the volume and timing of coordinated comments easiest to observe. A single hostile comment can be ignored, but hundreds of similar comments arriving within hours create a feeling of overwhelming, inescapable public condemnation.

### **4.5 Code-Switching and Platform-Evasion Strategies**

Finally, the data showed heavy switching between English, Urdu, and Roman Urdu (Urdu written using Latin letters) within comments and replies. Certain culturally loaded insults appeared to carry much more force in Urdu than their closest English equivalent, and comments often switched into Urdu or Roman Urdu specifically to make an insult stronger after starting in English. In other cases, this switch seemed to be used to avoid detection by platform moderation systems, since comments in Urdu or Roman Urdu that would likely be removed if posted in English often remained visible for longer. This strategy of avoiding detection has direct relevance for policy, discussed further in Section 6.

### **4.6 Summary of Findings for Research Question 1**

Together, these patterns show that online abuse against women in Pakistan is not simply general rudeness that happens to target a woman. It is a repeated, culturally specific form of language that draws on honour, shame, sexuality, and morality to reassert control over women, that is often organised rather than spontaneous, and that uses language switching to increase harm while avoiding both platform moderation and, as shown in the next section, the categories recognised by current law.

## **5. Legal and Policy Analysis**

### **5.1 Relevant Provisions of PECA 2016**

PECA 2016 remains the main law covering cyber offences in Pakistan. Its most directly relevant provision is Section 24, which makes cyberstalking illegal. This is defined broadly enough to cover repeated contact, monitoring, or communication meant to force, frighten, or harass a person, with harsher penalties when the victim is a woman or a minor (Government of Pakistan, 2016).

Other provisions cover the unauthorised use of a person's identity information, unauthorised interception of communications, and the harmful sharing of a person's photos or videos without consent, which is often used in image based abuse cases (Government of Pakistan, 2016). The Federal Investigation Agency's Cyber Crime Wing was named as the main body responsible for investigating these offences.

Existing legal commentary, supported by long standing civil society criticism, points to several structural weaknesses in this system, even before the 2025 Amendment (Digital Rights Foundation, 2016). These include definitions of harassment and cyberstalking that are broad enough to leave room for wide discretion, but not specific enough to reliably cover coded, culturally embedded, or organised abuse of the kind described in Section 4; long-term underfunding and limited digital forensic ability within investigation units, especially outside major cities; low reported conviction rates compared to the number of complaints filed; and a widely reported pattern of victims facing further distress during the reporting process, in which women reporting harassment face doubt, delay, or discomfort from mostly male investigating officers, which discourages future reporting.

### **5.2 The 2025 Amendment and Its Implications for Women**

The Prevention of Electronic Crimes (Amendment) Act, 2025, passed in January 2025, significantly shifted the law's priorities (Government of Pakistan, 2025). Its most notable new provision makes it a crime to spread information that is known or believed to be "fake or false" and likely to cause fear, panic, disorder, or unrest, or to harm the reputation of individuals or institutions including the judiciary, the armed forces, and parliament, with penalties of up to three years in prison and large fines (Government of Pakistan, 2025). The amendment also replaced the FIA's Cyber Crime Wing with a new National Cyber Crime Investigation Agency, and created new content regulation bodies with the power to order the removal of "unlawful" or "offensive" material, along with a tribunal for handling disputes (Human Rights Watch, 2025).

For this study's second research question, three points stand out. First, the amendment's central offence, the broad and unclear "fake or false information" rule, was not written with gendered online harassment in mind, and does not create any new, clearer definition of gender based online abuse (International IDEA, 2025). The cyberstalking and harassment provisions from the 2016 Act remain largely unchanged. Second, several human rights organisations and legal analysts have documented that this unclear "false information" offence has already been used, or clearly could be used, against women, including journalists, who publicly report their experiences of online harassment (Human Rights Watch, 2025; International Federation of Journalists, 2025). This can happen when those accused of harassment, or state actors, describe such reports as damaging to reputation or as unproven claims, which turns the law's protective purpose on its head. Third, limiting the right to appeal largely to higher courts, and giving new government appointed bodies the power to remove content, raises concerns about access for ordinary complainants, including harassment victims with limited money, who are far less able to pursue complex, high court level appeals than well funded state or company actors (National Commission for Human Rights, 2026).

Data from civil society groups, cited in recent human rights reporting, shows that women make up a large majority, cited at around 58 percent in Digital Rights Foundation helpline figures, of cyber harassment complainants (Digital Rights Foundation, n.d.; International IDEA, 2025). This

shows that gendered abuse makes up most of the underlying problem PECA was originally meant to solve, even though the law's most recent changes have focused on other issues.

### 5.3 Mapping Linguistic Findings Against Legal Categories

Comparing the findings in Section 4 directly against PECA's legal categories shows specific points where they do not match:

- Honour/shame shaming and character assassination (4.1, 4.3) rarely involve the repeated, targeted contact needed to meet a narrow reading of "cyberstalking." They more closely resemble defamation or harassment in a scattered, one time, or crowd based form, which current provisions do not clearly cover.
- Coordinated group harassment (4.4) involves large numbers of separate, often short-lived or anonymous accounts, each posting only once or twice. This pattern is hard to prosecute under a system built around identifying and charging a single stalker or harasser, and it strains the limited investigation resources described in existing legal commentary.
- Language switching and Roman Urdu abuse (4.5) is not addressed by any specific law or rule requiring platforms or investigators to build the ability to detect Urdu language abuse, leaving a documented gap in enforcement.
- Reporting itself, as described throughout Section 4, is made more difficult by the 2025 Amendment's "false information" offence, which, as noted in 5.2, can put women who publicly describe their harassment at risk of being accused or prosecuted in return. This directly discourages the reporting that effective enforcement depends on.

### 5.4 Answering Research Question 2

Based on the evidence gathered, current Pakistani law offers only partial and unevenly enforced protection against online abuse of women. PECA 2016 does make core acts such as cyberstalking and the non-consensual sharing of images illegal, and it has allowed some successful prosecutions, giving it value as a starting point. However, the law's definitions do not clearly match the coordinated and culturally specific patterns of abuse identified in this study. Enforcement is limited by resource constraints and by practices that are not sensitive to gender, which cause further distress to victims and reduce reporting. The 2025 Amendment, rather than closing these gaps, has shifted legal and institutional attention toward disinformation and reputational harm offences that mainly serve state and elite interests, while creating new legal risk for women who speak publicly about their own harassment. Overall, the law is formally present but not enough on its own, and in some documented ways it works against its stated goal.

## 6. Discussion

The findings of this study suggest that online abuse against women in Pakistan should be understood as an organised, linguistically skilled form of social control, rather than as scattered rudeness. The honour and shame pattern described in Section 4.1 shows that digital space in Pakistan has not replaced offline patriarchal norms, but has instead become another place where those norms are enforced, often by anonymous or loosely organised accounts rather than by known family members. This makes the abuse both more spread out and harder to address legally than similar offline behaviour.

The mismatch between this language pattern and PECA's legal categories helps explain a wider problem: much of the harassment documented in this study, such as a wave of coded insults from dozens of accounts, does not clearly fit the narrow definition of "cyberstalking" that investigators tend to apply, since it does not involve one identifiable person making repeated contact. This gap between real harm and a legally recognised offence fits with Citron's (2014) wider argument that harassment law built around a single attacker making repeated contact struggles to capture networked, crowd based abuse. This study finds this problem is common in the Pakistani context, where posts and comments show group based attacks with no single, easily identified harasser.

The 2025 Amendment's focus on disinformation and institutional reputation looks, against this background, like a missed opportunity for protecting women. The legislative and institutional effort needed to create new investigation agencies and regulatory bodies was clearly available, but it was directed toward offences with limited relevance to the gendered harassment that helpline data suggests is the main real world problem. The finding that the amendment's unclear "false information" offence can be, and reportedly has been, used against women who report harassment is especially important. It suggests the risk is not simply that lawmakers overlooked the issue, but that the law can actively, even if unintentionally, discourage the reporting that any system of enforcement depends on.

These findings should be read with some caution. The study's qualitative, purposefully sampled design means its findings describe common patterns rather than exact rates of occurrence. The data, drawn only from publicly visible posts and comments, may also understate forms of abuse that happen through private messages or closed groups, which other research suggests can be equally or more severe than public harassment. Future research using larger, more systematically sampled data, and comparison across Pakistan's regional languages, would help to further clarify the scope of the patterns identified here.

## **7. Policy Recommendations**

Based on the findings above, the following policy changes are suggested to more directly address online abuse against women in Pakistan, in response to Research Question 3.

### **7.1 Legislative Reforms**

- Introduce a clear, specific legal definition of gender based online harassment within PECA that plainly covers coordinated harassment by multiple accounts and honour and shame based threats used to frighten or silence women, rather than relying only on a narrow, single attacker model of "cyberstalking."
- Change or clarify the 2025 Amendment's "false information" provisions to include a clear, unambiguous exception for good faith reporting of a person's own experience of harassment or abuse, to remove the current discouragement to reporting documented in this study.
- Set up accessible, lower level appeal and complaint systems for harassment cases, so that recourse is not effectively limited to well funded people able to pursue high court appeals.

## 7.2 Institutional and Enforcement Reforms

- Create or expand specialised, gender sensitive units within the National Cyber Crime Investigation Agency, properly staffed with trained female investigators, to reduce further distress to victims during reporting and investigation.
- Invest in the ability to detect and analyse Urdu and Roman Urdu language content, given this study's finding that language switching is used both to increase abuse and to avoid detection.
- Set up standard, victim centred procedures for handling harassment complaints, including interview practices that take trauma into account and clear timelines for tracking complaints, developed together with organisations such as the Digital Rights Foundation.

## 7.3 Platform Accountability Measures

- Require social media platforms operating in Pakistan, including TikTok, Facebook, X, and Instagram, to publish clear reporting on how they moderate Urdu language content specifically, given the documented weaknesses in this area, and to invest in systems that can detect Urdu and Roman Urdu coordinated harassment.
- Encourage or require fast response reporting channels for coordinated group harassment, recognising that this pattern is different in practice from harassment by a single user and may need different detection methods, such as flags based on the volume and timing of similar posts.

## 7.4 Prevention, Education, and Support

- Add digital literacy and online safety lessons, including training on how bystanders can step in, to secondary school and university education, covering both how to recognise gendered online abuse and the social attitudes that allow it to continue.
- Expand funded, lasting helpline and mental health support services for women who experience online harassment, building on existing models such as the DRF Cyber Harassment Helpline, with attention to making these services available in regional languages.
- Support public awareness campaigns that directly challenge the honour and shame framing identified in this study as a main way that online abuse is used to control women.

## 7.5 Priorities for Implementation

Given limited resources, this study suggests that clarifying the "false information" exceptions for harassment reporting, described in 7.1, and setting up gender sensitive investigation ability, described in 7.2, should be treated as the most urgent priorities. Both directly address the barriers to reporting documented in Sections 4 and 5, and without addressing these barriers, other reforms, including better legal definitions, cannot turn into real protection for women.

## 8. Conclusion

This study set out to examine how language is used to harass women on Pakistani social media, whether current law adequately addresses that harassment, and what policy changes could improve protection. Using critical discourse analysis of public posts and comments from TikTok, Facebook, X, and Instagram, it identified five repeated patterns of language: honour and shame shaming, sexual insults and threats, character assassination, coordinated group harassment, and

strategic switching between Urdu and English. Together, these form a repeated, culturally embedded form of digital social control, rather than incidental online rudeness.

Measured against this pattern of language, Pakistan's legal framework, made up of PECA 2016 and its 2025 Amendment, offers meaningful but incomplete protection. Core offences such as cyberstalking provide a legal starting point, but the definitions do not clearly cover coordinated or culturally specific abuse. Enforcement remains under resourced and prone to causing further distress to victims. The 2025 Amendment's main changes address disinformation and institutional reputation rather than gendered harassment, while creating new legal risk for women who report their own abuse. Closing this gap will require clearer legislation, stronger institutions with specific attention to language and gender sensitivity, greater accountability from platforms, and continued investment in prevention and support, all of which are set out in Section 7. In the end, effective regulation of digital hate speech against women in Pakistan will depend on treating the problem for what the evidence shows it to be: not a minor side effect of online life, but a structured, specific way that offline gender inequality is repeated and enforced in digital space.

## References

- Amnesty International. (2025). *Response to Pakistan's PECA 2025: Threats to freedom of expression* [Press release]. <https://www.amnesty.org>
- Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.
- Committee to Protect Journalists. (2025). *PECA 2025: Implications for press freedom in Pakistan*. <https://cpj.org>
- Digital Rights Foundation. (2016). *The Prevention of Electronic Crimes Bill 2015: An analysis*. <https://digitalrightsfoundation.pk>
- Digital Rights Foundation. (n.d.). *Cyber Harassment Helpline annual reports*. Digital Rights Foundation, Pakistan. <https://digitalrightsfoundation.pk>
- Fairclough, N. (1995). *Critical discourse analysis: The critical study of language*. Longman.
- Freedom House. (2025). *Freedom on the net 2025: Pakistan*. <https://freedomhouse.org>
- Government of Pakistan. (2016). *Prevention of Electronic Crimes Act, 2016* (Act No. XL of 2016). National Assembly of Pakistan.
- Government of Pakistan. (2025). *Prevention of Electronic Crimes (Amendment) Act, 2025*. National Assembly of Pakistan.
- Human Rights Watch. (2025, February 3). *Pakistan: Repeal amendment to draconian cyber law*. <https://www.hrw.org>
- International Federation of Journalists. (2025, January 29). *Pakistan: PECA amendments further tighten government grip on digital expression*. <https://www.ifj.org>
- International IDEA. (2025). *Why Pakistan's cybersecurity law will not help women journalists*. International Institute for Democracy and Electoral Assistance. <https://www.idea.int>
- National Commission for Human Rights. (2026). *Report on PECA and the 2025 Amendment Act*. Government of Pakistan. <https://nchr.gov.pk>
- Reporters Without Borders. (2025). *Pakistan* [Country profile]. <https://rsf.org>
- Sexual Violence Research Initiative, UN Women, The Global Partnership for Action on Gender-Based Online Harassment and Abuse, & Association for Progressive Communications.

(2024). *Technology-facilitated gender-based violence: Developing a shared research agenda*. Sexual Violence Research Initiative. <https://www.svri.org>

Van Dijk, T. A. (1993). Principles of critical discourse analysis. *Discourse & Society*, 4(2), 249-283. <https://doi.org/10.1177/0957926593004002006>