Center for Management Science Research
ISSN: 3006-5291 3006-5283 Volume 3, Issue 8, 2025

CYBERSTALKING AND ONLINE HARASSMENT: A REVIEW OF CRIMINAL LAWS, ENFORCEMENT CHALLENGES, AND LEGAL REFORMS

Fahim Rasool

University Law College, University of The Punjab, Lahore, Pakistan

faheemch312@gmail.com

DOI:https://doi.org/10.5281/zenodo.22811588

Keywords
Cyberstalking; Online Harassment; Cybercrime Law; Digital Evidence; Criminal Justice; Legal Reform; Technology-Facilitated Violence

Article History
Received: 01 October 2025
Accepted: 07 December 2025
Published: 30 December 2025

Copyright @Author
Corresponding Author: *
Fahim Rasool

Abstract
Social media, messaging apps, online communities, and digitally-mediated communication have led to an explosion of opportunities for interpersonal interaction, yet at the same time, they have also allowed for continued instances of interpersonal abuse, such as cyberstalking and online harassment. Online harassment is defined as a wider variety of abusive online behaviours and cyberstalking is defined as repeated or intrusive digital behaviour that includes unwanted communication, online monitoring and surveillance, impersonation, threats, and the sharing of harmful information. While some countries have enacted criminal definitions of stalking, harassment, threats, privacy invasion and technology-facilitated abuse, there are significant challenges in defining offences, ascribing behaviours to offenders, securing the preservation of digital evidence, cross-border offences, and balancing victim protection with freedom of expression. This review considers the evolution of the concept of cyberstalking and online harassment, their primary forms, comparative U.S., U.K., European Union, Australian and Pakistani approaches to criminalizing these offences, and key challenges to enforcement. Special focus is placed on anonymity, jurisdiction, evidence in digital form, platform liability, under-reporting of victims and the new technologies that are fast developing, such as artificial intelligence and deep fake technology. The review contends that new offences are not enough to make an effective response. Criminal laws should be technology neutral and should include specific investigations powers, effective processes for handling digital evidence, international cooperation, victim-focused reporting processes, platform accountability, and protection for legitimate expression. There has been a recent shift to a wider institutional responsibility as reflected in the European Union Digital Services Act, the United Kingdom Online Safety Act, the amended Prevention of Electronic Crimes Act in Pakistan, and various new international laws. Legal changes in the future should therefore follow a rights-based, technology neutral and victim-centred approach, with a coordinated approach.

1. INTRODUCTION

The digital communication has revolutionized interpersonal communication, professional communication, political engagement, education and access to information (Chayko, 2020). Through social networking sites, instant messaging services, email, online gaming, devices that locate users and more, people can

communicate anywhere, all the time (Alrayes et al., 2025). They can also be used to spy, bully, harass, humiliate, or harass another person repeatedly. Cyberstalking and online harassment are thus significant concerns in the fields of criminal justice, cybersecurity, privacy law and human rights scholarship (Mythili and Nagamani, 2025).

Initial studies described cyberstalking as the equivalent of stalking behavior in the online environment. Relationships that were found between cyberstalking and offline stalking were identified by (ÇEVİK, 2025); (Çakıcı, 2024) later showed that cyberstalking can be manifested as persistent unwanted communication, monitoring, threats and other unwanted pursuits. It is worth pointing out that the definition of cyberstalking and that of simply being a nuisance or receiving an offensive message on the internet are different, as not all of the negative or uncomfortable communications online may constitute cyberstalking (Godavarthi et al., 2024).

Addressing cyberstalking can be challenging due to the change in the conventional relationship between the offender, victim, place and time (Henry et al., 2020). Victims may be contacted by an offender multiple times without actually meeting in person, more than one offender may establish an account, offenders may use pseudonyms or indirectly observe public information, or use technological means to track digital activities. The factors that may be related to cyberstalking victimization include online exposure, proximity to the motivated offender, guardianship, target attractiveness, and online behaviour, as suggested by the research that uses the cyberlifestyle-routine activities theory (Abu-Ulbeh et al., 2021).

The level of harassment online and the size of the audience are further reasons why legal action is still important. According to Pew Research Center, 41% of U.S. adults reported some type of online harassment in its 2017 nationally representative survey, and 18% said they experienced more serious harassment, such as stalking, physical threats, sexual harassment or continued harassment. Previous studies by (Vogels, 2021) also showed that university students experience online threatening, insulting and harassing communication and receive it over and over.

But the legality of the problem is complicated by the fact that there is a continuum to online harassment. The type of conduct can include offensive comments and trolling, repeated threats, doxxing, identity impersonation, distribution of intimate images without consent, and digital surveillance, as well as conduct that would cause a reasonable person to fear physical harm. As a result, criminal law needs to differentiate between expression that is protected and serious technology facilitated abuse, and not consider the latter as simply problematic online behaviour. The legal and enforcement aspects of cyberstalking and online harassment are therefore explored, selected jurisdictions compared, and enforcement problems persistently discussed with respect to possible directions for legal reform.

2. Conceptualizing Cyberstalking and Online Harassment

2.1 Cyberstalking

There is no one-size-fits-all legal or academic definition of cyberstalking. Typically, it means stalking behavior that is performed using electronic means. This can involve multiple unwanted messages, checking online behavior, surveillance, impersonation, threats, attempts at contact, publishing of personal information and digitally assisted intrusion. Cyberstalking has been related to unwanted pursuit and relational intrusion by Jain et al. (2021). In a similar vein, cyberstalking is defined as a type of stalking that uses Internet connected technologies (Krieger, 2020), and there are many ways to communicate via the Internet. Cyberstalking is not always clearly distinct from traditional stalking, either, as research indicates. In a study of 1,051 victims who identified as victims of stalking, Reyns and Fissel (2020) found significant involvement with the Internet and that cyberstalking may be similar to, but not necessarily distinct from, traditional stalking.

A large survey of 6,379 social network users conducted by Cheng et al. (2022) showed that prevalence estimates could vary significantly based on the definition. The total percentage of

unwanted Internet contact, duration, and fear resulted in 6.3% meeting the criteria for cyberstalking established in the study. The researchers also found that there were parallels between cyberstalking and offline stalking former intimate relationships were a significant factor.

2.2 Online Harassment

Cyberstalking is a subset of online harassment. May be offensive name-calling, threats, sexual harassment, continuous harassment/humiliation, doxxing, impersonation, unwanted sexual content or other abusive communications. Slaughter and Newman (2022) adopted six categories to define online harassment: offensive name-calling, deliberate embarrassment, physical threats, stalking, prolonged harassment, and sexual harassment. The general nature of the concept raises problems to the criminal law, as an act that is considered offensive by one may not meet a threshold of criminal law. Legal scholarship has thus focused on the need to draw a line between harmful behaviour and constitutionally and/or legally protected expression. For instance, de Perio Wittman (2021) stated that existing laws may lose their clarity and applicability when it comes to social networking settings.

3. Forms and Technological Characteristics of Cyberstalking and Online Harassment

Cyberstalking and online harassment can occur through multiple technological environments. The increasing integration of social media, location services, artificial intelligence, encrypted communication, and cloud-based services has expanded the available methods.

Table 1. Major forms of cyberstalking and online harassment

Form of conduct	Typical digital mechanism	Potential harm	Relevant legal concern
Repeated unwanted contact	Email, WhatsApp, SMS, social media	Fear, distress, intrusion	Stalking/harassment
Online surveillance	Social media monitoring, spyware, GPS	Loss of privacy, safety concerns	Cyberstalking, privacy offences
Threats	Messages, posts, emails	Fear of physical or psychological harm	Criminal threats
Doxxing	Publication of address, phone number, workplace	Safety and privacy risks	Privacy, harassment, stalking
Impersonation	Fake profiles/accounts	Reputational and social harm	Identity-related offences, fraud
Non-consensual intimate imagery	Social media, websites, messaging	Humiliation, reputational harm	Sexual-image abuse/privacy offences
Coordinated harassment	Multiple accounts/users	Psychological and reputational harm	Harassment, conspiracy or related offences
AI-generated abuse	Deepfakes, synthetic images/accounts	Reputational, sexual and psychological harm	Emerging cybercrime/communications offences
Cyberbullying	Social networks, gaming, messaging	Emotional and social harm	Criminal/civil/educational remedies
Digital coercive control	Account monitoring, location tracking	Loss of autonomy and safety	Domestic violence/stalking laws

The technological characteristics of these offences create several enforcement problems. An offender may use temporary accounts, VPNs, spoofed identifiers, disposable telephone numbers, or

third-party platforms. Moreover, evidence may be distributed across different providers and jurisdictions. The Australian eSafety Commissioner defines cyberstalking as the use of digital technology to track and harass someone and identifies repeated unwanted contact, abusive content, monitoring through location technology, and surveillance as examples.

4. Criminal-Law Approaches to Cyberstalking and Online Harassment

4.1 United States

The United States uses a combination of federal and state laws to address cyberstalking and online harassment. The federal statute against criminalized specified stalking behavior involving interstate or foreign commerce is 18 U.S.C. § 2261A and also encompasses conduct that would result in the killing, injuring, harassing, intimidating, or surveillance of others. The statute covers cases in which a person has a reasonable fear of death or serious bodily harm, and has suffered significant emotional distress.

The statute is being applied to digital campaigns that last and federal prosecutions illustrate that. For instance, in 2025, the U.S. Department of Justice pleaded guilty to cyberstalking, a case of extended electronic harassment and intimidation. In 2026, the federal government also filed a cyberstalking case involving fake social media profiles and AI-created nude images, as an example of the interaction between new technology and current cyberstalking legislation.

But U.S. cyberstalking law has raised constitutional issues as well. (Weinstein, 2020) explored the interplay between the federal cyberstalking statute and First Amendment values, noting the inherent tension between First Amendment freedoms and the need to protect people from cyber harassment.

4.2 United Kingdom

Historically stalking and harassment have been dealt with in the United Kingdom via the Protection from Harassment Act 1997, followed by specific provisions for stalking and the Stalking Protection Act 2019.

These include repeated contact, publication of material about a person, monitoring Internet or email use, and watching or spying. The Stalking Protection Act also provides for police to request civil protection for stalking orders without the need for a conviction.

Radebe (2021) noted challenges in the application of the Protection from Harassment Act when it comes to social-media offenders and called for criminal justice measures to be adapted to technology mediated offending.

The Online Safety Act 2023 extended and built on the UK's communications framework. It included the criminalisation of threatening communications and the abolition of some of the previous communications offences in England and Wales and Northern Ireland (McGlynn et al., 2024).

The UK approach is therefore a more multi-faceted approach, moving from primarily a general harassment legislation to a mix of stalking offences, protective orders, communications offences, and platform regulation

4.3 European Union

The European Union has taken a dual stance on tackling online harms by leveraging national criminal offences and supranational digital regulations. The Digital Services Act (Regulation [EU] 2022/2065) is not an EU cyberstalking law. Instead, it sets out duties on the part of intermediaries and online platforms to illegal content, transparency, notice-and-action, complaint mechanisms and platform accountability (Law, 2024). This model is important because it acknowledges that the fight against online harm cannot be solely based on action after the harm has been done: that is, criminal prosecution. Platforms have roles to play with illegal content and procedural mechanisms.

4.4 Australia

There are a number of Federal criminal provisions dealing with online abuse in Australia. Telecommunications networks offences are found in the Criminal Code Act 1995 such as making threats using a carriage service and to menace, harass or cause offence using a carriage service

(Keen et al., 2020). It also has rules about sexual material being passed on without consent. Australia also offers an important institutional model through its eSafety framework, which incorporates functions of regulation, education, reporting and victim support.

4.5 Pakistan

Pakistan is an important case study as the Prevention of Electronic Crimes Act (PECA) 2016 has given attention to cyber stalking (Iqbal et al., 2023). Historically, repeated unwanted contact, monitoring of electronic communications, watching or spying such that the person feels fear or serious alarm/distress, and some instances of the unauthorized release of photographs and/or videos were all part of Section 24 (Kaplun, 2023). Later, the government of Pakistan took a step to incorporate more institutional and regulatory bodies related to social media platforms through the Prevention of Electronic Crimes (Amendment) Act 2025 (Shaharyar et al.). According to the official Gazette, the Act was passed as Act No. II of 2025, assented to January 29, 2025. The revised framework creates a Social Media Protection and Regulatory Authority which has powers relating to online safety, unlawful or offensive content, powers over regulation of platforms and compliance with the rules (Batchelor, 2025). The shift in the legal landscape of Pakistan from an offence-centric approach to cybercrime to a more comprehensive approach with the inclusion of social-media platforms is reflected in the country's legal development (Ahmed et al., 2023).

5. Comparative Legal Analysis

Table 2. Comparative approaches to cyberstalking and online harassment

Jurisdiction	Principal legal mechanisms	Strengths	Major challenges
United States	18 U.S.C. § 2261A + state stalking/harassment laws	Specific federal cyberstalking offence; established prosecution mechanisms	First Amendment issues; interstate jurisdiction; attribution
United Kingdom	Protection from Harassment Act 1997; Stalking Protection Act 2019; Online Safety Act 2023	Criminal offences + protective orders + platform regulation	Application across rapidly changing technologies; enforcement consistency
European Union	National criminal laws + Digital Services Act	Platform accountability, notice mechanisms, transparency	Fragmentation among national criminal laws
Australia	Criminal Code Act 1995 + eSafety regulatory framework	Telecommunications-specific offences and regulatory support	Jurisdictional and technological complexity
Pakistan	PECA 2016, amended 2025 + institutional mechanisms	Express cyberstalking provision and expanding regulatory framework	Enforcement capacity, digital evidence, institutional coordination
International	Budapest Convention and cooperation mechanisms	Cross-border cooperation and procedural framework	Uneven participation and differences in national law

The comparison demonstrates that jurisdictions generally follow one of three approaches: criminalization, platform regulation, or a hybrid model. Criminal law establishes prohibited conduct and sanctions, while platform regulation focuses on prevention, reporting, content management, transparency, and user protection. The Council of Europe's Budapest Convention

remains a major international framework for cybercrime cooperation and electronic evidence. Its significance lies not in creating a universal cyberstalking offence but in facilitating international cooperation concerning cybercrime and electronic evidence.

6. Major Enforcement Challenges

6.1 Anonymity and Identity Attribution

One of the major issues with cyberstalking investigations is the anonymity of the perpetrator. Offenders can create fake social network profiles, temporary email addresses, pseudonymous accounts, use VPNs, spoofing or hacking into existing accounts. It does not imply that it is not possible to identify an online offender. Instead, there must be technical evidence that ties an online account or communication with a person. Aggarwal et al. (2005) noted the evidentiary challenges related to anonymity, data collection, verification and admissibility in cyberstalking cases.

6.2 Digital Evidence

Digital evidence is prone to change. Messages can be deleted, accounts can be removed, metadata can be modified, and platforms may only keep information for short periods of time. Preservation, acquisition, authentication and presentation of digital evidence, therefore, need to be carried out using specific procedures by investigators (Karagiannis and Vergidis, 2021).

The challenge here isn't just to get a screen shot. The courts will have to establish authenticity, provenance, integrity, authorship and relevance. There is a need, therefore, for a strong legal structure with clear protocols regarding preservation requests, provider cooperation, forensic acquisition, chain of custody and expert testimony (Heath et al., 2023).

6.3 Cross-Border Jurisdiction

Cyberstalking tends to go across borders. The victim can reside in Pakistan, the perpetrator in another nation and evidence kept by the platform in a third jurisdiction. Traditional territorial criminal jurisdiction is problematic in those times. This means that cooperation arrangements with other countries, mutual assistance, preservation requests and accelerated procedures for the exchange of electronic evidence are crucial. One of the most significant international cybercrime and electronic evidence cooperation frameworks is the Budapest Convention (Gull et al., 2025; Shaheen et al., 2024).

6.4 Limited Law-Enforcement Expertise

Conventional investigative skills must be utilized along with technical skills in cyberstalking cases. Police officers should be familiar with account attribution, digital preservation, platform records and metadata, social-media architecture and electronic communications. Studies that focus on the law enforcement problems highlight the following as significant problems: lack of awareness and skills; jurisdictional issues; and inability to get data on Internet accounts.

6.5 Victim Underreporting

Victims may not report cyberstalking/bullying due to fear of escalation, belief that they did something wrong, fear of loss of reputation, distrust of authorities, or if they do not believe that their situation is a crime. In an investigation of the factors that affect decisions to report stalking victims to the police, (Taylor-Dunn et al., 2021) found that offence seriousness and the relationship between the victim and the offender were important factors. A key problem of this is that many digital-abuse experiences exist between social norms and criminal-law thresholds (Cho et al., 2023).

6.6 Platform Cooperation

They have information that could be crucial to investigations, such as account registration information, IP logs, device information, content logs, and communication metadata. It is worth noting that there may be varying legal requirements, periods, privacy responsibilities, and international processes required to implement platform cooperation (Manzoor et al., 2025).

The EU's Digital Services Act is a blueprint for a regulatory framework aimed at providing clear tools for reporting illegal material and increasing platform responsibility.

6.7 Freedom of Expression

One of the key challenges of the law is the difference between criminal harassment and legitimate expression. Broad definitions can lead to the inclusion of political criticism, satire, journalism, public interest speech or even unpopular opinions (Godioli et al., 2025). This tension is represented in the U.S. constitutional debate. Byers (2020) explored the need for cyberstalking regulation to be within the limits of the First Amendment, and Citron (2024) addressed constitutional challenges to the federal cyberstalking statute. Accordingly, legal changes should take into account sufficiently clear thresholds, based on behavior, intent, repetition, credible threats, significant distress, invasion of privacy or other factors that are objectively determined.

7. Gender and Vulnerability Dimensions

Different groups of people are not equally impacted by cyberstalking and cyber harassment. Specific people, such as women, journalists, public figures, sexual minorities, young people or those who are victims of intimate-partner abuse, can be subject to specific forms of digital abuse. According to the Pew Research Centre's 2014 survey, young women were more likely to be the targets of online stalking and sexual harassment than men. In 2017, women also experienced higher emotional distress due to online harassment compared to men. Technology can also be used as a tool of coercive control in relationships. In "Technology-facilitated coercive control," (Cuomo and Dolci, 2021) the technology-facilitated nature of coercive control was explored, as were the tensions between digital platforms and domestic abuse. In recent years, the international context has tended to view online abuse as a continuum of online to offline abuse. UN Women has highlighted a number of forms of technology-facilitated violence against women and girls, including cyberstalking, online harassment, doxing, impersonation, image-based abuse, and associated behaviours.

8. Artificial Intelligence and Emerging Forms of Online Abuse

Artificial intelligence (AI) is generating fresh opportunities for cyberstalking and online harassment, including the creation of synthetic intimate images, the generation of deep fake pornography, fake identities, automated harassment, impersonation, manipulated audio and automated messaging, targeted disinformation, and coordinated abuse (Shirish and Komal, 2023). As shown through recent U.S. federal prosecution, existing cyberstalking laws can be applied to stalking via an AI-generated nude image and fake social-media accounts. This raise concerns over the possibility of enacting technology specific offences, or keeping the offences under the umbrella of harmful conduct (Senarathna, 2025). Legislation that is technology neutral may continue to apply to changes in technology, and provisions that could aggravate may be relevant when there is a meaningful increase in the extent of deception, scale, invasiveness, or harm that is caused by AI. UN Women has also highlighted the importance of holistic laws to include the various types of technology-facilitated violence, as opposed to piecemeal laws (Maras and Logie, 2024).

9. Legal Reform Strategies

The coordinated nature of legal and institutional reform is necessary for effective responses to cyberstalking and online harassment. Legislation should use technology neutral definitions of repeated unwanted communication, digital surveillance, location tracking, impersonation, publication of personal information, threats, coordinated harassment and conduct that causes serious fear or distress. To distinguish between criminal harassment and legitimate expression, clear criminal thresholds can be adopted based on factors like repetition, intent, credible threats, substantial emotional distress, privacy invasion, etc. (Jain et al., 2021). Authorities need to establish more advanced cybercrime teams that have access to digital forensics, electronic evidence, social media investigation and multi-jurisdictional cooperation skills. Legal frameworks should also allow for the quick preservation of

digital evidence and provide judicial and privacy protections. Furthermore, Internet platforms should have reporting mechanisms and complaint processes that are readily available to use, as well as co-operative procedures with lawful investigations. Reporting options should be easy to access for the victim, providing guidance on how to preserve evidence, legal assistance, privacy, and support for victim services should be made available to victims (Iqbal et al., 2023; Krieger, 2020; Law, 2024).

9.1 Technology-Neutral Definitions

Cyberstalking laws must be directed at harmful behaviour, not at certain technologies or platforms as they are constantly changing. The modern definition should encompass "repeated unwanted communications", "electronic surveillance", "monitoring of online activity", "location tracking", "impersonation", "publication of personal information", threats, "coordinated harassment" and other "conduct involving technology" which creates serious "fear" or "distress" or "intrusion" on the person's "privacy". This could ensure the continuity of legislation in the event that the offenders use a new platform, app or technology (de Perio Wittman, 2021; Gull et al., 2025).

9.2 Clear Criminal Thresholds

Criminal law ought to provide clear guidelines and definitions for distinguishing between legally protected and offensive communications and unlawful harassment. Factors might include repeated behaviour, recklessness or intent to cause harm, knowledge that the communication is unwanted, threats that are believed to be serious, significant emotional distress, fear of physical harm, serious invasion of the privacy of another person, or substantial personal or reputational harm. Clear thresholds can enhance the consistency of investigators and courts, and minimise the risk of potential under-criminalisation and the over-criminalisation of certain provisions (Godavarthi et al., 2024; Maras and Logie, 2024; Reyns and Fissel, 2020).

9.3 Specialized Cybercrime Units

Police departments need to establish dedicated Internet-forensics, social-network investigation, electronic evidence analysis, open-source intelligence, and/or platform collaboration teams to investigate cases of cyberstalking and online harassment. The units should also include provisions for victim protection and cooperation between states where the offences often occur in multiple jurisdictions involving offender, victim, platform, and evidence in various jurisdictions. Digital evidence can be more effectively identified, preserved and interpreted with specialized expertise (McGlynn et al., 2024; Reyns and Fissel, 2020).

9.4 Faster Evidence Preservation

There is a need for legal frameworks to put in place measures to quickly preserve relevant electronic evidence as electronic evidence can be deleted, altered, and may become inaccessible. Within proper legal procedures, investigators should have the ability to ask that the account information, communications and other relevant records be preserved. These mechanisms should provide for judicial control, and privacy protection to guarantee that the efficiency of investigations will not compromise individual rights (Shaharyar et al.).

9.5 Improved Platform Accountability

Online platforms play an important role in responding to cyberstalking and online harassment, as they are the owners of a number of systems that create and propagate abusive content. Platforms should offer reporting tools that are accessible, clear complaint processes, evidence preservation and processes for users to challenge moderation decisions (Radebe, 2021). The European Union's Digital Services Act is one example of a combination of notice-and-action mechanisms, transparency requirements, and platform accountability (Slaughter and Newman, 2022).

9.6 Victim-Centred Reporting

Victim-centred reporting systems must not require detailed knowledge of complex cybercrime laws

when reporting online harassment and cyberstalking (Weinstein, 2020). Good systems should include straightforward reporting processes, advice on how to preserve evidence, risk assessment, referral to law enforcement, legal support, privacy protection, and suitable support services. The research literature also underscores the benefits of approaches that take a more targeted and constructive approach to victims than simply criminal prosecution, like Nova Scotia's CyberScan unit (Keen et al., 2020).

10. Pakistan: Specific Reform Considerations

The Prevention of Electronic Crimes Act (PECA) 2014 has provisions against cyber stalking and the amendment in 2025 has added to the institutional and regulatory framework in relation to social media platforms and content. The recent National Strategy to Counter Technology-Facilitated Gender Based Violence also identifies cyberstalking, online harassment, image-based abuse, impersonation and coordinated intimidation as issues (Godavarthi et al., 2024). Cybercrime investigation and digital-forensics capacity should be enhanced; procedures should be standardized for the collection and preservation of electronic evidence; the coordination of investigations with prosecutors should be made more effective; mechanisms to support victims of cybercrime should be put in place; international cooperation should be increased and public awareness of available legal remedies should be raised. Online-safety measures must also include suitable protection for due process, privacy, and legitimate expression (Chayko, 2020).

11. Proposed Integrated Legal-Response Framework

Successful cyberstalking and online harassment prevention and response will require an integrated legal and institutional approach that links prevention, detection, reporting, evidence preservation, investigation, prosecution, victim protection, judicial remedies and platform accountability. It should not only be a criminal punishment system but include preventive measures, quick reporting, effective digital-evidence collection, a specialist investigation, assistance for victims, judicial supervision and platform cooperation. This multi-faceted approach can offer a more harmonized reaction to technology-facilitated abuse while simultaneously retaining the proper legal and procedural safeguards.



Figure 1: Integrated framework for responding to cyberstalking and online harassment

12. Discussion

The literature shows that cyberstalking and online harassment need not be considered as completely distinct from other types of interpersonal abuse. Rather, the dynamics by which harassment takes place, its scope, duration, documentation and impact are altered by digital technology. However, our research (Byers, 2020; ÇEVİK, 2025; de Perio Wittman, 2021) suggests that there is a significant overlap between online and offline stalking. The main legal question is not necessarily to establish a new class of crime, but to ensure that the principles of criminal responsibility apply to the digital world. Meanwhile, the online harassment goes beyond stalking. Messages sent via offensive communications, doxing, impersonation, abuse involving images, coordinated harassment and the use of AI created content may be sent without meeting traditional stalking requirements. Current legal frameworks need a multi-layered approach. Comparative evidence indicates that none of the jurisdictions has fully overcome these problems. The United States offers an example of the significance of specific government laws regarding cyberstalking and serves as an example of constitutional issues (Law, 2024). The United Kingdom is a melding of harassment and stalking offences, protective orders and newer communications regulation. The European Union is focusing on intermediary and platform accountability with the Digital Services Act. Australia has adopted a holistic approach to the issue of on-line safety, including the implementation of criminal laws, and a specific regulatory framework for the internet. Pakistan has formulated specific clauses on cyberstalking in PECA and recently enhanced its institutional and regulatory framework (Manzoor et al., 2025).

It is suggested that effective regulation does not only depend on punishment-based approaches. A

comprehensive system is needed that will tie together criminal law, civil protection, digital evidence, platform governance, victim assistance, and international cooperation. Another key concern is technological neutrality. Legislation inscribed for a particular social media platform can easily get outdated (Maras and Logie, 2024). It would be more appropriate to define the underlying prohibited conduct in the context of technology-neutral terms. Laws should also include aggravating factors when the technology causes a significant increase in harm, including through coordinated attacks, the creation of sexual imagery via AI, location tracking, or disclosure of sensitive information about the person (Citron, 2024). Lastly, there must be a balance between safety and fundamental rights in legal reform. Widely interpreted harassment laws can lead to confusion and even lead to the criminalization of legitimate expression. But too specific legislation can be unhelpful if it fails to provide meaningful relief from significant digital abuse. Statutory limits, judicial review, evidentiary requirements, and procedural protections are thus crucial..

13. Future Research Directions

Comparative empirical research should explore the way the cyberstalking law is implemented, not just its language. Second, prosecutors' rates, case results, evidence failures and victims' experiences should be examined in each jurisdiction. Thirdly, AI-powered harassment is a very specific type of harassment. Fake or manipulated media and Deepfakes make it hard to distinguish the truth and can worsen the amount and severity of harassment. Fourth, there is a need for further studies with regard to platform cooperation and the interaction between private moderation systems and criminal investigations. Finally, there is a need for further empirical studies in countries like Pakistan on the implementation of PECA, effectiveness of cybercrime investigations, reporting rates by victims, and the cybercrime relationship between law enforcement and prosecutors, as well as courts and digital platforms.

14. Conclusion

Cyberstalking and online harassment pose major issues for today's criminal justice system as the use of digital tools has increased the ability to communicate, monitor, harass, impersonate, threaten, and abuse others in an ongoing manner. Previous studies show that cyberstalking is more closely correlated with traditional stalking and that there are instances of cyber harassment which are not adequately covered by traditional criminal-law classifications. Comparative analysis shows that jurisdictions are increasingly integrating a range of protective order, platform regulation, digital-evidence and victim support measures with criminal offences. Different aspects of this evolving legal landscape are demonstrated in the United States, the United Kingdom, the European Union, Australia, and Pakistan. The central problem is not just a lack of criminal laws, however. Enforcement capacity, evidence preservation, jurisdiction, platform cooperation, victim reporting, technological change, and protection of legitimate expression are all important. Further reform should be technology neutral, clear criminal thresholds should be in place, specialist investigative powers should be enhanced, closer cooperation between jurisdictions should be promoted, digital-evidence preservation should be simplified, and victim-centred remedies should be made available. The reform agenda is especially relevant in the context of new technologies like Artificial Intelligence. A full answer must take into account online harm and the offline impacts of protection, as well as the need for cooperation between legislators, law-enforcement, courts, technology companies, civil society organizations and victims to achieve effective protection. The goal of future cybercrime policy should, therefore, be a workable policy that balances the rights of individual citizens from harm and protects their privacy, due process and freedom of legitimate expression.

REFERENCES:

Abu-Ulbeh, W., M. Altalhi, L. Abualigah, A.A. Almazroi, P. Sumari, and A.H. Gandomi. 2021. Cyberstalking victimization model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations. *Electronics*. 10:1670.

Ahmed, Z.S., I. Yilmaz, S. Akbarzadeh, and G. Bashirov. 2023. Digital authoritarianism and activism for digital rights in Pakistan. *European Center for Populism Studies (ECPS)*.

Alrayes, F.S., A.I. Abdelmoty, and W. El-Geresy. 2025. User profile visualisation for privacy awareness on Geo-Social Networks. *Journal of Location Based Services*. 19:43-77.

Batchelor, I. 2025. Data privacy management behaviour of social media users in South Africa. Cape Peninsula University of Technology.

Byers, L. 2020. Stalking or Talking? An Analysis of State v. Shackelford, Stalking, and the First Amendment. *First Amend. L. Rev.* 19:99.

Çakıcı, Z. 2024. Cyberstalking practices among youth in Türkiye: Motivational drivers, digital avenues, and perceptual paradigms. *Türkiye İletişim Araştırmaları Dergisi*:1-22.

ÇEVİK, Ş.N. 2025. A Meta-analysis of Studies on Cyberstalking.

Chayko, M. 2020. Superconnected: The internet, digital media, and techno-social life. SAGE Publications, Incorporated.

Cheng, C., O.V. Ebrahimi, and J.W. Luk. 2022. Heterogeneity of prevalence of social media addiction across multiple classification schemes: Latent profile analysis. *Journal of Medical Internet Research*. 24:e27000.

Cho, S., C. Kim, and J.G. Owens. 2023. Understanding of factors associated with reporting to the police, helping seeking, and adopting in self-protection among stalking victims: A latent class analysis. *Psychosocial Intervention*. 32:141.

Citron, D.K. 2024. From Bad to Worse: Stalking, Threats, and Chilling Effects. *The Supreme Court Review*. 2023:175-212.

Cuomo, D., and N. Dolci. 2021. New tools, old abuse: Technology-enabled coercive control (TECC). *Geoforum*. 126:224-232.

de Perio Wittman, J. 2021. A Trend You Can't Ignore: Social Media as Government Records and Its Impact on the Interpretation of the Law. *Alb. LJ Sci. & Tech.* 31:53.

Godavarthi, S.K., S.V. Ganimisetty, S. Palanati, R.R. Chintala, and V.P. Chennamsetty. 2024. Confronting the offensive stalking risks: With standing cyber stalkers. *In* 2024 international conference on advances in computing, communication and applied informatics (ACCAI). IEEE. 1-7.

Godioli, A., S. Jacques, J. Young, and A. Matamoros-Fernández. 2025. What's in a joke? Assessing humor in free speech jurisprudence.

Gull, S., M.B. Shaheen, and N. Akhtar. 2025. A Comparative Study of Pakistani and International Laws on Online Harassment: Challenges and Opportunities. *ACADEMIA International Journal for Social Sciences*.

Heath, H., Á. MacDermott, and A. Akinbi. 2023. Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? *Forensic Science International: Digital Investigation*. 46:301585.

Henry, N., A. Flynn, and A. Powell. 2020. Technology-facilitated domestic and sexual violence: A review. *Violence against women*. 26:1828-1854.

Iqbal, M., S.R. Talpur, A. Manzoor, M.M. Abid, N.A. Shaikh, and S. Abbasi. 2023. The prevention of electronic crimes act (PECA) 2016: understanding the challenges in Pakistan. *Siazga Research Journal*. 2:273–282-273–282.

Jain, A.K., S.R. Sahoo, and J. Kaubiyal. 2021. Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*. 7:2157-2177.

Kaplun, K. 2023. Tracking and trailing each other: tracing stalking and harassment laws through time and technology. Rutgers University-Graduate School-Newark.

Karagiannis, C., and K. Vergidis. 2021. Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. *Information*. 12:181.

Keen, C., R. Kramer, and A. France. 2020. The pornographic state: The changing nature of state regulation in addressing illegal and harmful online content. *Media, Culture & Society*. 42:1175-1192.

Krieger, M.A. 2020. Image-based sexual violence: Victim experiences and bystander responses. University of Windsor (Canada).

Law, S. 2024. Effective enforcement of the Online Safety Act and Digital Services Act: unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation. *Journal of Media Law*. 16:263-300.

Manzoor, I., R. Ghani, and K. Hamid. 2025. Challenges of data extraction from Facebook & WhatsApp applications. *Journal of Computing & Biomedical Informatics*.

Maras, M.-H., and K. Logie. 2024. Countering the complex, multifaceted nature of nude and sexually explicit deepfakes: an Augean task? *Crime Science*. 13:31.

McGlynn, C., L. Woods, and A. Antoniou. 2024. Pornography, the Online Safety Act 2023 and the need for further reform. *Journal of Media Law*. 16:211-239.

Mythili, K., and K. Nagamani. 2025. Safeguarding women in digital spaces: Legal responses to cyber harassment and objectification on social media. *Development Policy Review*. 43:e70039.

Radebe, F. 2021. Towards a mobile application to aid law enforcement in diagnosing and preventing mobile bully-victim behaviour in Eastern Free State High Schools of South Africa.

Reyns, B.W., and E.R. Fissel. 2020. Cyberstalking. *In* The Palgrave handbook of international cybercrime and cyberdeviance. Springer. 1283-1306.

Senarathna, J.I. 2025. AI Ethics in Social Media.

Shaharyar, S., M. Umar, and S. Rauf. THE JOURNAL OF RESEARCH REVIEW.

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

Shirish, A., and S. Komal. 2023. A socio-legal inquiry on deepfakes. *Cal. W. Int'l LJ*. 54:517.

Slaughter, A., and E. Newman. 2022. New frontiers: Moving beyond cyberbullying to define online harassment. *Journal of Online Trust and Safety*. 1.

Taylor-Dunn, H., E. Bowen, and E.A. Gilchrist. 2021. Reporting harassment and stalking to the police: A qualitative study of victims' experiences. *Journal of interpersonal violence*. 36:NP5965-NP5992.

Vogels, E.A. 2021. The state of online harassment. Pew Research Center Washington, DC.

Weinstein, J. 2020. The Federal Cyberstalking Statute, Content Discrimination and the First Amendment. *UC Davis L. Rev.* 54:2553.