Page 5419 - 5429 **DOI:** *https://doij.org/10.10000/IJLMH.119623*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Online Harrasment and Cyberstalking

TULU SINGH[1] AND DR ARUN D RAJ[2]

ABSTRACT

The fast pace of development in digital technology has changed how we connect, communicate and engage in bad behaviour (e.g. cyberstalking, online harassment) worldwide. While online abuse depends on the accessibility and anonymity of the internet, it is also behaviour that can pose impacts on victims that can have dire implications for them (e.g. emotional damage, harm to reputation, and harmful effects on the victim's security).

There are many forms of online harassment - doxxing, trolling, impersonation, threats, blackmail, and bullying - that are all targeted to elicit fear or control someone. Cyberstalking is a specific type of harassment that can involve obsessive monitoring and sending numerous messages, or spreading false information to cause harm. Cyberstalking, unlike online harassment, is often carried out repetitively or in a systematic manner, which raises it to the level of a serious concern.

The psychological and social consequences of cyberstalking are extensive and serious. Victims of cyberstalking experience a gamut of feelings including anxiety, stress, fear, loss of their privacy, and if applicable, loss of professional status. In terms of legal reform, many countries have laws protecting against cybercrimes, including cybercrime laws, privacy laws, and defamation laws. In India, cyberstalking is punishable under the Information Technology Act, 2000 and the Indian Penal Code (IPC), allowing the victims of cyberstalking to have some means of protection.

Individuals have the power to mitigate their own behaviour online to limit personal risk and improve their online security, limit what they share, report and block everyone who harasses them, and secure evidence for potential prosecution. Victims of cybercrime can seek justice through governments official cybercrime reporting portals and law enforcement officers, as well as attorneys. Individuals can also contribute to creating a safer digital environment through education and awareness raising activities.

As online threats evolve and become more complex, the implications will be ongoing and new laws, tech responses, and community initiatives will be ongoing. Governments, technology and online communities need to work together to address online security, improve filtering content, and raise the public's understanding of responsible digital behaviour. If we have solid and reliable legal protections in place, technology evolves and develops, and the community has a working knowledge of issues through public initiatives

[1] Author is a student at Vellore institute of Technology Chennai, India.
[2] Author is a Professor at Vellore Institute of Technology Chennai, India.

 [ISSN 2581-5369]

social acts, then the public can address issues of online harassment and cyber stalking at the same time, and the community can enjoy safer digital spaces.

Keyword: *Online harassment, cyber stalking, security, protection, online threats*

I. INTRODUCTION

In the modern digital world, the internet has become an integral part of the everyday human experience, and has changed the way individuals communicate, share information, and interact altogether. However, along with those changes, more negative uses of the internet—for example, online harassment and cyberstalking—have been created. Online harassment and cyberstalking are forms of digital abuse that involve abusive and threatening behaviours through the use of the internet and other electronic communication tools. Online harassment is behaviour that involve sending threats and intimidations, sending abusive messages, disseminating false information about someone, impersonating an individual, and/or doxxing. Cyberstalking is a more serious and more constant form of online harassment, which involves persistent threats and/or observing a person's activities in an attempt to control or intimidate that same individual. Both domestic abuse and harassment can have significant psychological and emotional implications, which may lead to anxiety, depression, fear and social withdrawal. Victims tend to suffer in silence or quietly, as digital anonymity and ease of access complicate identification or culpability of the abuser, or at the very least the anonymity may prevent the perpetrator from re-entering the victim's life. Victims often sustain reputational harm or privacy breaches, especially if some personal information has been shared, or their personal photographs or videos—it is completely understandable for many victims that they don't want the world to know the extent of the abuse they have endured, and don't want to be "outed" for their interest in social media or their profession. As awareness is generated, laws still vary considerably between jurisdictions, and many cannot keep pace with the relentless speed and development of technology. That being said, the internet can also be an effective defence: social media platforms have created report features, or have not had them in place, and can subsequently increase privacy protection. Increasingly, victims also have access to an array of cyber security tools to "re-take" their space. As online behaviour continues to expand, especially with respect to various devices and platforms, responding to and/or preventing online harassment and stalking have taken on crucial significance to help ensure the internet is safe and egalitarian for all users.

 [ISSN 2581-5369]

II. TYPES OF ONLINE HARASSMENT

There are many different forms of online harassment, each with its own tactics, goals, and impact. These types often overlap and adapt with technology, making them harder to identify and address. Being aware of these types of online harassment is important in recognizing abuse, providing support to victims, and working to create safer online environments.

Cyberbullying is one of the most common and recognizable forms of online harassment. This form of harassment involves the repeated targeting of an individual by a perpetrator's hostile behaviour, usually using insults, rumour spreading, or threats. Cyberbullying is usually not just limited to children's and youth's harassment; adults can also be cyberbullied. Cyberbullying can take place via text messages, social media posts, an email, or through online gaming communities. While online bullying is a wide variety of different tactics and emotions involved, they always have a level of anonymity and distance that gives bullies more courage than they would ever have face-to-face.

Another common form of online harassment is trolling. Trolls are people who, as a main goal, want to intentionally post inflammatory, off-topic, or provocative messages in an online community. Their aim is to evoke a reaction from other users and intentionally disrupt the normal flow of conversation in a forum. Some trolls are just annoying and mean, while others deliberately harass, or manipulate, or discredit their targets. Trolls can act for amusement purposefully disruptive can potentially lead to targeted harm and harassment, especially when trolls work as a group to collectively disrupt or bully someone.

Doxxing is an extreme and harmful harassment tactic that a person may experience when their privately identifiable information (home address, phone number, email, workplace) is publicly published without consent. The ultimate goal of this violation is to harass, retaliate against, or threaten the person being doxxed. The victim may experience real-world consequences, including threats, stalking, physical harm, and loss of employment. Doxxing is particularly dangerous as it may threaten the online or offline safety of the victim.

Revenge porn, or more accurately, non-consensual sharing of images, is a significant violation form of harassment that mostly harms women and other marginalized communities. These images or images are commonly shared by an ex-partner, or an online person intending to control, embarrass, or retaliate against the victim. Victims are subjected to intense emotional torment, loss of reputation, and often, forced to find a lawyer, in order to remove the images.

Impersonation is another type of online harassment that refers to someone creating a fake identity or account to impersonate the victim. This usually intends to transmit misinformation,

 [ISSN 2581-5369]

solicit others, or otherwise injure the person's reputation. In a professional context, impersonation may have financial repercussions or lead to work consequences for the victim. Impersonation is usually used with other types of harassment, such as phishing or blackmail.

In serious cases, online harassment can turn into cyberstalking, which involves persistent acts and wilful conduct. Cyberstalking can involve monitoring the victim's online behaviour, sending threatening messages, and tracking the physical location of the victim using GPS and surveillance technology. Cyberstalking creates high distress to the target and allows for a continuous sense of fear and helplessness. It can sometimes lead to police interaction and protective orders.

In addition to impersonation and cyberstalking, harassment can be in the form of hate speech/discrimination, when the target of the harassment is deliberately targeted on the basis of their race, gender, sexual orientation, religion or disability. Hate speech/discrimination usually found in section or virtual bulletin boards, and general social space contributes to harmful, negative environment to marginalized communities online where they become less visible.

Overall, these types of online harassment highlight the nuance and severity of the issue. As technology continues to advance, so do the harassers' methods, making it even more important for individuals, platforms and policy-makers to be mindful of online harassment in all of its forms. Recognizing the multitude of online harassment is the first step to prevention and accountability in the digital age.

III. UNDERSTANDING CYBERSTALKING

Cyberstalking is one of the most serious and invasive forms of online abuse. Cyberstalking refers to the repeated use of digital technologies to monitor, control, stalk, intimidate, or threaten someone. Unlike long-term or random online abuse, cyberstalking tends to be obsessive and consistent. A cyberstalker behaves in ways that partly resemble conventional (if terrifying) stalking behaviours, but these behaviours occur in an online and digital context. Some possible examples of cyberstalking include sending harassing messages or emails, following the target's online actions, hacking social media accounts, tracking a victim's location using GPS-enabled apps, and impersonating the person being targeted online. Cyberstalks often embrace the anonymity and accessibility of online platforms to abuse someone while avoiding detection or consequence.

What distinguishes cyberstalking from other crimes is the persistent feeling of being watched. Many victims feel as though they are constantly being monitored, which often results in high levels of anxiety, insomnia, depression and fear of going in public or using the internet. Since

 [ISSN 2581-5369]

the crime of cyberstalking can pervade many different aspects of a victim's life—both public (like reputation) and private (such as personal relationships)—it can ultimately lead to mental health issues. In many instances, the stalker will either make threats of physical violence, or the stalker will graduate from online stalking to an in-person confrontation, increasing the overall danger to the victim and the urgency of immediate action.

Cyberstalking perpetrators can include former intimate partners, acquaintances or even complete strangers. In the case of an intimate relationship, cyberstalking tends to occur after a break-up as one-party refuses to accept the relationship has ended and uses technology as a means to retain control over the other party. In other situations, it may be triggered by jealousy, fixation, vengeance or even ideological, especially where the victims are public figures or activists. There are cyberstalkers that work solo, but there are also cyberstalkers that attempt to engage a group in acts of harassment, as in the cases of online abuse where the group is coordinating attacks or when a group is launching attacks based on cancel culture.

The resources and techniques used in cyberstalking are numerous and will continue to change. Cyberstalkers might collect information through social media, create fake profiles to harass the victim or contact, install spyware on devices, or use technical methods to fool privacy settings and security protocols. The proliferation of information available for public consumption online – be it voluntary or data breach – has simplified the lives of stalkers by creating an affordable way to locate targets, identify potential victims, and manipulate or threatened them.

While it can be very impactful, the scope of cyberstalking is not consistently viewed or dealt with legally in many regions. Legal definitions and protections differ greatly and, in some situations, there may also be jurisdictional obstacles that prevent victims from obtaining help due to a lack of digital evidence. Support is expanding along this continuum and many nation-states have started to amend their cybercrime laws to recognize cyberstalking as a substantive offence. Victims should keep a copy of all interactions, secure other digital devices, use good privacy settings, and contact advice or organizations who can help if they feel they are threatened.

Understanding cyberstalking is important for the purposes of prevention, as well as for the purposes of detection and intervention. This type of stalking can be serious, with major consequences for victims, and cyberstalking is becoming increasingly common in today's technological world. Being able to identify and recognize the signs of cyberstalking, along with knowing how to respond, can be important to help protect yourself or others from an undesirable and lingering outcome. Raising awareness, providing strong laws, and holding offenders

 [ISSN 2581-5369]

accountable are crucial steps to ensure safe and healthy spaces in our digital world.

IV. PSYCHOLOGICAL AND SOCIAL EFFECTS

The psychological and social consequences of online harassment and cyberstalking for victims can be severe and long-lasting. Online harassment transcends physical distance and time, unlike traditional, in-person harassment. Digital abuse might occur at 3 a.m. to the detriment of one's most intimate spaces. These intrusive elements of digital harassment can lead to continuous anxiety, stress, and fear that stem from continual threats, unwanted attention, or offensive material at all times and in almost all places with few ways to disengage. Consequently, victims may develop a feeling of being "watched" or attacked, hyper-vigilance regarding their physical surroundings, alterations in sleep patterns, and worsened mental health. Online harassment victims may experience economic loss, family issues, relationship problems, mental health instability, long-term changes in their levels of and comfort with technology, and even the potential outcomes from collapsing social capital.

Victims who experience online harassment and/or cyberstalking have also dealt with the loss of privacy and personal security; many victims may suddenly discover that their private images, private conversations, and personal information are now available on various online platforms often without consent of any kind. Victims of harassment and/or stalking may develop a general anxiety regarding technology and subsequent technology use, including platforms they previously considered safe; when victims encounter or use these previously safe situations, people or platforms, they will likely experience fear, stress, and anxiety. For example, the required responses of simply checking and responding to a message, scrolling through social media, or engaging in a video conference can be exhausting and sometimes traumatic for victims.

One of the most disconcerting aftermaths is the loss of privacy and safety physically and personally. Victims will see their private photographs or chat messages or private particulars shared very publicly without consideration or consent. The privacy violations are so severe that places once felt safe become dreadful and isolated spaces. The privacy violations can turn connections to friends, family, and colleagues into feelings of emotional exhaustion, or trauma. Scenarios that were once the norm of an online existence (e.g., checking messages; scrolling social media; joining video calls) can be viewed as daunting and further undermine victims whose feelings of stress are triggered or distorted. Victims will withdrawal myself totally from online worlds to social isolation and while inexperience feelings of disconnect and late disassociates themselves from important, personal and -professional networks.

 [ISSN 2581-5369]

Moreover, many victims will find problems of reputation and professional injury, especially when private and harsh descriptions of themselves are presented online with their intimate media, defamatory online secure by public event in live settings. Such access to new information on the person potentially means influencing a public perception, hence harming personal relationships and future career opportunities. In a world as connected, where practically every individual presence is often, if not exclusively digitally represented: where the damage of reputation can impact employability

Often overlooked are the psychological effects of online harassment and cyberbullying. The emotional pain suffered by victims can be very serious, specifically; anxiety, feelings of low-self-esteem, and even panic attacks or a sense of worthlessness. Victims may now become suspicious of people that they would interact with online, also impacting the way they manage their interpersonal relationships. Victims experience other emotions such as feelings of hopelessness, shame, and frustration - primarily in relation to not being able to find assistance, through legal and/or institutional means, or feeling that whatever assistance offered is inadequate or inaccessible.

Eventually, the social and psychological consequences of suffering through this type of online abuse extend beyond the parameters of the screen; they can affect the victims' life in entirety - they leave behind invisible scars. It is critical to understand and acknowledge the implications of loss in order to be able to provide some suitable assistance, produce the robust and well-informed policy responses, and manifest digital empathy to individuals and organizations.

V. REGULATORY FRAMEWORK AND PROTECTIONS:

As the problem of cyberstalking and online harassment grows, the world is seeing an increase in regulatory frameworks; many legal systems are recognizing, grappling with, and acknowledging the significance of online crimes. Governments and courts have taken unprecedented steps in developing legal protections of individuals experiencing forms of online abuse to acknowledge the responsibility of the offenders. Accordingly, while the likely methods of assuring survivors' protections from perpetrator conduct will differ from nation to nation, the goal remains the same: to deter and regulate acting out and hostile conduct in cyberspace, while ensuring victims the options to seek for justice.

In India, laws against cyberstalking and online harassment are drawn from two significant statutory frameworks: The Information Technology Act, 2000, and the Indian Penal Code. The Information Technology Act is meant to regulate e-commerce, but now regulates new forms of cybercrime and online abuse. For example, Section 66E relates to the invasion of privacy, and

Section 67 prohibits selling obscene electronic material, which is *published or transmitted for profit. In general, the sections protect cases when there is misuse of digital space, notably in contexts of non-consensually distributing private images or information.

While there are some additional protections under the IPC, the provisions in the IPC are minimal. For example, IPC Section 354D defines of cyberstalking as a person who "follows another person, by the means of electronic communication" after a victim signal's they do not wish to have further electronic communications. If it is established that a person was guilty of cyberstalking, depending on those factual circumstances, the consequences may include imprisonment and/or fines. Other IPC sections, as relevant to harm online, may include IPC Section 499 (defamation), Section 503 (criminal intimidation), and Section 507 (intimidation via anonymity) for the many online danger and harassment methods victims may be faced with.

Once again, while all of these laws theoretically apply, there will still be issues with enforcement. The victims might not even know they have 'rights'; they might be afraid and/or ashamed to disclose it even to the police, and/or might just be uncertain of what might happen because they have never had an experience with the legal system before. The anonymity of the internet allows for offenders to act from relative safety in most circumstances, and in many instances, there may be problems identifying who the person is as a result of the offending; this can cause issues even further with fake accounts and/or now offenders residing in foreign jurisdictions. Thus, creating legal remedies will require supportive mechanisms such as good cyber-policing, trained investigation units and the promotion of public awareness campaigns to increase the public's knowledge of their statutory rights and protections.

There are also countries around the world including the United States, the United Kingdom, Australia, and many European nations that have passed laws specific to online abuse, digital stalking and internet-related gender-based violence and in many cases developed cybercrime units, protocols for digital evidence, and services for victim support that work in conjunction with law enforcement.

To conclude, the legal landscape related to online harassment and cyberstalking is evolving to respond to the nature of digital threats. India, along with other countries, has made meaningful legislative steps however; there's still more work to be done using a comprehensive approach to combat cybercrime including legislative reform, technological advancement, public education, transferrable laws across borders, etc. It is essential to empower victims and strengthen the accountability of actors, so collective and individual digital environments are safe for use.

 [ISSN 2581-5369]

VI. PREVENTION AND ONLINE SAFETY

Taking proactive measures to ensure online safety is critical in the digitally-connected world to protect yourself against harassment or cybers stalking. Although legal tools and platform policies are important, an individual must also think of strategies to limit their risk and maintain control of their online presence. Arguably, the most important preventative mechanism is to increase digital security. You should have different, strong passwords for each of your accounts and include two-factor authentication (2FA) where possible. Additionally, you should regularly update your software and privacy settings to avoid being accessed by other users.

Limiting the amount of personal information, you share online is another important preventative measure. Statistically, we think harmless details like location and birthday, workplace, daily routines, etc., but these can easily be organized and misused by stalkers or malicious individuals to find you or impersonate you. Using privacy settings on social media to limit who can view content, not oversharing details of your life, and only allowing certain people to access content will help decrease your risk.

If harassment does happen, be sure to block and report the harasser as soon as possible using the built-in tools provided by most social media and communication platforms. These tools are set up to stop any further ability to contact you and to report the conduct for moderation attention. Just deleting harmful messages is not sufficient; it is highly recommended that victims gather and keep evidence of the abuse. In the case of social media, that can be screenshots; in the case of email or chat that will be saving or retaining emails, chats logs, and documentation including date and time. This would be especially noteworthy evidence if there is a decision to pursue any legal claims over the harassment, or if it escalates.

If things are serious, or chronic, it is recommended to get professional help. This may include legal advice from a lawyer to understand your rights, law enforcement for potential protection, or professional cybersecurity assistance for your online safety. It also is certainly reasonable to think about mental health therapy for support after the harassment. Harassment can have some serious emotional impacts.

VII. THE ROLE OF SOCIAL AND TECHNOLOGICAL SYSTEMS

While legal approaches and personal preventative strategies play an important role in the response to online harassment and cyberstalking, ultimately it is the responsibility of society and the providers of technology. Digital platforms (social media platforms, messaging platforms, and search engines) have a social responsibility and ability to minimize abuse simply

by better cybersecurity infrastructure, stricter enforcement of their community standards, and a quicker response to user reports. Automated moderation of abusive content, artificial intelligence nuisance detection, and more robust privacy settings to limit the exposure to online harassment, are only a few of the resources o technology systems could implement to lessen the exposure to negative online behaviours. However, using better technology is only part of the solution; you also need a joined social effort to address online actions and misinformation and shifting negative online cultures. Responses must include a focus on user education and the digital literacy; ethics, empathy, and monitoring behaviour hinged on on-line consequences (personal and societal) to cyber abuse. Local communities, schools, employers, media, and organizations need to contribute to sharing ideas and building awareness that have a positive impact on digital behaviours.

In addition, public discourse has to shift from shaming victims, to supporting victims so that when victims feel they can speak out against abuse, they are met with public support instead of silence and isolation. When tech companies, legislators, educators and users unite to prioritize safety, respect, and humanity the internet can continue to move away from a space for endangerment and to a collaborative space for empowerment. The ultimate enemy is the collective as a whole not only technology or legislation and each effort marks what it means to express and embody a public understanding of empathy and resiliency.\

VIII. Conclusion

Online abuse and cyberstalking present serious problems to individuals, communities and the world. As our digitized world continues to be ubiquitous in our everyday lives, the opportunities for abuse and malice to occur through technology are becoming more common. Understanding how online harassment looks, the social and psychological impacts of online harassment, as well as knowing how to access the existing legal structures for protection can assist victims with taking self-protective steps.

Through deterrent actions— such as improving digital surveillance options, limiting their personal information, and know how to report harassment, victims can counteract the powerlessness they feel when their digital lives are intruded upon. However, counteracting online abuse and harassment cannot rely solely on the efforts of victims. Technology companies must take the initiative and the responsibility to ensure that they enforce policies in a way that protects victims from abuse on their platform. Society must also come together to implement a collective culture of respect and compassion on social networks so that abusive behaviour is swiftly labelled as unacceptable. The legal framework and the law must continue to develop

 [ISSN 2581-5369]

and change to confront new technologies, hold online abusers accountable, provide victims with support and compassion, and access to the courts.

In the end, the responsibility to create a safer internet not only belongs to the people who are victims of cyberstalking, but to anyone who goes online. By collectively being vigilant, advocating for positive online behaviours, and refusing to tolerate abuse, we can build a safer, more respectful and inclusive online space.

*****

 [ISSN 2581-5369]