ACADEMIA International Journal for Social Sciences
Volume 4, Issue 4, 2025 ISSN-L (Online): 3006-6638

A Comparative Study of Pakistani and International Laws on Online Harassment: Challenges and Opportunities

Shahla Gull
shahla.gull@uog.edu.pk
Assistant Lecturer University of Gujrat, Department of History

Muhammad Babar Shaheen
bsharal@yahoo.com
Lecturer, College of Law, Government College University, Faisalabad

Dr. Noreen Akhtar
noreen.butt@ymail.com
Assistant Professor in Law, GC University Faisalabad
Corresponding Author: * Shahla Gull shahla.gull@uog.edu.pk

Received: 11-09-2025 **Revised:** 08-10-2025 **Accepted:** 24-10-2025 **Published:** 03-11-2025

ABSTRACT

The paper is a comparison of the legal provisions in Pakistan regarding online harassment and newer international strategies in Europe, United Kingdom, United States, India, and Australia. The research depends on a qualitative doctrinal approach close reading of the statutes, regulatory guidance and intergovernmental reports and discusses definitions, scope, platform obligations, enforcement structures, remedies and due-process protections. It identifies the Prevention of Electronic Crimes Act, 2016 (PECA) and other instruments used in Pakistan as having significant points of attack against cyberstalking and crimes against dignity and modesty, but it is still not well-coordinated between criminal law and protection-based systems in the workplace, and the ability to apply it is uneven. International Newer platform-duty regimes (EU DSA, UK Online Safety Act, Australia Online Safety Act) place responsibilities on intermediaries, which have a risk assessment, removal order, and transparency requirement; whereas the U.S. mostly retains a riveter-of-news role under Section 230, and India is qualifying safe-harbor on due diligence under its Intermediary Rules 2021. The article names lack of definition, evidence and jurisdictional barriers, resource limitations, and threats to speech as the challenges and proposes opportunities that can help Pakistan modernise its situation through defining the offences (e.g., doxxing, deepfakes), enhancing victim-centred processes, and applying moderated platform-duty and transparency frameworks.

Keywords: *Online Harassment, PECA 2016, Doxxing, Deepfakes, Cyberstalking*

INTRODUCTION

Online harassment has become one of the most widespread issues in the digital era that includes the following behaviors: cyberstalking, doxxing, non-consensual distribution of intimate images, impersonation, and targeted online hate. Such activities do not only undermine the autonomy and privacy of individuals but also undermine the democratic participation by silencing the voices of the marginalized and discouraging civic participation (Faisal et al., 2024). The emergence of social media has only made the latter forms of abuse even more pronounced, the contexts in which offenders can operate anonymously and whose impact on legal systems is typically not effectively addressed through traditional means (Shaheen et al., 2024). Therefore, states across the world have been trying to modernize their systems of law to fight these new forms of digital evils.

The most important legal framework that regulates online crimes in Pakistan is the Prevention of Electronic Crimes Act (PECA) 2016. PECA also criminalizes cyberstalking, unauthorized access of personal data, as well as the delivery of defamatory or obscene information by electronic means (Ahsan & Ali, 2025). The Federal Investigation Agency (FIA) has also been given powers by the law to investigate and prosecute cybercrimes. In addition to PECA, the Protection against Harassment of Women at the Workplace (amendment) act 2022 broadens protection against online harassment in the workplace since online harassment is no longer limited to physical space as it is becoming more and more a daily occurrence (Javed et al., 2025). Regardless of such phenomenon, critics believe that tools and mechanisms of enforcement are still weak, and procedural protections are limited to combat the cross-jurisdictional and complex character of online harassment (Thakur & Kumar, 2019).

Relatively, foreign jurisdictions have embraced various practices. Digital Services Act (DSA), which was introduced in the European Union in 2024, was a paradigm shift of reactive criminalization to proactive regulation of internet-based platforms. It gives rise to due-diligence duties, in which platforms have to evaluate and reduce systemic risk comprising unlawful material and cyber-abuse (Butt et al., 2023). Likewise, the Online Safety Act 2023 of the United Kingdom puts in place statutory obligations of care on social media companies so that they can protect their users, particularly underage users, against harmful or unlawful content (Ofcom, 2024). The eSafety Commissioner has the power to issue an order to remove abusive content and enforce compliance by the service provider under the Online Safety Act 2021, in Australia (Naseri et al., 2021).

On the other hand, the United States still leans strongly on Section 230 of the Communications Decency Act (1996) granting the internet intermediaries widespread immunity on third party material. Though this provision has played a key role in safeguarding free expression, it has also restricted victims who want to take action against the platforms that host or ignore the contents that are harmful (Gillespie, 2018). In India, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 include the so-called moderation by prioritizing intermediary immunity based on due diligence, including the introduction of grievance officers and the removal of illegal content as quickly as possible (Qureshi et al., 2020).

The current comparative research takes the qualitative, doctrinal method and uses it to assess the law structure of Pakistan regarding the alignment or deviation of the legal framework to these international models. The analysis is based on three aspects: (1) substantive definitions of online harassment and related crimes; (2) the mechanisms of procedures and enforcement that are offered to the victims; and (3) the responsibility distribution between an individual wrongdoer and a digital intermediary. The paper will endeavor to suggest the best practices and possible reforms that can enhance the ability of Pakistan to deal with online harassment without putting the freedom of expression and due process at risk by comparing legislative responses by the best international jurisdictions.

METHODOLOGY

The study follows a qualitative doctrinal approach to review and contrast the legal systems of dealing with online harassment in Pakistan and the chosen international jurisdictions. The doctrinal approach is concerned with the analysis of the existing laws, statutes and legal principles in order to comprehend how various systems conceptualize, define and regulate the online harassment (Hutchinson and Duncan, 2012). The fact that it focuses on interpretation, context, and meaning as opposed to quantitative measurement makes it qualitative.

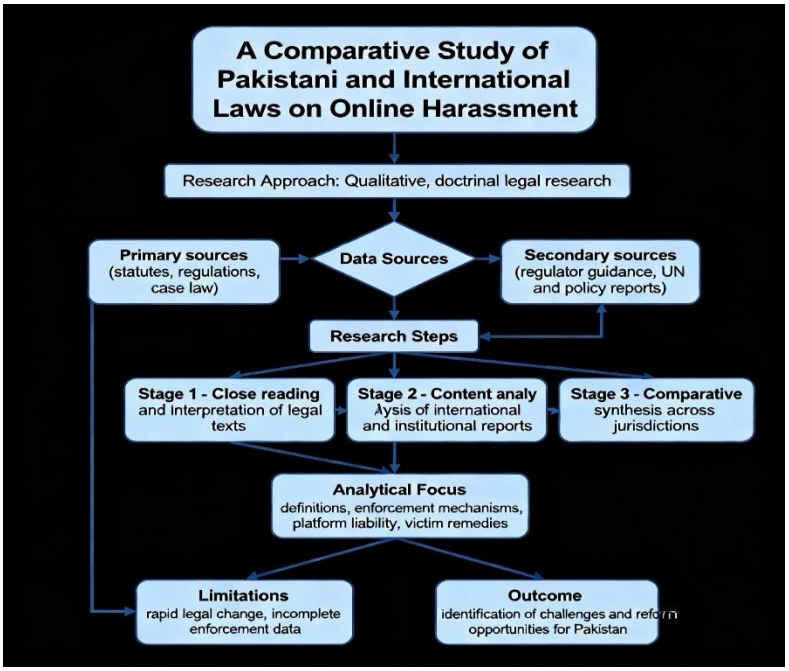

Figure 1: Methodology Structure

The research process is carried out in three major steps. First, it will entail a close-up analysis of primary legal sources, such as statutes, rules, and official explanatory sources. In Pakistan, the Prevention of Electronic Crimes Act (PECA) 2016 and the Protection against Harassment of Women at the Workplace (Amendment) Act 2022 are in the center of attention. To be compared, the international acts of the European Union Digital Services Act (2024), the United Kingdom Online Safety Act (2023), the Australian Online Safety Act (2021), the United States communications Decency Act (Section 230), and the Indian Information Technology Rules (2021) are examined.

Second, normative and human-rights-based criteria against which sufficiency of such legal responses can be assessed is that of a content analysis of regulatory guidance, judicial commentary, and reports of international organizations including the United Nations and UN Women. This assists in establishing a context of domestic legislation as per the international norms of internet safety, dignity and freedom of expression. Third, the research makes a comparative synthesis of different jurisdictions to discover similarities and differences in the structure of the legislation, enforcement tools, and responsibility of the platforms. There were no human participants to consider and, hence, there was no necessity of an ethical approval. Lastly, this research paper recognizes some of the weaknesses such as the dynamic nature of cyber laws, the difference in the degree of transparency in implementation, and lack of access to official information. In spite of these limitations, the qualitative doctrinal method enables the systematic, context-sensitive, and normative assessment of the law of response to online harassment.

LEGAL FRAMEWORKS

It is in this section where I have given a thorough study of the legal provisions that cover the online harassment in Pakistan and the five foreign jurisdictions, which are: the European Union (EU), the United Kingdom (UK), the United States (US), India, and Australia. The discussion brings to focus the conceptualizations of these legal systems regarding online harassment, outline platform responsibilities, and implement systems of victim protection. Both frameworks portray different strategies through which privacy, dignity, and freedom of expression could be balanced in the digital era.

Pakistan

Core Statutes and Scope

The main law that regulates the cybercrimes in Pakistan is the Prevention of Electronic Crimes Act (PECA) 2016, which was enacted to cope with the crimes that were carried out with the help of electronic systems and networks. PECA offers extraterritorial jurisdiction, that is, it governs crimes committed outside of Pakistan when they impact people and systems in the nation (Yongmei & Afzal, 2023). The legislation punishes a broad spectrum of the online harassment related offenses such as cyberstalking, unauthorized access to personal data, the spread of defamatory content and infraction of modesty and privacy. Particularly, Section 21 punishes the crimes committed against the dignity of an individual, which includes sharing of intimate pictures without authorization, whereas Section 24 is a crime of cyberstalking, which is broadly defined as the monitoring, contacting, or harassment of another person by using electronic means(Aleem et al., 2021).

Under PECA, implementation and enforcement is conducted through the Federal Investigation Agency (FIA) and its National Response Centre of Cyber Crimes (NR3C) and investigates complaints lodged via the official platforms like complaint.fia.gov.pk. The FIA has a right to gather evidence, charge criminals, and arrange partnership with internet service providers to retrieve data and delete the content (Haq & Zarkoon, 2023).

Besides PECA, there is also a similar legal framework dealing with workplace-related online misconduct in the Protection against Harassment of Women at the Workplace Act 2010 (amended 2022) of Pakistan. The amendment provided protection to the digital areas, acknowledging the fact that harassment online, such as that through messaging applications, email, or various social media, is a type of misconduct in the workplace (Zahid et al., 2024). This enlargement represents a recognition of the hybrid and remote working conditions, making sure that the harassment of the virtual work environment is compared to the offenses committed in the physical workplace.

Observations

Although PECA is a broad-based language, there are still existing gaps in how the new types of digital harm, such as doxxing (public release of personal information), deep fake pornography, and organized online harassment campaigns, are tackled. In 2016, these issues did not feature prominently in legislative discussions, so they remain unclear in terms of whether they are covered by the current laws (Lu et al., 2022). The excluded communities like transgender or eunuchs are harassed by the male community in Punjab, Pakistan (Rafiq-uz-Zaman et al., 2025). In addition, the civil redress of victims including injunctions or damages is restrained because PECA is mainly criminal in nature, with a restorative or compensatory justice being secondary to the punitive one.

The other ongoing problem is the issue of capacity to enforce and accessibility. Victims especially women and marginalized people have complained of trouble in the process of filing complaints, uneven reliability of FIA cyber units, and little knowledge of legal solutions to the problem (Sherwani & Zia, 2023). Differences in provincial infrastructure are also reasons of unequal implementation results. PECA does not place any statutory obligations on intermediaries at the platform level, other than in collaboration in investigations and data retention requirements. Takedown systems are extensively based on self-organized cooperation with such platforms as Facebook and Twitter, which are governed by their internal community rules, but not domestic law (Shah, 2024). Thus, the system in Pakistan is still perpetrator-focused, and criminal responsibility is in the spotlight of regulation of digital intermediaries, as opposed to systemic or preventive regulation.

Nevertheless, the privacy, dignity, and cyberstalking features of PECA is a significant move in fighting cyberstalking. It has extraterritorial jurisdiction which enables cross border application and this is necessitated by the global nature of cyber offenses. Nonetheless, there is still a need to further modernize the legislation so as to address the discrepancy between conventional legal terms and the modern online harms.

European Union

One of the most extensive legal frameworks in the world to regulate online platforms is the Digital Services Act (DSA) that comes into effect in 2024 by the European Union. The DSA no longer focuses on criminalizing individual offenders but rather makes digital intermediaries set systemic responsibility and hold them accountable, transparent, and risk-averse (Müller & Kettemann, 2024). The DSA proposes varying accountabilities to the various types of online actors: intermediary services, hosting services, and very large online platforms (VLOPs) according to their size and the social effect they have. Some of its most important provisions are due-diligence obligations which entail platforms, the establishment of effective notice-and-action systems of the elimination of unlawful content, clear terms of service, and disclosure of moderation decisions (Atzori, 2024). Most importantly, the DSA requires risk assessment and mitigation of VLOPs to detect the systemic risks, i.e., disinformation, online harassment, and gender-based violence. It is mandatory that independent audits are performed to ensure compliance by platforms and researchers have access to platform data to facilitate transparency (Novovic, 2024). The European Commission still has the right to enforce, and it is able to impose the fines up to 6% of worldwide yearly turnover in case of non-compliance. When considering the issue of online harassment, the focus on procedural accountability that the DSA took as opposed to the emergence of the new criminal offenses represents a major change in the philosophy of the policy. It acknowledges that digital harms can only be tackled by platform governance and user protection systems and not only by conventional criminal prosecution.

United Kingdom

The areas covered by the Online Safety Act 2023 of the United Kingdom also address platform responsibility as opposed to just broadening the criminal law. The Act imposes commercial responsibilities of care of user-to-user and search services, requiring companies to curb the spread of unlawful content, to keep users off dangerous content, and to protect children on the Internet (Fenwick & Coe, 2025). It is supervised by the Office of Communications (Ofcom) that has the authority to provide codes of practice, inquire about violations, and fine a significant amount of money in case the rules are not followed. According to the Act, the platforms will have to put in place active systems and procedures to ensure that illegal or harmful contents are minimized, including a mechanism to authenticate the age of users and those provided with content filters (Farrand, 2024).

The implementation of the Online Safety Act is in stages, and the initial compliance obligations will be in operation in March 2025. The advice provided by Ofcom also defines what the Act entails, in particular, which online services can be subject to regulatory supervision, e.g. social networks, video-sharing websites, and messaging applications. Unlike PECA, the model of the UK pays much attention to preventive regulation, which is one that makes sure that the intermediaries actively participate in risk reduction. It combines both criminal responsibility and administrative control, providing a two-tiered way of digital harms (Gosztonyi & Lendvai, 2024).

United States

Online harassment in the United States is handled in a piecemeal manner by a combination of both federal and state laws. On the federal level, 18 U.S.C.37 2261A makes it a crime to stalk and harass a person, including in cases where the criminal utilizes electronic communications, with the intent of the person causing fear or significant emotional distress (Filmeridis et al., 2024). This provision gives a chance to prosecute cyberstalking cases which cross the national borders or state lines. Nevertheless, the U.S. legal context is characterized by a prevalence of Section 230 of the Communications Decency Act (1996) that offers online platforms heavy immunity against legal responsibility on the content that has been posted by derivatives (Bachmann et al., 2025). Though Section 230 has been celebrated as a source of free expression and innovation, it has been criticized as a way to make platforms evade responsibility in hosting or not hosting harmful and harassing content (Flesaker et al., 2025).

On a state level, different jurisdictions have issued cyber-harassment laws that criminalize on-line threats, revenge pornography, and stalking. As an example, the Penal Code of California (653.2) forbids electronic communication that is supposed to intimidate or harass someone, whereas in New York and Texas, the non-consent to share images is criminalized (Al Nagrash et al., 2024). Reform initiatives are still debating whether the First Amendment has provided the extent of platform liability and free speech. Though the U.S. model gives more emphasis on freedom of expression, it offers minimal avenue to the victims who wish to hold the intermediaries responsible to the victims- a primary difference with the EU and UK models.

India

The Rules to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) of 2021 which was promulgated under the Information Technology Act, 2000, govern the liability of online intermediaries. The regulations create a conditional safe harbour regime, whereby platforms will be exempted when liable provided they comply with recommended due diligence duties(Mythili & Nagamani, 2025).

These obligations include:

- Establishment of grievance officers to deal with complaints and liaise with law enforcement.
- Content takedown processes are executed within the given time constraints after a legal notification is received.
- The release of the name of the initial source of information when authorities are asked to do so in situations of severe crimes like online harassment or violation of national security.
- Other conditions requiring important social media intermediaries, including the traceability of messages and the requirement to report compliance.

The Indian model is one of the hybrid models that finds a balance between regulatory accountability and intermediary immunity. It highlights the attention of the government to the responsibility of the platforms and transparency of the procedures without violating the freedom of speech within the rules of the constitution. Nonetheless, opponents disapprove that traceability requirements can ignite privacy of users and end-to-end encryption, which is a matter of concern regarding surveillance and abuse (Lal et al., 2024). However, the history of the evolution of regulations in India shows that the country attempts to adjust the legal frameworks to the mass digital communication and cross-platform harassment realities.

Australia

The Online Safety Act 2021 of Australia is a well-developed victim-focused measure against online violence and abuse. The Act, which is given by the eSafety Commissioner, builds upon earlier laws about

cyber-safety and establishes a system of complaints and stringent enforcement (Wood et al., 2021). By the Act, one may bring a complaint regarding cyberbullying, adult cyber-abuse, image based abuse and harmful online material. eSafety Commissioner has the authority to give removal notices to sites and individuals requiring them to remove hateing content within 24 hours. Avoidance may attract hefty fines or restriction of services. The Act is also explicit in the procedure that can be followed by the complainants so that they are accessible and addressed in a timely manner (Baker, 2021). Australia is unique in its focus on child protection and efficiency of its administration. In contrast to the criminal-intensive model in Pakistan, the Australian system is based on regulatory enforcement and remedial interventions and provides victims with a quicker and more viable way of redressing as well.

Comparative Overview

The six jurisdictions show that there are differences in the philosophy of dealing with online harassment.

- Pakistan has mostly depended on the criminal law, where the focus is on punishing the offenders but does not have any systematic controlling responsibilities to platforms.
- EU, UK and Australia have regulatory systems that focus on platform responsibility, disclosure and procedural protections.
- The U.S. gives precedence to free expression and immunity of intermediaries, which leads to restricted, platform, liability.
- India adopts a compromise strategy, which trains immunity on the conditioning of due diligence compliance.

Summing up, PECA 2016 provided a much-needed base to combat cyber harassment in Pakistan but needs some modernization to cover harms developed in the sphere and improve in accordance with international standards. The capacity of the Pakistani government to address digital harassment and balance constitutional rights by introducing more transparent platform responsibilities, enhancing victim support mechanisms, and more inter-agency coordination may help (Hussain et al., 2023).

ONLINE HARASSMENT COMPARATIVE LEGAL ANALYSIS.

This segment of the paper draws a comparative study of the legal frameworks that deal with online harassment in the United Kingdom (UK), the United States of America (US), the European Union (EU), and India respectively. It also talks about the definition of online harassment by these jurisdictions, the role played by digital platforms, the way harassment can be enforced and the possible remedies that victims can seek. The analysis also reflects the new difficulties in addressing the issue of online harassment and provides the information about the possible reforms and the emphasis on the disparities of definitions, platform responsibilities, distribution of enforcement structures, and support systems to victims.

The following definitions and protected interests will be used in this case:

Pakistan

PECA 2016 is the main law in Pakistan on cybercrimes, including on-line harassment. It also criminalizes cyberstalking, crimes against personal dignity and modesty, and violations of privacy where the clauses involve sharing explicit material without consent (Section 21) and stalking electronically (Section 24) (Saeed et al., 2025). Though PECA covers general types of online harassment, PECA does not specify new types of abuse like doxxing (publication of personal information), deep fake sexual abuse (manipulated video or image), and organized harassment or brigading (harassment mounted by groups). Such actions, which became increasingly widespread with the emergence of digital technology, are still somewhat unregulated since the statute cannot keep up with the latest types of abuse(Javaid, 2025).

Also, the Protection against Harassment of Women at the Workplace Act (2010) (modified in 2022) now applies to online services, which encompasses online harassment within the workplace. Nevertheless, the scope of this legislation is rather narrow in harmful conditions in professional environments, and it does not cover as many more extensive types of online harassment in non-work-related matters (Cheema et al., 2019).

Table 1

Type of Harassment	Legal Addressed in Pakistan
Cyberstalking	Section 24, PECA 2016
Doxxing	Not explicitly addressed
Deepfake Sexual Abuse	Not explicitly addressed
Workplace Harassment	Protection against Harassment of Women at the Workplace Act (2010, amended 2022)

EU/UK/Australia

Unlike Pakistan, EU, UK and Australia have applied more procedural and broad approaches to the area of online harassment, targeting inappropriate categories of illegal content instead of enshrining all the possible types of harassment. These frameworks give due-diligence responsibilities on platforms that they must analyze and address the risks of illegal or harmful content that includes harassment, hate speech, and material that promotes child sexual abuse.

European Union: The Digital Services Act (DSA) was adopted in 2024, which focuses on a large platform, requiring it to evaluate the risk of its service and take actions to alleviate any harm. This comprises the removal processes, appeal system, and transparency reports on content moderation systems. DSA does not seek to establish the specific subtypes of each subtype of harassment but requires the platforms to act on illegal materials and malicious conduct, using internal systems (Farooq & Ali, 2022).

United Kingdom: The Online Safety Act 2023 is no exception since it is concerned with illegal content, but the provisions address a wide spectrum of crimes, including cyberbullying and hate speech on the Internet. The Act imposes on platforms to have a system that helps to detect and curb harm, such as children being exposed to harmful materials, but once again, fails to mention all forms of online harassment. Rather, it focuses on platforms, which helps to establish systems that can mitigate various bad practices, such as harassment (Alhaboby et al., 2021).

Australia: Under the Online Safety Act 2021, the eSafety Commissioner has the authority to issue removal notices to harmful content, and in doing so is especially concerned with child protection and cyber bullying of children. It focuses on procedural responsibilities instead of spelling out all of the subtypes of harassment. The platforms should adhere to certain timeframes to remove toxic content and offer the platform users a chance to appeal decisions (Reed et al., 2020).

Table 2

Type of Harassment	Legal Addressed in EU/UK/Australia
Cyberstalking	Risk mitigation, removal of harmful content
Doxxing	Removal of illegal content, transparency reports
Deepfake Sexual Abuse	Harmful content removal
Workplace Harassment	Workplace-specific protections in the UK

U.S./India

Criminal law is more central in the U.S. and India as a means of solving online harassment, especially in the area of stalking and threats.

United States: Cyberstalking is criminalized under 18 U.S.C. 2261A when either of the following is met: it requires the element that the stalking occurs across the state line or that the stalking causes fear or emotional distress (Legal Information Institute, 2023a). Nonetheless, there is a number of new types of harassment, which are not explicitly stipulated by the U.S. laws (e.g., doxxing or deepfakes). Rather, liability protection to platforms is mostly covered under Section 230 of Communications Decency Act, which immunizes a platform against liability based on user-generated content, but there are exceptions to federal crimes, intellectual property infringement, and sex trafficking (Reed et al., 2020).

India: The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 regulates the platform immunity on how to meet the due-diligence requirements, such as taking down the harmful content within the stipulated deadlines (Ministry of Electronics and Information Technology, 2021). The regulations indirectly influence the issue of online harassment because it puts the burden of controlling the content and responding to grievances in due time on the platforms. Nevertheless, there is still no definitional clarity on most types of online harassment.

Table 3

Type of Harassment	Legal Addressed in U.S./India
Cyberstalking	18 U.S.C. § 2261A (U.S.)
Doxxing	Indirectly addressed in both countries
Deepfake Sexual Abuse	Not explicitly addressed
Workplace Harassment	Not addressed directly

Platform Duties & Liability

Pakistan

In Pakistan, there is no statutory duty-of-care regime of platforms against online harassment. PECA 2016 covers the needs of cooperation like the ability to respond to law enforcement requests and remove harmful content where it is needed. These obligations are however presented in a more procedural obligation, but not as systemic regulatory obligations. Platforms are not legally obligated to develop internal content moderation policies or even proactively determine and avert harassment (Imam, 2024).

Table 4

Platform Duty	Pakistan
Content Moderation	Voluntary, based on cooperation
Proactive Identification of Harmful Content	Not required
Transparency and Reporting	Not mandated

EU/UK/Australia

Conversely, the EU, UK, and Australia explicitly statutorily require the platforms to be safe and transparent to users. These responsibilities are accompanied by control and control tools:

European Union: The Digital Services Act (DSA) requires platforms to implement the risk mitigation measures, such as the routine risk assessment and content moderation practices auditing. The platforms

should include easy access to content moderation policies and access to researchers to ascertain adherence (Abbas et al., 2024).

United Kingdom: The Online Safety Act 2023 gives platforms statutory responsibilities of care to ensure harm is avoided and users, including children, are not harmed by any illegal material (Ofcom, 2024). It should also be through platforms that ensure that good appeal procedures are available and transparency reports are also up to date in order to show that they are upholding these responsibilities.

Australia: The Online Safety Act 2021 compels a platform to offer a straightforward route of complaints and appeals by any user who fell prey to harmful content. The eSafety Commissioner works with compliance, such as sending notice of removal of cyberbullying or other harmful materials (Khan, 2022).

Table 5

Platform Duty	EU/UK/Australia
Content Moderation	Required, with clear policies
Proactive Identification of Harmful Content	Mandated through risk assessments
Transparency and Reporting	Required, including reporting compliance

U.S./India

In the US, the Communications Decency Act, Section 230 of the law still protects platforms against liability on actions by users with some exceptions on particular crimes. This has resulted in failure of proactive regulatory responsibilities on platforms as far as in moderating harmful content is concerned. Nevertheless, it is becoming more controversial whether this protection ought to be revisited and made more accountable to platforms in case of user-generated harassment (Gillespie, 2018). In India, the Intermediary Guidelines and Digital Media Ethics Code (2021) establishes an exceptionally safe harbor on platforms in India that need to take certain due-diligence measures. This involves the placement of the grievance officers, content moderation, and compliance reporting within designated timeframes (Prabhkaran & Rameshkumar, 2025). Although this is a better solution, it is not a proactive system, but a reactive one, which prevents bad behavior.

Table 6

Platform Duty	U.S./India
Content Moderation	Indirectly addressed
Proactive Identification of Harmful Content	Not required
Transparency and Reporting	India: Required

Enforcement Architecture

Pakistan: Cybercrimes are enforced in Pakistan through the centralized Federal Investigation Agency (FIA) that houses the National Response Centre of Cyber Crimes (NR3C). The complaints may be made through official complaint portal (complaint.fia.gov.pk), and FIA is mandated to conduct investigation and prosecute the offenses involving the cyber world. But the problem is there is a lack of resources, hence there are usually delays in the investigations as well as some problems with the support of the victims, particularly in the country.

EU/UK/Australia: Administrative regulators are important enforcers in such jurisdictions. Sanctioning powers to impose fines on platforms that do not comply, issue removal orders, and carry out an audit to assess the content moderation practices of platforms are all granted to the European Commission, Ofcom (UK), and the eSafety Commissioner (Australia).

U.S: The criminal system of the U.S. punishes cyberstalking and harassment with federal laws like 18 U.S.C. 2261A. It is, however, not easy to directly implicate platforms in terms of liability under Section 230 so that victims may seek responsibility on the part of a platform unless there is a particular criminal act,

Remedies & Victim Pathways

Pakistan: PECA gives sanctions to perpetrators of online harassment, such as incarceration and fines in Pakistan. The employment-related harassment may also be relieved by the victims using the laws of workplace harassment, whereby complaints are handled by the ombudsmen. Nevertheless, victim support systems are patchy and in many cases difficult to find and there are also complaints of long queues in processing complaints (Digital Rights Foundation, 2022).

EU/UK/Australia: These jurisdictions have an order of removal and appeals that are statutory. The users may ask to have the space cleared of such harmful material and the authorities (e.g. European Commission, Ofcom, eSafety Commissioner) can impose penalties. The DSA provides the EU with 6 percent affected turnover as a fine in case of non-compliant platforms (European Commission, 2024).

In the comparative analysis, it is observed that countries have similarities and differences in their regulation and response to online harassment. Although PECA offers an effective starting point in dealing with cybercrimes in Pakistan, its imprecision in listing the new types of online abuses and platform responsibilities creates loopholes in addressing of such intricate cybercrimes as doxxing, deepfakes, and organized harassment. Conversely, some jurisdictions, such as the EU, UK, and Australia, have put up stronger systems, where platforms do have regulatory obligations, with removal notices enforced and procedural protectors to the victims. The U.S. and India are both interested in criminal law, though the application of platform immunity pursuant to Section 230 in the U.S. and its due-diligence approach in India presents some unique problems.

In the case of Pakistan, the addition of specific definitions of the new types of harassment, more rigorous platform regulation, and more victim-supportive procedures would greatly help the country to stop online harms against its people.

KEY CHALLENGES

Definitional Gaps, Evidentiary Gaps

The absence of clear legal definitions of new forms of abuse (deepfakes or manipulated videos or images) and doxxing (publication of personal information) is one of the most severe issues in dealing with online harassment. Such actions have developed quickly with the development of digital technologies, much faster than the current laws such as PECA 2016 (Government of Pakistan, 2016). These types of harassment are not specifically covered in the legislation and this creates huge loopholes in protection. Moreover, the standards of proof of such crimes, particularly of digital forensics, are quite high. The fact that online abuse is attributed to particular offenders, particularly when perpetrators of online abuse are anonymous or pseudonymous, makes the legal process of prosecution and victim redress more challenging regardless of jurisdiction (Pakistan Code, 2016).

Jurisdiction Cross-border enforcement

Although the extraterritorial provision of PECA can be taken to respond to cybercrimes targeting the Pakistani nationals, no one can easily cooperate through mutual legal assistance and cross-border enforcement. Through legal frameworks, lack of proper data-sharing policies, and slow feedback to takedown requests is common in international collaboration between law enforcement agencies. Although

such international authorities as the Digital Services Act (DSA) and other national lawmakers as Ofcom and the eSafety Commissioner provide enforcement mechanisms, timely redress remains an issue because of such jurisdictional frictions (European Commission, 2024; Ofcom, 2024). This is especially challenging in international cases, whereby digital evidence is saved on international servers.

Platform Accountability/ vs. Speech

Another important problem is the freedom of speech and platform accountability. The duty-of-care approach in the EU and UK (and the Section 230 immunity in the U.S.) can cause a net effect of over-removal of harmful content, stifling free speech, and the all-purpose consequence of the negation of harmful content and harassment in platforms (Congress.gov, 2023). This leads to the dilemma: How can one make sure of good moderation without violating the privacy and dignity and expression? To balance this, there must be a transparent governance model.

Constraints of Resources and Capacity

Lastly, insufficient resources and capability of digital forensics, training of investigators, and support of victims is a rampant problem. Advanced forensic technologies and experts are needed to examine complicated instances of digital abuse. According to the reports by UN Women, integrated responses to online violence against women and girls (VAWG) are needed not just in terms of technological capacity but with victim-centered services to offer proper legal and psychological assistance (UN Women, 2021).

OPPORTUNITIES FOR PAKISTAN

Explain and Overhaul Offense Definitions

The availability of a chance to revise and define terms of online harassment in the Prevention of Electronic Crimes Act (PECA) 2016 is one of the most burning opportunities in Pakistan. Other newer types of abuse like doxxing (public disclosure of personal information without permission), non-consentual sexual depictions made with deepfakes, and organized internet bullying or brigading, should be explicitly tackled by amendments. The law must be formulated to help clarify these crimes and proportional punishment and definite mens rea (intent) should be established to help penalize the offenders accordingly (Pakistan Code, 2016). This modernization would make the legal system of Pakistan up to date and efficient enough to combat the emerging world of digital abuse.

Bring in Calibrated Platform-Duty and Transparency Obligations

Pakistan has an opportunity to implement the large platforms administrative regulation based on the European Union Digital Services Act (DSA), UK Online Safety Act, and the Online Safety Act of Australia. Such rules mandate sites to have a system of notice and action, user appeals, transparency report and an assessment of harm of harassment. Pakistan must make these factors Pakistan specifics to its constitutional reality where there is a light but strict touch. Clarifying responsibilities of care would place the platforms in the position of actively finding, solving, and reducing online harassment (Starr, 2025).

Enhance Victim-Centered Procedures

The other potential opportunity is victim support strengthening. This is in addition to the standardization of time-bound takedown cooperation with platforms to promote the timely removal of bad material. Another way in which Pakistan can increase survivor support services such as legal assistance and psychosocial assistance is by extending it to women and disadvantaged populations who are frequently overrepresented in online harassment. Besides, the complaint portal provided by FIA can be improved

with new options like tracking the status and language assistance so that the victims feel well-informed and can use the portal effectively (Miller & Rolley, 2024).

Investigator and Judiciary Capacity Building

Pakistan is in dire need of capacity building amongst investigators as well as the judiciary. A regular training on digital evidence and deep-fakes forensics has to be conducted, and specialized bench books on cyber-harassment cases have to be developed. Integrated responses are necessary as stipulated by UN Women to effectively and comprehensively address digital abuse (Azhar et al., 2025). This would provide the law enforcing bodies and courts with means that would support dealing with sophisticated cases of digital harassment.

Access to Researcher Data (With Protection)

Another precaution that Pakistan may adopt to examine the dynamics of online harassment is by applying privacy-compliant data-access pilots, as in the case with the DSA researcher access model. Such data access programs may be useful to assess the effectiveness of the current policies, determine the trends in harassment, and shape future reforms (European Commission, 2024). One will have to be careful in order to guarantee privacy protection and adherence to international standards.

Workplace-Online Bridge

Last but not the least, the opportunity of operationalizing the amendments made to the Protection against Harassment of Women at the Workplace Act (2022) in the context of remote and hybrid workplaces is also an important opportunity. New regulations may imply the rules of evidence preservation on platforms and ombudsman-FIA referral procedures so that the harassment on the platform in the working place should be treated with the same severity as the one offline. This would establish a better guideline on how to support victims and offer legal retribution in digital workplaces (Mangi et al., 2025).

With the above opportunities, Pakistan would be able to refine their legal and procedural system in handling online harassment to provide better protection of the victims and hold the offenders accountable.

DISCUSSION

The comparative study of online harassment legislation shows that different jurisdictions apply the laws in different ways to achieve the desired goal of protecting victims, upholding free speech, and holding the platforms responsible in different ways. The framework of Pakistan, which is also based on the Prevention of Electronic Crimes Act (PECA) 2016, has a perpetrator-centric and criminal law-oriented nature by the virtue of its emphasis on the punishment of the people who have perpetrated the online harassment. This model considers online harassment one as a chain of criminal acts where the Federal Investigation Agency (FIA) is the body in charge of the responsibility. Although such a strategy does offer certain legal implications to violators, it does not offer a holistic framework to cover systemic risks created by digital platforms, including content moderation, and content prevention of abuse (Pakistan Code, 2016).

Conversely, a more regulative and platform-governance framework has been embraced in the European Union (EU), the United Kingdom (UK) and the Australia (AU) overlaying platform responsibilities with criminal law. Some of the laws enacted include the Digital Services Act (DSA) of the EU, Online Safety Act in the UK and Online Safety Act in Australia. These regulations provide a level of due diligence to platforms to control illegal or harmful content, provide transparent reporting and assessment of a systemic risk. It is concentrated on preemptive control of platforms, which means that they should be able to do everything to curb online harassment and other types of digital abuse prior to their transformation to criminal acts. It is a regulatory framework that platforms are not passive ways of users creating content,

but are active contributors to the harm prevention and reduction (European Commission, 2024; Ofcom, 2024; Federal Register of Legislation, 2021).

Instead, the United States is still largely dependent on Section 230 of the Communications Decency Act (CDA), which protects platforms against liability over the content created by users. Although this clause has played a major role in safeguarding freedom of speech, it also implies that the platforms are not held liable to any of the ill effects that users spread on their websites unless it is associated with certain unlawful behaviors such as sex trafficking or threats to life (Congress.gov, 2023). It has produced contradictory outcomes: high levels of protection of the speech, but low levels of responsibility of the platforms to respond to harassment or harmful information in time and in a clear way.

India offers a compromise with its Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These regulations offer platforms a conditional safe-harbor if they undertake the due diligence steps like appointing a grievance officer, acting on complaints by the users and removing the illegal content in a stipulated time. Although the latter puts more responsibility on the platforms than the U.S. model, it, nonetheless, leaves certain extent of responsibility on the self-regulation of platforms. The model adopted by India is a compromise between the freedom of speech and platform immunity, and the understanding that platforms should actively intervene in the elimination of online abuse (Ministry of Electronics and Information Technology, 2021).

In the case of Pakistan, an international model that is custom-made can be able to blend the strengths of these models. The criminal essence of PECA might be sustained so that such gross offenses as cyberstalking and revenge pornography could be duly punished. Nevertheless, an even more holistic solution would be that of introducing administrative platform responsibility so as to handle systemic risks, including the encouragement of harassment by the suggestion of algorithms, or platforms having an inadequate response to harmful content. The platforms must be obliged to adopt risk estimates, content control mechanisms and user complaints and all these would help in curbing abuse before it manifests into criminal activities.

Moreover, victim routes and support networks should be increased so that victims of online harassment could find access to the timely legal assistance, psychosocial support, and proper reporting channels. Pakistan can improve its capabilities to investigate and prosecute digital crimes effectively by investing in capacity building to the law enforcement and the judiciary and by safeguarding the right of the victims to their privacy and dignity as well.

The combination of a criminal law response to online harassment with platform governance and victim support would be the most effective way to have Pakistan facing online harassment in a transparent, comprehensive, and rights-respecting way. Through the examples of the EU, UK, AU, U.S., and India, Pakistan will be able to develop a flexible and adaptive legal framework reflecting the dynamically evolving digital environment and providing justice to the victims without breaching the basic rights of users.

CONCLUSION AND POLICY RECOMMENDATIONS

The existing model of dealing with online harassment, which is, until now, represented by the Prevention of Electronic Crimes Act (PECA) 2016, provides the premises to go about handling the cybercrimes but leaves much to be desired regarding new forms of digital criminality, such as doxxing and deepfakes. It is essential to revise PECA in order to adequately cover these new types of abuse so as to modernize and provide proper protection. Definitions are to be brought into conformity with global best practices, and the procedures of accelerated evidence conservation are to be legalized in order to easily instigate legal prosecution. There should be a regulatory layer that creates rules on platform-duty to large tech

companies. Such regulations must consist in notice- and action-procedures, system of user appeals, and transparency reports, and non-adherence should be clearly punished. The responsibilities must be different depending on the size and scale of the service and should make sure that small platforms are not overwhelmed and promote the big platforms to be more responsible of their broader impact on the society. In order to enhance procedural justice, victim-oriented channel of complaints should be refined. Ensure better enforcement of anti-harassment laws, such as the Women Protection Harassment Acts, to protect women in politics from verbal, physical, and online harassment (Malik et al., 2025).

These involve assured response times and in-built support services which provide legal, psychological and victim advocacy. Such open reporting by FIA to the public about dealing with cyber-harassment cases would enhance transparency and promote trust among the people (complaint.fia.gov.pk, 2023). By investing in digital forensics and judicial training capacity building, as well as access that preserve privacy to independent researchers, Pakistan can be more able to counter digital abuse. Lastly, cross-border templates and MOUs with the leading platforms should be promoted in order to ensure consistency with global standards, such as the DSA, and local laws are not ignored.

REFERENCES

Abbas, G., Kamal, M., Zahid, G. R., Bashir, S., Naveed, M. A., Jaffery, S., Imran, M., Farah, H., Farooq, U., & Mahmood, U. (2024). Equity And Accountability: Harassment And Electronic Crimes at Workplace in Pakistan, Its Physio-Psychological Effect on Victims, And Role of Legislative Initiatives to Prevent the Curse. International Journal for Electronic Crime Investigation, 8(4). https://www.researchgate.net/profile/Ghulam-Abbas-50/publication/387653324_Equity_And_Accountability_Harassment_And_Electronic_Crimes_at_Workplace_in_Pakistan_Its_Physio-Psychological_Effect_on_Victims_And_Role_of_Legislative_Initiatives_to_Prevent_the_Curse/links/6777605400aa3770e0d3197c/Equity-And-Accountability-Harassment-And-Electronic-Crimes-at-Workplace-in-Pakistan-Its-Physio-Psychological-Effect-on-Victims-And-Role-of-Legislative-Initiatives-to-Prevent-the-Curse.pdf

Ahsan, M., & Ali, F. (2025). The cost of speaking out: Cyber harassment and abuse against feminist activists in Pakistan. Media, Culture & Society, 01634437251360378. https://doi.org/10.1177/01634437251360378

Al Nagrash, A., Aldosari, T., Aldulaimi, S., Alsamman, A., & Lateef, M. (2024). Addressing the Menace of Cyber Harassment: Legislative Responses and Countermeasures. 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), 48–56. https://ieeexplore.ieee.org/abstract/document/10459485/

Aleem, Y., Asif, M., & Ashraf, M. U. (2021). The Prevention of Electronic Crimes Act 2016 And Shrinking Space for Online Expression in Pakistan. Ilkogretim Online, 20(2). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=13053515&AN=150154070&h=jxYc28AHD8pXpnn4GkEttvrpNZgUXjuwqcYFPIBMZIWtD%2BmO3RJtuaJPLMOnYV4T6iIs493%2FWF0mTK4TANYC8A%3D%3D&crl=c

Alhaboby, Z. A., Al-Khateeb, H. M., Barnes, J., Jahankhani, H., Pitchford, M., Conradie, L., & Short, E. (2021). Cyber-Disability Hate Cases in the UK: The Documentation by the Police and Potential Barriers to Reporting. In H. Jahankhani, A. Jamal, & S. Lawson (Eds.), Cybersecurity, Privacy and Freedom Protection in the Connected World (pp. 123–133). Springer International Publishing. https://doi.org/10.1007/978-3-030-68534-8_8

Atzori, M. (2024). The Digital Services Act and the Freedom of Expression in the European Union: A Political Perspective. Available at SSRN 4887181. https://www.researchgate.net/profile/Marcella-Atzori/publication/382542457_The_Digital_Service_Act_and_the_Freedom_of_Expression_in_the_European_Union_A_Political_Perspective/links/66a79a02c6e41359a84998ac/The-Digital-Service-Act-and-the-Freedom-of-Expression-in-the-European-Union-A-Political-Perspective.pdf

Azhar, S., Rizvi, S. A. A., & Asghar, U. (2025). Criminal Procedure Code in Pakistan: Evaluating the Process and Challenges in Investigating Crimes. The Critical Review of Social Sciences Studies, 3(2), 789–799.

Bachmann, I., Harp, D., & Loke, J. (2025). Digital media and emerging tactics of gendered harassment. In Handbook on Gender and Digital Media (pp. 232–242). Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/book/9781035313570/chapter18.xml

Baker, V. L. (2021). Exploring adolescent violence and abuse towards parents: The experiences and perceptions of young people [PhD Thesis, University of Central Lancashire]. https://clok.uclan.ac.uk/39684/1/39684%20Baker_Victoria_PhDThesis_Final_August2021.pdf

Butt, K. M. A., Shah, M. U., & Hussain, R. (2023). Analysis of Anti-Sexual Harassment Legislation in Pakistan Under International Human Rights Law Obligations. Islamabad Law Review, 7(2), 125–147.

Cheema, A., Chacko, J., & Gul, S. (2019). Mobilising mass anxieties: Fake news and the amplification of socio-political conflict in Pakistan. Fake News, 17. https://asiacentre.org/wp-content/uploads/2020/10/Conference-Proceedings_Fake-News-and-Elections-in-Asia-2019.pdf#page=23

Faisal, S. M., Khan, N. T., & Ahmad, I. (2024). Challenges in Combating Cybercrime: A Comparative Study of Pakistani and International Legal Frameworks. The Journal of Research Review, 1(04), 228–242.

Farooq, A., & Ali, A. (2022). India's growing cyber partnerships and challenges for Pakistan. Margalla Papers, 26(2), 49–61.

Farrand, B. (2024). How do we understand online harms? The impact of conceptual divides on regulatory divergence between the Online Safety Act and Digital Services Act. Journal of Media Law, 16(2), 240–262. https://doi.org/10.1080/17577632.2024.2357463

Fenwick, H., & Coe, P. (2025). The Online Safety Act 2023: Fostering democratic participation while combatting anti-democratic harms? Northern Ireland Legal Quarterly, 76(AD1), 83–135.

Filmeridis, I., Hodel, R., & Oliver, T. (2024). California Threats and Harassment Initiative: A Literature Review Contextualizing the Environment of Threats and Harassment of Local Elected Officials in the United States between 2013 and 2024. https://digital.sandiego.edu/ipj-research/101/

Flesaker, M., Bailar, S., Tan, A. S. L., Austin, S. B., & Gordon, A. R. (2025). Exposure to Online Harassment and Disordered Eating in Transgender and Gender-Diverse Young Adults. International Journal of Eating Disorders, eat.24550. https://doi.org/10.1002/eat.24550

Gillespie, T. (2018). Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

https://books.google.com/books?hl=en&lr=&id=cOJgDwAAQBAJ&oi=fnd&pg=PA1&dq=Gillespie,+2018&ots=PiRGAWOQn9&sig=PQ3IXfcba64CmHQdmgBdO7I8WsQ

Gosztonyi, G., & Lendvai, G. F. (2024). Online platforms and legal responsibility: A contemporary perspective in view of the recent US developments. Masaryk University Journal of Law and Technology, 18(1), 125–141.

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.

Hussain, S., Ashraf, S., Al Hamadi, H., & Abideen, Z. U. (2023). A Critical Analysis on Cybercrimes. 2023 International Conference on Business Analytics for Technology and Security (ICBATS), 1–7. https://ieeexplore.ieee.org/abstract/document/10111414/

Imam, S. K. (2024). Cyber Bullying in Pakistan: The Silent Menace. Islamabad: Center for Governance Research Pakistan. https://cgr.com.pk/wp-content/uploads/2024/07/Cyber-Bullying-in-Pakistan.pdf

Javaid, N. (2025). The Double-Edged Sword: Artificial Intelligence, Electoral Integrity, and the Future of Democracy in Pakistan. ASSAJ, 4(02), 102–113.

Javed, H., Ashraf, J., & Ashraf, S. J. (2025). The Regulation of Cyberbullying and Online Harassment: Analyze the Regulation of Cyberbullying and Online Harassment, Including Issues Related to Freedom of Expression, Anonymity and Accountability. Annual Methodological Archive Research Review, 3(6), 63–82.

Khan, M. A. (2022). Criminal Defamation Laws in Pakistan, and Their Use to Silence Victims of Sexual Harassment, Abuse, or Rape. LUMS LJ, 9, 43.

Lal, D., Giri, U. K., & Tiwari, S. K. (2024). Virtual Vulnerability: Addressing Cyber Harassment against Women in India. https://www.academia.edu/download/119139464/CYS_V2I3P101.pdf

Lu, A., Posetti, J., & Shabbir, N. (2022). Legal and normative frameworks for combatting online violence against women journalists. https://www.icfj.org/sites/default/files/2023-05/UNESCO_GlobalStudy_LegalChapter_v3.pdf

Malik, N., Rafiq-uz-Zaman, M., Bugti, M. A., & Bangulzai, W. A. (2025). Harassment of women in South Punjab politics: Impacts and strategies for enhanced leadership. ACADEMIA International Journal for Social Sciences, 4(3), 2575-2590. https://doi.org/10.63056/ACAD.004.03.0547

Mangi, D. B., Magsi, L. A., & Ali, U. (2025). Need of Judicial Reforms in Pakistan: Ensuring Accountability and Transparency in Courts. Pakistan Social Sciences Review, 9(1), 182–194.

Miller, K., & Rolley, K. (2024). Tools to Implement Victim-Centered Practices in Fraud Investigations and Prosecutions. Dep't of Just. J. Fed. L. & Prac., 72, 185.

Müller, M., & Kettemann, M. C. (2024). European approaches to the regulation of digital technologies. Hannes Werthner· Carlo Ghezzi· Jeff Kramer· Julian Nida-Rümelin· Bashar Nuseibeh· Erich Prem·, 623.

Mythili, K. C., & Nagamani, K. (2025). Safeguarding women in digital spaces: Legal responses to cyber harassment and objectification on social media. Development Policy Review, 43(5), e70039. https://doi.org/10.1111/dpr.70039

Naseri, F., Taghvaei, D., Saleh Sedghpour, B., & Ahmadi, G. A. (2021). A Comparative Study on the Opportunities and Threats of the Internet and Considering the Rights of Kids Online in Australia, Brazil, Iran, and South Africa. Iranian Journal of Comparative Education, 4(4), 1550–1574.

Novovic, M. (2024). The EU Digital Services Act (DSA): A Commentary. Kluwer Law International BV. https://books.google.com/books?hl=en&lr=&id=480gEQAAQBAJ&oi=fnd&pg=PT8&dq=legal+frameworks+in+the+world+to+regulate+online+platforms+is+the+Digital+Services+Act+(DSA)+that+comes+into+effect+in+2024+by+the+European+Union&ots=PNb54dOxlD&sig=EcmiRZhT--aw1G65iFwxx5bCZIA

Prabhkaran, V., & Rameshkumar, M. S. (2025). Fintech's Role In Financial Inclusion In The Indian Landscape. Metallurgical and Materials Engineering, 151–158.

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.

Rafiq-uz-Zaman, M., Khalid, N., & Susanto, E. (2025). Addressing Environmental and Social Challenges: A Mixed-Method Study on the Education and Inclusion of Eunuchs in South Punjab, Pakistan. Social Science Review Archives, 3(1), 284-299. https://doi.org/10.70670/sra.v3i1.311

Reed, E., Wong, A., & Raj, A. (2020). Cyber Sexual Harassment: A Summary of Current Measures and Implications for Future Research. Violence Against Women, 26(12–13), 1727–1740. https://doi.org/10.1177/1077801219880959

Saeed, A., Rehman, T. U., Abid, A., Zawar, A., & Bukhari, S. A. A. (2025). Cyber Legislation and Cyber-Victimization in Pakistan. AL-HAYAT Research Journal (AHRJ), 2(3), 435–441.

Shah, S. K. A. (2024). A Critical Analysis of Efficacy of the Prevention of Electronic Crimes Act, 2016: Irritants and Remedies. Journal of Pakistan Administration, 45(2), 66–91.

Shaheen, M. B., Zahid, M., & Ahmad, Z. U. D. (2024). The intersection of technology and law: Challenges and opportunities in prosecuting cyberstalking cases in Australia and Pakistan. Journal of Politics and International Studies, 10(1), 213–228.

Sherwani, M., & Zia, F. (2023). International Human Rights Law and the Right to Privacy under Pakistan's Prevention of Electronic Crimes Act, 2016. Al-Qanṭara, 9(3), 233–241.

Starr, K. (2025). Where There Are Rights: Starr Legal Theories. KS Enterprises. https://books.google.com/books?hl=en&lr=&id=6B6HEQAAQBAJ&oi=fnd&pg=PT11&dq=Bring+in+Calibrated+Platform-Duty+and+Transparency+Obligations&ots=f_z-WUkh_7&sig=PzOpn82bN2CHwgwFVF0YgbYUzBg

Thakur, S., & Kumar, S. (2019). Sexual harassment in academic spaces: A comparative analysis of legal processes in India and Pakistan. Jindal Global Law Review, 10(2), 173–196. https://doi.org/10.1007/s41020-019-00096-z

Wood, W. R., Suzuki, M., Hayes, H., & Bolitho, J. (2021). Roadblocks and Diverging Paths for Restorative Justice in Australia and Aotearoa/New Zealand. In T. Gavrielides (Ed.), Comparative Restorative Justice (pp. 197–221). Springer International Publishing. https://doi.org/10.1007/978-3-030-74874-6_10

Yongmei, C., & Afzal, J. (2023). Impact of enactment of 'the prevention of electronic crimes act, 2016'as legal support in Pakistan. Academy of Education and Social Sciences Review, 3(2), 203–212.

Zahid, M. A., Muhammad, A., Khakwani, M. A. K., & Maqbool, M. A. (2024). Cybercrime and criminal law in Pakistan: Societal impact, major threats, and legislative responses. Pakistan Journal of Criminal Justice, 4(1), 223–245.