Journal of Law & Social Studies (JLSS)
Volume 8, Issue 1, pp 43-60
www.advancelrf.org

Cyberbullying in Pakistan: Legal Gaps, Gendered Harms, and Social Consequences in a Deepening Digital Environment

Uzair Junaid
Lecturer, University Gillani Law College, Bahauddin Zakariya University, Multan
Email: uzairjunaid@bzu.edu.pk

Abstract
Cyberbullying has emerged as a significant socio-legal challenge in Pakistan, intensified by rapid digitalisation, increased internet accessibility, and widespread engagement with social media platforms. This study critically examines the multidimensional nature of cyberbullying, focusing on its psychological, social, and legal implications within the Pakistani context. Particular attention is given to the disproportionate impact on women and marginalised groups, driven by entrenched socio-cultural norms, stigma, and systemic underreporting. The research evaluates Pakistan's principal legislative framework, namely the Prevention of Electronic Crimes Act (PECA) 2016, highlighting structural deficiencies in enforcement, evidentiary challenges, and persistently low conviction rates. Through a comparative lens, the study situates Pakistan's experience within broader global patterns, identifying common regulatory and technological challenges in addressing cyberbullying across jurisdictions. Furthermore, the study explores the potential of emerging technological interventions, including artificial intelligence-based detection systems, alongside the role of educational initiatives, parental engagement, and media awareness in mitigating online abuse. The findings underscore the necessity for an integrated approach combining legal reform, institutional capacity-building, and socio-cultural transformation. The paper concludes by advocating for strengthened national frameworks aligned with international standards, enhanced digital literacy, and coordinated global cooperation to effectively combat cyberbullying and safeguard digital rights in Pakistan.

Keywords: Cyberbullying, Pakistan, PECA 2016, Online Harassment, Digital Rights, Gender-Based Violence, Cyberstalking, Platform Governance

1. Introduction

The expansion of digital technologies has fundamentally transformed patterns of human interaction, creating unprecedented opportunities for communication while simultaneously giving rise to new forms of harm. Among these, cyberbullying has emerged as a pervasive and complex phenomenon, characterised by the use of electronic platforms to inflict psychological, emotional, or reputational harm on individuals (PACER, 2022). Unlike traditional forms of bullying, cyberbullying operates within a borderless, continuous, and often anonymous digital environment. This allows perpetrators to engage in harmful conduct without immediate accountability, thereby intensifying the frequency and severity of victimisation. The absence of temporal and spatial limitations means that victims may experience harassment at any time, often within spaces previously considered safe, such as their homes (UNICEF, 2024).

In Pakistan, the rise of cyberbullying is closely linked to increased internet penetration, smartphone accessibility, and the proliferation of social media platforms. According to the Pakistan Telecommunication Authority (2023), internet usage has expanded rapidly over the past decade, creating a digital ecosystem that, while beneficial, has also facilitated online abuse and harassment. The post-COVID-19 era has further accelerated this trend, as education, employment, and social interactions have increasingly shifted to online spaces (Sorrentino et al., 2023). The consequences of cyberbullying extend beyond individual harm, affecting broader societal structures. Victims frequently experience psychological distress, including anxiety, depression, and in extreme cases,

suicidal ideation. Additionally, cyberbullying contributes to social fragmentation, fostering environments of mistrust, fear, and exclusion, particularly for vulnerable groups such as women, minorities, and journalists (Hinduja & Patchin, 2022).

The gendered dimension of cyberbullying is especially pronounced in Pakistan, where patriarchal norms and cultural stigmas often discourage reporting and amplify victim-blaming narratives. Women who participate in public discourse are disproportionately targeted, facing harassment intended to silence or discredit them (Jamil, 2020). From a legal standpoint, Pakistan has attempted to address cyberbullying through the enactment of the PECA 2016. While the legislation provides a foundational framework for regulating online conduct, its practical effectiveness remains limited due to enforcement challenges, procedural inefficiencies, and a lack of specialised expertise within law enforcement agencies. This study aims to critically analyse the phenomenon of cyberbullying in Pakistan by examining its nature, prevalence, legal regulation, and societal implications. It further seeks to identify gaps within existing frameworks and propose evidence-based recommendations for developing a more effective and holistic response to cyberbullying (Bauman et al., 2013).

Table 1: Estimated Cyberbullying Prevalence Across Selected Countries

Country	Estimated Prevalence (%)	Key Contributing Factors
India	80–85% (youth exposure)	High internet growth, low awareness
United States	70–73%	Social media usage, anonymity
Belgium	~25%	Multilingual digital environment
Sweden	~23%	Social media penetration
United Kingdom	~18%	Underreporting, online hate speech
Australia	~19%	Digital dependency
Canada	~20%	Mental health concerns, anonymity
China	~17%	Social pressure, controlled internet

Sources: Cook (2024); Cyberbullying Research Centre (2024); Office for National Statistics (2024); eSafety Commissioner (2024)

2. Review of Related Literature

2.1 Conceptualising Cyberbullying

Cyberbullying is generally understood as deliberate and repeated harm inflicted through digital technologies, including social networking sites, instant messaging applications, online forums, gaming platforms, and email (Smith & Steffgen, 2013). Although the phenomenon shares certain conceptual features with traditional bullying, such as intent, repetition, and a power imbalance, it differs in ways that intensify the victim's vulnerability. Digital abuse can occur continuously, may be anonymous, and often reaches audiences far beyond the immediate social circle of the victim. As a result, cyberbullying is not merely an online version of conventional bullying; it is a qualitatively distinct form of victimisation shaped by the architecture of digital communication. A central feature of cyberbullying is the collapse of boundaries between public and private spaces. In conventional settings, bullying often occurs in identifiable environments such as schools, workplaces, or neighbourhoods. By contrast, cyberbullying follows the victim into domestic and personal spaces through mobile phones and internet-connected devices. This permanent accessibility produces a form of psychological siege in which the victim may feel that harassment is inescapable (UNICEF, 2024). The permanence and replicability of online content further distinguish cyberbullying from offline

aggression. Hurtful messages, humiliating images, or defamatory posts can be copied, recirculated, and archived indefinitely, prolonging humiliation long after the original act.

Scholars have also emphasised that anonymity reshapes the power dynamics of bullying. In traditional bullying, the aggressor is often physically known to the victim. In digital contexts, however, perpetrators may conceal their identities through fake profiles, anonymous accounts, or temporary communication channels. This concealment lowers social inhibition and may embolden aggressors to engage in more extreme or sustained abuse (Jane, 2016). For victims, anonymity deepens fear, because the source of harm remains uncertain and difficult to confront. The inability to identify the offender may produce prolonged stress, mistrust, and feelings of helplessness. Another defining feature concerns audience amplification. Harmful content posted online may be viewed not by a single person but by dozens, hundreds, or even thousands of users. The public visibility of humiliation can intensify emotional injury and increase reputational damage. Smith et al. (2008) note that this exposure often magnifies the emotional consequences of bullying, as victims face not only the abuse itself but also the awareness that others are witnessing, sharing, or silently tolerating it. For adolescents in particular, social validation and peer perception are central to identity formation; thus, public online humiliation can inflict deep psychological harm. The literature also highlights the fluidity of roles within cyberbullying environments. Individuals may move between categories of victim, perpetrator, and bystander, especially within group chats, comment threads, and networked peer cultures. A user who initially witnesses abuse may later amplify it by sharing content, reacting publicly, or remaining silent in ways that normalise aggression. This participatory structure complicates legal and ethical accountability and distinguishes cyberbullying from one-to-one harassment models (Niederman & Baker, 2023).

2.2 Cyberbullying and Traditional Bullying: Points of Convergence and Divergence

The relationship between cyberbullying and traditional bullying has been widely debated. Some scholars treat cyberbullying as an extension of preexisting bullying behaviour into digital spaces, while others argue that it constitutes a separate category due to its unique technological characteristics. Both forms involve aggressive conduct and often emerge from social hierarchies, peer conflict, or prejudice. Yet the mechanisms through which harm is inflicted differ significantly. Traditional bullying commonly involves direct verbal abuse, physical intimidation, or social exclusion within face-to-face settings. Because it typically occurs in proximate spaces, opportunities for adult intervention may be greater, even if such intervention is not always effective. Cyberbullying, in contrast, frequently unfolds outside institutional oversight. Harm may occur late at night, across jurisdictions, or through encrypted or disappearing platforms, making detection more difficult and response slower (Spyropoulos, 2025).

The emotional impact of cyberbullying may also be more enduring because of its repetitive exposure. A schoolyard insult may eventually fade from public memory, but an online post can remain searchable, screen-captured, and repeatedly redistributed. Espelage and Hong (2017) observe that digital persistence intensifies trauma by allowing the abusive act to be relived multiple times. In this sense, cyberbullying can be both event-based and archival: a single post may continue to cause harm through ongoing circulation. Another difference lies in the altered perception of power. In traditional bullying, power often derives from physical strength, age, popularity, or social status. In cyberbullying, power can stem from technological literacy, access to private information, manipulation of digital identities, or the ability to mobilise online audiences. A physically less powerful individual may become highly influential in digital harassment by controlling narrative, virality, or group participation. This redistribution of power complicates simplistic understandings of bullying and requires frameworks that account for technological mediation. At the same time, literature shows a strong overlap between offline and online victimisation. Many victims of traditional bullying also experience cyberbullying, and perpetrators may use digital tools to extend or intensify conflicts originating offline (Yang et al., 2021). This overlap suggests that effective interventions

should not isolate cyberbullying as a purely technological issue. Rather, it should be addressed as part of broader patterns of aggression, exclusion, misogyny, and social domination.

2.3 Forms and Tactics of Cyberbullying

Cyberbullying manifests through a wide range of practices, each producing distinct legal and psychological consequences. The literature commonly identifies several recurring tactics: harassment, impersonation, cyberstalking, outing, exclusion, denigration, trolling, and non-consensual dissemination of images or information. These forms may occur separately, but in many cases, they overlap and escalate one another. Harassment involves repeated abusive messages, threats, or humiliating communication directed at a victim through digital means. This is among the most common forms of cyberbullying and may include obscene language, moral shaming, sexualized insults, or threats of violence. In Pakistan, such harassment is often heavily gendered, especially when directed toward women in public-facing roles.

Impersonation occurs when a perpetrator creates a false profile or gains unauthorised access to a victim's account to post harmful content, damage reputation, or manipulate others. This form of abuse is particularly injurious because it undermines both identity and credibility. Plunkett (2019) notes that identity-based digital harms are especially difficult to reverse once harmful content circulates widely. In societies where honour and public reputation are socially significant, impersonation may have severe offline consequences. Cyberstalking refers to persistent surveillance, monitoring, threats, or unwanted communication conducted through electronic means. It often creates intense fear because the victim experiences the perpetrator as constantly present. Macnish (2017) emphasises that surveillance-based harms erode autonomy by making individuals feel perpetually watched. In Pakistan, cyberstalking frequently intersects with gendered coercion, blackmail, or reputational violence.

Outing involves the disclosure of private, personal, or intimate information without consent. This may include screenshots of private chats, personal photographs, contact information, or allegations about relationships, sexuality, or family life. Willard (2007) observed that outing is particularly harmful because it weaponises trust. The injury caused is not limited to embarrassment; it can alter family relations, educational prospects, employment opportunities, and marriage-related social standing. Trolling is often described as provocative or inflammatory online behaviour designed to distress others or derail discussion (Phillips, 2015). Although some forms of trolling are framed as performative mischief, the distinction between trolling and targeted abuse is often thin. Where trolling becomes repetitive, identity-targeted, or socially coordinated, it functions as cyberbullying. In public discourse spaces, women, journalists, and activists are particularly vulnerable to troll-based silencing. Exclusion is another significant tactic, especially among adolescents. It involves deliberately excluding someone from digital groups, online communities, or shared communication spaces to humiliate or isolate them. Although less visible than direct abuse, exclusion can inflict serious emotional harm by signalling rejection and social worthlessness. These tactics demonstrate that cyberbullying is not a single act but a spectrum of digitally mediated harms (Anderson, 2026). Legal responses must therefore be flexible enough to address varied forms of abuse without collapsing them into a single undifferentiated category.

2.4 Global Trends in Cyberbullying

The international literature shows that cyberbullying is a widespread and increasing concern across both developed and developing societies. While prevalence estimates vary depending on methodology, age group, and definitional scope, the global trend indicates that cyberbullying is now a core child protection, mental health, and digital governance issue. In the United States, research from the Cyberbullying Research Center consistently reports significant exposure among school-going youth, with social media and texting serving as primary sites of abuse (Cyberbullying Research Center, 2024). American literature also shows strong correlations between cybervictimization and depression, school disengagement, and self-harm. Race, gender, disability, and sexual orientation

frequently shape patterns of online victimisation, indicating that cyberbullying often reflects broader social inequalities rather than random interpersonal hostility.

India presents a different but equally serious picture. Rapid digital expansion, widespread mobile phone adoption, and uneven digital literacy have created conditions in which cyberbullying has grown faster than institutional responses. Kaur and Saini (2023) note that legal and educational initiatives exist, but implementation remains inconsistent. Social stigma around mental health and victimisation may further discourage reporting, especially among girls (World Health Organisation, 2020). European countries provide instructive comparative examples. In the United Kingdom, bullying and online abuse are increasingly treated as interconnected public policy issues, with emphasis on child safety, platform accountability, and school-based intervention (European Union Agency for Fundamental Rights, 2014). Yet underreporting remains a persistent problem. Belgium and Sweden also demonstrate that strong welfare and education systems do not eliminate cyberbullying; rather, they shape the mode of response. Preventive education and digital literacy appear more institutionalised in these contexts, but online harassment continues to affect youth and marginalised groups (Office for National Statistics, 2024).

Australia and Canada have adopted relatively proactive public safety models, including regulatory agencies, reporting mechanisms, and awareness programs. The Australian eSafety framework is frequently cited as a notable institutional response because it combines user complaint systems, content removal procedures, and educational outreach (eSafety Commissioner, 2024). Nevertheless, critics argue that reactive complaint-based frameworks do not sufficiently address structural causes or platform design issues. China illustrates a distinct regulatory environment in which state control over digital ecosystems coexists with ongoing cyberbullying. Despite high levels of content regulation, peer-to-peer harassment persists, particularly among adolescents. This indicates that censorship alone cannot substitute for broader strategies involving mental health support, digital ethics, and user education. Overall, comparative literature reveals several common themes: the normalization of online aggression, difficulty in reporting, inadequate institutional responses, the role of anonymity, and the disproportionate vulnerability of specific groups (Zhou, 2021). At the same time, local contexts matter. Cultural attitudes toward honour, shame, gender, privacy, and authority strongly influence both the prevalence of cyberbullying and the willingness of victims to seek help.

2.5 Gendered Dimensions of Cyberbullying

One of the most consistent findings in contemporary scholarship is that cyberbullying is not gender-neutral. Women and girls often experience forms of digital abuse that are sexualized, moralized, and closely tied to patriarchal control. While men may also be victims of cyberbullying, the nature of abuse directed at women tends to be more explicitly degrading, reputational, and coercive. This is particularly evident in societies where female respectability is heavily policed and where public participation by women may itself be contested. Jamil (2020) demonstrates that Pakistani female journalists face persistent online abuse, including threats, misogynistic attacks, and professional delegitimisation. Such harassment is often designed not merely to insult but to silence. The same pattern appears globally, where women in media, politics, academia, and activism are targeted disproportionately through coordinated digital hostility. Jane (2016) describes this as a broader ecosystem of online misogyny in which abuse becomes a disciplinary tool used to restrict female visibility.

Gendered cyberbullying often includes threats of sexual violence, doctored images, impersonation, non-consensual sharing of photographs, and attacks on family honour. In Pakistan, these forms of abuse are aggravated by cultural stigmas that place the burden of shame on the victim rather than the perpetrator. Thus, a woman subjected to digital defamation may experience social consequences extending far beyond the platform on which the abuse occurred. The fear of family backlash, reputational harm, and institutional indifference contributes to severe underreporting. Trans persons and gender-nonconforming individuals face similar or even heightened vulnerabilities. Because their

identities are already socially contested in many settings, online harassment may combine mockery, exposure, hate speech, and threats. The literature increasingly recognises that intersectionality is essential to understanding cyberbullying. Gender interacts with class, age, profession, religion, sexuality, and digital visibility in shaping patterns of victimization (Pedersen et al., 2023).

2.6 Psychological and Social Consequences in the Literature

The psychological consequences of cyberbullying are well established across the literature. Victims commonly report anxiety, chronic stress, shame, loss of self-esteem, depression, sleep disturbances, social withdrawal, and academic decline (Mishna et al., 2010). The intensity of harm often depends on duration, public visibility, relationship to the perpetrator, and availability of support. Repeated exposure can produce a condition of constant vigilance in which victims begin to anticipate abuse even when not actively online. Hinduja and Patchin (2010, 2022) have documented a significant association between cybervictimization and suicidal ideation. This relationship does not imply simple causation, but it underscores the seriousness of repeated online abuse, especially when combined with existing vulnerabilities such as isolation, prior trauma, or lack of adult support. For adolescents, whose social identities are still forming, digital humiliation can be especially destabilising.

The impact is not limited to individuals. Families may experience distress, helplessness, anger, and conflict when one member is targeted online (O'Brien & Moules, 2010). Parents often feel technologically outmatched or uncertain about how to intervene. In communities where victimisation is stigmatised, families may discourage reporting in order to avoid further exposure. Thus, cyberbullying can produce collective silence as well as individual suffering. The literature also highlights the social normalisation of online cruelty. Where digital aggression is framed as humor, banter, or inevitable internet culture, victims may struggle to have their experiences taken seriously. This minimisation is particularly harmful because it delays intervention and deepens self-blame. Livingstone and Blum-Ross (2020) argue that children's rights in digital environments require not only access and participation but also protection from normalized harm. This perspective is highly relevant to Pakistan, where the legal and educational discourse on cyberbullying remains underdeveloped relative to the scale of digital expansion.

3. Objectives of the Study

This study seeks to provide a comprehensive examination of cyberbullying within the evolving digital landscape of Pakistan by addressing multiple interconnected dimensions of the phenomenon. It aims to analyze both the conceptual foundations and practical manifestations of cyberbullying in order to understand its nature, scope, and implications in the Pakistani context. A central objective of the research is to critically evaluate the effectiveness of Pakistan's legal framework, particularly the PECA 2016, in addressing cyberbullying and related forms of online harm, while identifying gaps in enforcement and regulatory mechanisms. Furthermore, the study explores the gendered dimensions of cyberbullying, with particular emphasis on the experiences of women, journalists, and other vulnerable or marginalized groups who are disproportionately affected by digital harassment. It also seeks to assess the psychological and social consequences of cyberbullying, not only for individual victims but also for their families and broader communities, thereby highlighting its wider societal impact. In addition, the research undertakes a comparative analysis of Pakistan's approach with selected international models to identify best practices and policy lessons that may be adapted within the local context. Ultimately, the study aims to develop well-grounded, evidence-based recommendations that can contribute to more effective legal, institutional, and societal responses to cyberbullying in Pakistan.

4. Research Methodology

This study adopts a qualitative doctrinal-cum-analytical methodology supported by secondary quantitative data. The purpose of using this mixed analytical approach is to examine cyberbullying not merely as a behavioural problem but as a legal, social, and policy issue. The research, therefore, integrates legal analysis, literature review, policy comparison, and data-based contextualization. The

doctrinal component focuses primarily on Pakistan's statutory and regulatory framework, especially the PECA 2016. Relevant sections relating to dignity, privacy, harassment, cyberstalking, and offenses involving minors are analyzed to assess whether the existing framework is conceptually adequate and practically enforceable. This part of the study also draws upon judicial materials, institutional reports, and commentary on the evidentiary and procedural challenges associated with digital offenses.

The analytical and comparative component reviews scholarship and official reports from Pakistan and other jurisdictions to identify broader trends in cyberbullying prevention and regulation. Comparative references to countries such as the United States, the United Kingdom, Australia, Canada, India, and Sweden are used not to replicate foreign models uncritically, but to identify adaptable lessons for Pakistan. The study relies substantially on secondary sources, including peer-reviewed journal articles, books, statutory texts, court materials, government reports, NGO publications, institutional datasets, and media accounts. Such materials are particularly useful in the Pakistani context, where direct national datasets on cyberbullying remain fragmented. Reports by the Digital Rights Foundation, Pakistan Telecommunication Authority, UNICEF, the Cyberbullying Research Center, and other recognized organizations are used to provide contextual and empirical grounding (Canadian Centre for Child Protection, 2014).

A thematic method of analysis is employed throughout. The collected material is organized under recurring themes: conceptualization of cyberbullying, forms and tactics, legal challenges, gendered victimization, psychological harm, institutional shortcomings, and policy responses. This allows the research to move beyond description and toward a critical assessment of how cyberbullying is understood and governed in Pakistan. The methodology has certain limitations. First, Pakistan lacks a single standardized national dataset exclusively devoted to cyberbullying, which means that some discussions rely on broader cyber harassment or online abuse data. Second, legal enforcement statistics often do not disaggregate cyberbullying from related categories such as cyberstalking or online harassment. Third, because underreporting is a major issue especially for women and marginalized victims the scale of the problem is likely larger than official complaint figures suggest. These limitations, however, do not undermine the value of the study; rather, they point to an urgent need for improved data collection and policy transparency. Despite these constraints, the chosen methodology is suitable for the present research because it enables a multidimensional examination of cyberbullying in Pakistan. It facilitates legal critique, socio-cultural interpretation, and policy-oriented recommendations within a single coherent framework.

Table 2: Selected Forms of Cyberbullying and Their Primary Consequences

Form of cyberbullying	Description	Likely consequences
Harassment	Repeated abusive or threatening digital messages	Anxiety, fear, emotional distress
Impersonation	Fake accounts or unauthorised use of identity	Reputational damage, social mistrust
Cyberstalking	Persistent monitoring, threats, or surveillance	Fear, hypervigilance, loss of safety
Outing	Disclosure of private information without consent	Shame, humiliation, social exclusion
Trolling	Provocative or inflammatory abuse in public forums	Emotional exhaustion, withdrawal from online participation

Exclusion	Deliberate removal from digital groups or communities	Isolation, lowered self-worth
Non-consensual image sharing	Distribution of intimate or personal images	Severe reputational harm, trauma, and blackmail risk

Sources: Willard (2007); Smith et al. (2008); Phillips (2015); Moreno et al. (2019).

Table 3: Indicative Pakistani Institutional and Social Challenges in Addressing Cyberbullying

Challenge	Nature of the problem	Practical effect
Underreporting	Victims fear stigma, retaliation, or disbelief	Official data underestimates prevalence
Limited digital literacy	Users and families may not recognise legal remedies or reporting options	Delayed response and weak prevention
Evidentiary difficulties	Digital content may be deleted, altered, or anonymously circulated	Weak prosecutions and procedural failures
Institutional capacity gaps	Limited technical expertise and investigative resources	Slow and ineffective enforcement
Gender-based stigma	Women face reputational and social consequences for reporting	Silencing of victims and normalisation of abuse
Platform response inconsistency	Reporting tools and moderation systems are uneven	Harmful content remains online longer

Sources: Digital Rights Foundation (2024); Pakistan Telecommunication Authority (2023); Sohail and Durrani (2023); Kamran et al. (2019).

5. Cyberbullying in Pakistan: A Critical and Contextual Analysis

5.1 The Digital Transformation and Rise of Cyberbullying

Over the past decade, Pakistan has undergone a significant digital transformation characterised by rapid expansion in internet connectivity, mobile penetration, and social media usage. While this transformation has facilitated economic growth, communication, and access to information, it has simultaneously created an environment conducive to new forms of harm, particularly cyberbullying. According to the Pakistan Telecommunication Authority (2023), the number of internet users in Pakistan has increased exponentially, crossing over 120 million users. This expansion has been accompanied by a corresponding surge in social media engagement, particularly among youth. Platforms such as Facebook, Instagram, Twitter (X), TikTok, and WhatsApp have become integral to everyday communication. However, the same platforms have also become primary sites for harassment, defamation, and digital abuse.

Cyberbullying in Pakistan has evolved from sporadic online hostility into a systemic and normalised phenomenon. Unlike earlier forms of offline bullying, digital harassment in Pakistan often operates within a framework of anonymity, rapid dissemination, and weak regulatory enforcement. This transformation reflects broader global patterns but is intensified by local socio-cultural and institutional factors. One of the most critical drivers of cyberbullying in Pakistan is the gap between technological advancement and digital literacy. While access to digital tools has expanded rapidly, awareness regarding safe online behaviour, privacy protection, and legal remedies has not progressed at the same pace. As a result, users, especially adolescents, are often ill-equipped to navigate online risks or respond effectively to harassment. Moreover, cyberbullying in Pakistan cannot be understood in isolation from existing social hierarchies and cultural norms (Iqbal & Jami, 2022). Online abuse

frequently mirrors offline inequalities, including gender discrimination, class divisions, and ideological polarisation. Consequently, digital platforms do not merely host new forms of aggression; they amplify pre-existing patterns of exclusion and hostility.

Table 4: Growth of Digital Access and Reported Cyber Harassment in Pakistan

Indicator	Estimated Value	Source
Internet users	120+ million	Pakistan Telecommunication Authority (2023)
Social media users	70+ million	PTA (2023)
Annual cyber harassment complaints	130,000+	Digital Rights Foundation (2024)
Female victims (approx.)	60–70% of complaints	DRF (2024)
Youth (15–29) internet users	Majority demographic	PTA (2023)

Sources: Pakistan Telecommunication Authority (2023); Digital Rights Foundation (2024)

5.2 The Role of Social Media Platforms

Social media platforms occupy a central role in the proliferation of cyberbullying in Pakistan. These platforms provide spaces for interaction, expression, and identity formation, but they also enable anonymity, virality, and amplification of harmful content. On one hand, social media facilitates the rapid spread of abusive messages, misinformation, and defamatory content. A single post can be shared widely within minutes, exposing victims to mass humiliation and sustained harassment. Features such as comment threads, anonymous accounts, and private messaging systems create multiple entry points for abuse.

On the other hand, social media has also been used as a tool for resistance and accountability. Victims and activists have utilised these platforms to expose harassment, mobilise public support, and demand institutional action. Hashtag activism and digital advocacy campaigns have played a role in bringing attention to cyberbullying cases that might otherwise remain invisible. However, the response of technology companies remains inconsistent. While most platforms provide reporting mechanisms and community guidelines, their enforcement is often slow, opaque, and culturally insensitive. Global moderation policies may fail to adequately address local forms of harassment rooted in language, cultural context, or gender norms (Saleem et al., 2021). The absence of localised content moderation and limited collaboration with Pakistani authorities further weakens platform accountability. As a result, harmful content may remain accessible for extended periods, exacerbating the impact on victims.

5.3 High-Profile Cases and Public Awareness

High-profile cyberbullying cases in Pakistan have played a significant role in highlighting the severity of the issue and exposing institutional shortcomings. These cases illustrate not only the prevalence of cyberbullying but also the systemic barriers that victims face in seeking justice. The case of Fatima Aamir is frequently cited as an example of prolonged institutional inaction. For several years, she faced severe online harassment, including threats of violence. Despite repeated complaints, meaningful intervention occurred only after the case gained public and media attention. This delay underscores the reactive nature of law enforcement and the reliance on public pressure to trigger action. Similarly, prominent public figures such as Meesha Shafi and Bina Shah have been subjected to coordinated online harassment. In these cases, cyberbullying was used as a tool to discredit, intimidate, and silence women who challenged social norms or spoke out on sensitive issues. These

incidents demonstrate how cyberbullying intersects with gender politics, freedom of expression, and societal power structures (Haq & Zarkoon, 2023). Such cases reveal a broader pattern: cyberbullying in Pakistan is often not random, but targeted, sustained, and socially embedded. It frequently aims to control narratives, enforce conformity, and punish dissent.

5.4 Gendered Nature of Cyberbullying in Pakistan

Cyberbullying in Pakistan exhibits a pronounced gender dimension. Women, particularly those in public roles such as journalists, activists, and entertainers, face disproportionately high levels of online harassment. This harassment often takes forms that are explicitly sexualized, reputational, and coercive. Research indicates that a significant majority of female journalists in Pakistan have experienced online abuse, including threats of violence and character assassination (Johansson & Englund, 2021). Such harassment not only affects individual well-being but also undermines press freedom and democratic participation. The gendered nature of cyberbullying is closely linked to patriarchal norms that regulate women's visibility and behaviour. Online abuse is frequently used as a mechanism to enforce social control, discourage public participation, and reinforce traditional gender roles. Women who challenge these norms may be subjected to intensified harassment. Underreporting remains a critical issue. Many victims choose not to report incidents due to fear of stigma, victim-blaming, or further harassment. In some cases, families discourage reporting to avoid reputational damage. This creates a cycle in which cyberbullying remains both widespread and under-documented. Marginalised groups, including transgender individuals, also face heightened vulnerability (Amadori et al., 2025). Their experiences highlight the intersectional nature of cyberbullying, where multiple forms of discrimination converge in digital spaces.

5.5 Psychological and Social Consequences

The psychological impact of cyberbullying in Pakistan is profound and multifaceted. Victims often experience a range of emotional and mental health challenges, including anxiety, depression, low self-esteem, and feelings of isolation. One of the most damaging aspects of cyberbullying is its continuous and pervasive nature. Unlike offline bullying, which may be confined to specific locations or times, cyberbullying can occur at any moment, leaving victims with little opportunity for respite. This constant exposure can lead to chronic stress and emotional exhaustion. The anonymity of perpetrators further exacerbates psychological harm. Victims may feel powerless and unable to confront their abusers, leading to increased fear and uncertainty. In severe cases, cyberbullying has been linked to self-harm and suicidal ideation (Hinduja & Patchin, 2022). The impact extends beyond individuals to families and communities. Families may experience distress, helplessness, and social stigma. Victims may withdraw from social interactions, leading to isolation and reduced participation in education or employment. Cultural attitudes also play a significant role. In many cases, victims are blamed for their experiences, which discourages them from seeking help. This victim-blaming culture reinforces silence and perpetuates the cycle of abuse (Agatston et al., 2012).

5.6 Legal Framework: PECA 2016 and Its Limitations

The PECA 2016 represents Pakistan's primary legislative response to cybercrime, including cyberbullying. The Act criminalises various forms of online misconduct, including harassment, defamation, cyberstalking, and offences against privacy (National Crime Prevention Council, 2009).

Key provisions relevant to cyberbullying include:

- **Section 21**: Offences against the dignity of a natural person
- **Section 22**: Protection against child exploitation
- **Section 24**: Cyberstalking

These provisions provide a legal basis for addressing cyberbullying. However, their effectiveness is significantly limited by implementation challenges. One of the most critical issues is the low conviction rate. Despite a high number of reported complaints, only a small fraction result in

successful prosecution. This gap reflects broader systemic issues, including weak evidence collection, procedural delays, and limited technical expertise (Qureshi et al., 2020).

Table 5: Cybercrime Complaints vs Convictions in Pakistan (Illustrative)

Period	Complaints Filed	Convictions	Approx. Conviction Rate
2018–2024	27,000+	60–70	<1%

Source: Kamboyo (2024); media and institutional reports

5.7 Enforcement Challenges

Several structural challenges hinder the effective enforcement of cyberbullying laws in Pakistan:

1. **Evidentiary Issues**

   Digital evidence can be easily altered or deleted, making it difficult to collect and preserve in admissible form. Law enforcement agencies often lack the technical capacity required for digital forensics (Kamran et al., 2019).

2. **Anonymity and Identification**

   Identifying perpetrators is particularly challenging due to the use of fake accounts, VPNs, and encrypted platforms.

3. **Institutional Limitations**

   Agencies such as the Federal Investigation Agency (FIA) face resource constraints and increasing caseloads. The establishment of the National Cyber Crime Investigation Agency (NCCIA) represents a step forward, but coordination issues remain.

4. **Judicial Constraints**

   Courts may lack specialised knowledge of cybercrime, leading to procedural inefficiencies and inconsistent judgments (Usman, 2017).

5. **Public Awareness Deficit**

   Many victims are unaware of legal remedies or reporting mechanisms, which limits the effectiveness of existing laws.

5.8 Cyber Crime Reporting Centres (CCRCs)

Cyber Crime Reporting Centres have been established across Pakistan to facilitate complaint registration and investigation. These centres have contributed to increased reporting, as evidenced by the growing number of complaints.

However, their effectiveness is constrained by:

- Limited staffing and resources
- Lack of advanced forensic tools
- Low public awareness
- Delays in case processing

Despite these challenges, CCRCs remain a critical component of Pakistan's cybercrime response infrastructure and require further strengthening.

5.9 Strategies for Preventing and Combating Cyberbullying

Addressing cyberbullying in Pakistan requires a comprehensive, multi-layered approach that integrates legal reform, technological innovation, educational initiatives, and societal transformation. Isolated interventions, whether legal or technological, are insufficient to tackle a problem that is deeply embedded in both digital infrastructures and socio-cultural dynamics.

5.9.1 Education and Digital Literacy

Education remains one of the most effective long-term strategies for preventing cyberbullying. Digital literacy programs should be incorporated into school curricula at all levels, emphasising responsible online behaviour, empathy, privacy awareness, and the consequences of cyber harassment. Early education can play a critical role in shaping digital ethics and fostering respectful online interaction. Schools and universities should adopt structured anti-cyberbullying policies that include reporting mechanisms, disciplinary frameworks, and counselling services. Teachers and administrators must be trained to identify signs of cyberbullying and respond appropriately. Research indicates that proactive educational interventions are significantly more effective than reactive disciplinary measures (Hinduja & Patchin, 2014).

5.9.2 Role of Parents and Families

Parental involvement is essential in mitigating cyberbullying, particularly among adolescents. Parents must be equipped with the knowledge and tools necessary to monitor online activities, recognise warning signs, and engage in open dialogue with their children. A supportive family environment can encourage victims to report incidents without fear of judgment or punishment. Mesch (2009) emphasises that parental mediation, both restrictive and communicative, can significantly reduce exposure to online risks. In the Pakistani context, awareness programs targeting parents are especially important due to generational gaps in digital literacy.

5.9.3 Technological Interventions and AI-Based Detection

Technological innovation offers promising tools for identifying and preventing cyberbullying. Artificial intelligence (AI) and machine learning algorithms can analyse large volumes of data to detect patterns of abusive language, threats, and harmful behaviour in real time (Reynolds et al., 2011). These systems can assist platforms in flagging content, prioritising reports, and removing harmful material more efficiently. However, the deployment of AI must be accompanied by safeguards to address ethical concerns, including privacy violations, algorithmic bias, and false positives. In multilingual societies like Pakistan, AI systems must also be adapted to local languages and cultural contexts to ensure accurate detection. Without localisation, many forms of abuse, especially those expressed in Urdu or regional languages, may go undetected.

5.9.4 Platform Responsibility and Regulation

Technology companies play a central role in shaping online environments and must be held accountable for addressing cyberbullying. Platforms should implement:

- Clear and enforceable community guidelines
- Efficient and user-friendly reporting mechanisms
- Transparent moderation processes
- Timely removal of harmful content

Collaboration between technology companies and national regulatory bodies is essential. In Pakistan, stronger engagement between social media platforms and authorities such as the Pakistan Telecommunication Authority can enhance content moderation and victim support.

5.9.5 Victim Support Systems

Effective response strategies must prioritise the well-being of victims. Access to psychological counselling, legal assistance, and peer support networks is critical for recovery. Counselling services

should be accessible both online and offline, particularly for individuals in remote or underserved areas. Peer support groups can provide safe spaces for victims to share experiences and receive emotional support (Slonje & Smith, 2008). Institutionalising victim support mechanisms within schools, universities, and workplaces can help reduce stigma and encourage reporting (Boyd, 2014).

5.10 The Imperative of International Cooperation

Cyberbullying is inherently transnational, often involving perpetrators, victims, and platforms located in different jurisdictions. This cross-border nature complicates enforcement and necessitates international cooperation.

5.10.1 Global Collaboration and Legal Harmonisation

Effective responses to cyberbullying require harmonised legal frameworks, shared investigative protocols, and coordinated law enforcement efforts. International organisations such as INTERPOL and the United Nations play a vital role in facilitating cooperation and knowledge exchange (INTERPOL, n.d.). Countries must work together to establish standardised procedures for reporting, investigating, and prosecuting cyberbullying cases. Such cooperation can enhance the capacity of national institutions and reduce jurisdictional barriers (Hellfeldt et al.,2019).

5.10.2 The Budapest Convention on Cybercrime

The Budapest Convention (Council of Europe, 2001) represents the most comprehensive international treaty addressing cybercrime. It provides a framework for:

- Criminalising cyber offences
- Facilitating cross-border investigations
- Sharing digital evidence
- Strengthening international cooperation

Despite its significance, Pakistan has not ratified the Convention, citing concerns over sovereignty and data-sharing provisions. While these concerns are valid, non-participation limits Pakistan's ability to engage in coordinated global responses to cybercrime.

5.10.3 Challenges in Cross-Border Enforcement

Cross-border cyberbullying cases face several challenges:

- Differences in legal definitions and standards
- Variations in data protection laws
- Jurisdictional conflicts
- Delays in mutual legal assistance

Wicki-Birchler (2020) highlights that inconsistencies in legal frameworks often hinder effective cooperation. Addressing these challenges requires both legal reform and diplomatic engagement.

6. Conclusions and Recommendations

6.1 Conclusion

Cyberbullying has emerged as a complex and pervasive issue in Pakistan, reflecting the intersection of technological advancement, socio-cultural dynamics, and legal limitations. This study demonstrates that cyberbullying is not merely an individual behavioural problem but a systemic challenge requiring coordinated responses across multiple sectors. The findings reveal that while Pakistan has established a legal framework through the PECA 2016, significant gaps remain in enforcement, institutional capacity, and public awareness. Low conviction rates, evidentiary challenges, and underreporting undermine the effectiveness of existing laws. The gendered nature of

cyberbullying further complicates the issue, with women and marginalised groups facing disproportionate levels of abuse. Cultural stigmas and victim-blaming attitudes exacerbate the problem, discouraging reporting and perpetuating silence. At the same time, global comparisons indicate that Pakistan is not alone in facing these challenges. Cyberbullying is a worldwide phenomenon, and its effective management requires both national reforms and international cooperation.

6.2 Key Recommendations

An effective response to cyberbullying in Pakistan necessitates comprehensive legal and institutional reforms aimed at strengthening both the substantive and procedural dimensions of existing frameworks. In this regard, the implementation of the PECA 2016 must be enhanced through the development of clearer procedural guidelines and the provision of specialised training for law enforcement personnel and members of the judiciary. Such training should focus on the technical complexities of cybercrime, including digital evidence collection, preservation, and admissibility. Furthermore, the establishment of dedicated cybercrime courts would significantly expedite the adjudication process, reducing delays and improving access to justice for victims. Alongside these reforms, investment in advanced digital forensic capabilities is essential to ensure that investigative agencies are equipped to effectively handle complex cyberbullying cases. In addition to legal reforms, capacity building within institutional structures is critical to improving the overall response to cyberbullying. This includes the allocation of adequate resources, expansion of specialised cybercrime units, and continuous professional development programs for investigators, prosecutors, and judicial officers. Strengthening coordination between agencies such as the Federal Investigation Agency (FIA) and the National Cyber Crime Investigation Agency (NCCIA) would further enhance efficiency and reduce jurisdictional ambiguities (Sahoutara, 2022).

Public awareness and education also constitute a vital component of any comprehensive strategy. Nationwide campaigns should be initiated to educate citizens about cyberbullying, digital rights, and available reporting mechanisms. Integrating digital citizenship and online safety education into school curricula can foster responsible online behaviour from an early age, thereby addressing the root causes of cyberbullying. These initiatives should be inclusive and culturally sensitive to ensure broad societal engagement. Given the pronounced gendered nature of cyberbullying in Pakistan, it is imperative to adopt gender-sensitive policies that provide targeted protection for women and marginalised groups. Confidential and accessible reporting mechanisms should be developed to encourage victims to come forward without fear of stigma or retaliation. Legal and institutional responses must also address the specific forms of harassment faced by women, including reputational abuse and online intimidation.

The role of technology companies must also be strengthened through greater accountability and collaboration with regulatory authorities. Social media platforms should be required to implement localised content moderation policies, transparent reporting systems, and efficient complaint-handling procedures. Enhanced cooperation between these platforms and national institutions would contribute to a more effective and timely response to cyberbullying incidents. Technological innovation, particularly the use of artificial intelligence and machine learning, offers significant potential in detecting and preventing cyberbullying. However, the deployment of such technologies must be accompanied by appropriate ethical safeguards to ensure the protection of user privacy and the prevention of algorithmic bias. These tools should complement, rather than replace, human oversight in content moderation processes.

Equally important is the establishment of robust victim support mechanisms. Access to psychological counselling, legal assistance, and peer support networks should be expanded to ensure that victims receive comprehensive care. Institutionalising these services within educational institutions and workplaces can help reduce stigma and promote a culture of support and resilience. Finally, addressing the transnational nature of cyberbullying requires active international engagement.

Pakistan should explore greater participation in global frameworks, including instruments such as the Budapest Convention on Cybercrime, to enhance cross-border cooperation. Strengthening partnerships with international organisations can facilitate knowledge exchange, capacity building, and coordinated responses to cybercrime, thereby contributing to a safer and more secure digital environment.

References

Agatston, P. W., Limber, S., & Kowalski, R. M. (2012). *Cyberbullying: Bullying in the digital age*. Wiley-Blackwell.

Amadori, A., Real, A. G., Brighi, A., & Russell, S. T. (2025). An intersectional perspective on cyberbullying: Victimization experiences among marginalized youth. *Journal of Adolescence*, *97*(4), 931-940.

Anderson, B. (2026). *Doxxed: How Privacy Abuse Harms*. Policy Press.

Bauman, S., Cross, D., & Walker, J. (2013). Principles of cyberbullying research. *definition, methods, and measures*, 2013.

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Canadian Centre for Child Protection. (2014). Reducing cyberbullying and exploitation among teens in Canada. Retrieved from https://protectchildren.ca/en/press-and-media/news-releases/2014/cyberbullying_modules

Cook, S. (2024). *Cyberbullying data, facts and statistics for 2018–2024*. Comparitech. Retrieved from https://www.comparitech.com/internet-providers/cyberbullying-statistics/

Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Opened for signature November 23, 2001; entered into force July 1, 2004.

Cyberbullying Research Center. (2024). *2023 cyberbullying data*. Retrieved from https://cyberbullying.org/2023-cyberbullying-data

Digital Rights Foundation. (2024). *Cyber harassment helpline report 2023*. Retrieved from https://digitalrightsfoundation.pk/wp-content/uploads/2024/04/DRFs-Cyber-Harassment-Helpline-Report-2023.pdf

eSafety Commissioner. (2024). *Cyberbullying*. Retrieved from https://www.esafety.gov.au/key-topics/cyberbullying

Espelage, D. L., & Hong, J. S. (2017). Cyberbullying prevention and intervention efforts: current knowledge and future directions. *The Canadian Journal of Psychiatry*, *62*(6), 374-380.

European Union Agency for Fundamental Rights. (2014). *Violence against women: An EU-wide survey*. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf

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

Hellfeldt, K., López-Romero, L., & Andershed, H. (2019). Cyberbullying and Psychological Well-being in Young Adolescence: The Potential Protective Mediation Effects of Social Support from Family, Friends, and Teachers. *International journal of environmental research and public health*, 17(1), 45.

Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of suicide research*, *14*(3), 206-221.

Hinduja, S., & Patchin, J. W. (2014). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Corwin Press.

Hinduja, S., & Patchin, J. W. (2022). *Cyberbullying: Identification, prevention, and response*. Cyberbullying Research Center. Retrieved from https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2022.pdf

INTERPOL. (n.d.). *Cybercrimes cross borders and evolve rapidly*. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime

Iqbal, S., & Jami, H. (2022). Exploring definition of cyberbullying and its forms from the perspective of adolescents living in Pakistan. *Psychological studies*, *67*(4), 514-523.

Jamil, S. (2020). Suffering in silence: The resilience of Pakistan's female journalists to combat sexual harassment, threats and discrimination. *Journalism Practice*, *14*(2), 150-170.

Jane, E. A. (2016). Misogyny online: A short (and brutish) history.

Johansson, S., & Englund, G. (2021). Cyberbullying and its relationship with physical, verbal, and relational bullying: A structural equation modelling approach. *Educational Psychology*, *41*(3), 320-337.

Kamboyo, S. H. (2024). *Cybercrime investigation agency: A panacea for all digital ills*. The Express Tribune. Retrieved from https://tribune.com.pk/story/2467358/cyber-crime-investigation-agency-a-panacea-for-all-digital-ills

Kamran, A., Arafeen, Q. U., & Shaikh, A. A. (2019). Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. *International Journal of Cyber-Security and Digital Forensics*, *8*(3), 241-250.

Kaur, M., & Saini, M. (2023). Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions. *Education and Information Technologies*, *28*(1), 581-615.

Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a digital future: How hopes and fears about technology shape children's lives*. Oxford University Press, USA.

Macnish, K. (2017). *The ethics of surveillance: An introduction*. Routledge.

Meera Shafi etc. Vs. Federation of Pakistan etc. (2021). *Writ Petition No. 24397/2021*. Lahore High Court, Lahore.

Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *Cyberpsychology & behaviour*, *12*(4), 387-393.

Mishna, F., Cook, C., Gadalla, T., Daciuk, J., & Solomon, S. (2010). Cyberbullying behaviours among middle and high school students. *American Journal of Orthopsychiatry*, *80*(3), 362-374.

Moreno, M. A., Midamba, N., Berman, H. S., Moreno, P. S., Donlin, M., & Schlocker, E. (2019). Cyberbullying among adolescents: stakeholder-driven concept mapping approach. *JMIR Pediatrics and Parenting*, *2*(1), e12683.

National Crime Prevention Council. (2009). Information and resources to curb the problem of cyberbullying. Retrieved from https://www.ncpc.org/resources/cyberbullying/#

Niederman, F., & Baker, E. W. (2023). Ethics and AI issues: old container with new wine?. *Information Systems Frontiers*, *25*(1), 9-28.

O'Brien, N., & Moules, T. (2010). The impact of cyber-bullying on young people's mental health.

Office for National Statistics. (2024). *Bullying and online experiences among children in England and Wales: Year ending March 2023*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/bullyingandonlineexperiencesamongchildreninenglandandwales/yearendingmarch2023

PACER. (2022). Cyberbullying. Retrieved from https://www.pacer.org/bullying/info/cyberbullying/

Pakistan Telecommunication Authority. (2023). Annual report 2023. Retrieved from https://www.pta.gov.pk/assets/media/pta_annual_report_12022024.pdf

Pedersen, W., Bakken, A., Stefansen, K., & von Soest, T. (2023). Sexual victimization in the digital age: A population-based study of physical and image-based sexual abuse among adolescents. *Archives of sexual behavior*, *52*(1), 399-410.

Phillips, W. (2015). *This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture*. MIT Press.

Plunkett, L. A. (2019). *Sharenthood: Why we should think before we talk about our kids online*. MIT Press.

Prevention of Electronic Crimes Act, 2016 (PECA) (Pakistan).

Qureshi, S. F., Abbasi, M., & Shahzad, M. (2020). Cyber harassment and women of Pakistan: analysis of female victimization. *Journal of Business and Social Review in Emerging Economies*, *6*(2), 503-510.

Reynolds, K., Kontostathis, A., & Edwards, L. (2011, December). Using machine learning to detect cyberbullying. In *2011 10th International Conference on Machine Learning and Applications and Workshops* (Vol. 2, pp. 241-244). IEEE.

Sahoutara, N. (2022). *FIA told to submit reports on hundreds of cybercrime complaints within 15 days*. Dawn. Retrieved from https://www.dawn.com/news/1667998

Saleem, S., Khan, N. F., & Zafar, S. (2021). Prevalence of cyberbullying victimization among Pakistani Youth. *Technology in Society*, *65*, 101577.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian journal of psychology*, *49*(2), 147-154.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, *49*(4), 376-385.

Smith, P., & Steffgen, G. (Eds.). (2013). *Cyberbullying through the new media: Findings from an international network*. Psychology Press.

Sohail, M., & Durrani, R. (2023). *Digital rights in Pakistan: A review of 2023*. Digital Rights Foundation. Retrieved from https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Digital-Rights-in-Pakistan_-A-Review-of-2023-1.pdf

Sorrentino, A., Sulla, F., Santamato, M., di Furia, M., Toto, G. A., & Monacis, L. (2023). Has the COVID-19 Pandemic Affected Cyberbullying and Cybervictimization Prevalence among Children and Adolescents? A Systematic Review. *International journal of environmental research and public health*, 20(10), 5825.

Spyropoulos, F. (2025). Techno-Ethical and Legal Aspects of Cyberbullying: Structural Analysis of Power Imbalances in the Digital Sphere. *Journal of Digital Technologies and Law*, *3*(3), 472-496.

UNICEF. (2024). Cyberbullying: What is it and how to stop it. Retrieved from https://www.unicef.org/end-violence/how-to-stop-cyberbullying

Usman, M. (2017). cybercrime: Pakistani perspective. *Islamabad Law Review*, *1*(03), 18-40.

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*(1), 63-72.

Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research Press.

World Health Organization. (2020). *Mental health considerations during the COVID-19 outbreak*. Retrieved from https://iris.who.int/bitstream/handle/10665/331490/WHO-2019-nCoV-MentalHealth-2020.1-eng.pdf?sequence=1

Yang, B., Wang, B., Sun, N., Xu, F., Wang, L., Chen, J., ... & Sun, C. (2021). The consequences of cyberbullying and traditional bullying victimization among adolescents: Gender differences in psychological symptoms, self-harm and suicidality. *Psychiatry Research*, *306*, 114219.

Zhou, S. (2021). Status and risk factors of Chinese teenagers' exposure to cyberbullying. *SAGE Open*, *11*(4), 21582440211056626.