LEGAL FRAMEWORKS ADDRESSING CYBERSTALKING AND ONLINE HARASSMENT

Anushka Mathur, Manipal University, Jaipur

ABSTRACT

In the present era of information technology, cybercrimes have become a grave concern as novel modes of abuse and exploitation are facilitated by technological advances at an exponential rate. Among these, cyber harassment and online stalking have become the foremost threats to individuals' safety, privacy, and well-being, especially against women and children. Ongoing surveillance, threatening, and using the internet to inflict psychological trauma come under these categories of cybercrime. With the proliferation of smartphones, social media, and internet-enabled communication, perpetrators find new and evolving methods to intimidate, harass, or manipulate victims in both public and private digital spaces.

This document addresses the legal, social, and psychological effects of cyberstalking and online harassment. It emphasizes the increasing prevalence of these crimes and the need for immediate action and more protective legislation. The deficiencies of current legislative frameworks, enforcement issues, and the need for increased knowledge and responsibility are all covered in the research. The study concludes with practical policy recommendations for legislative, technical, and pedagogical reforms that would improve online safety and encourage responsible online conduct.

INTRODUCTION

"***Once, reputation was hard-earned and carefully guarded. Today,***

Your reputation can be created or destroyed in just a few clicks."[1]

Words can hurt and injure any person's reputation, whether spoken by a stranger or someone they know. In this modernized world with heavy dependency on technology, people have advanced to hurting people's reputations through words on online platforms in the form of cyberbullying and online harassment. Although the internet has opened a lot of windows of opportunity for people, making communication easier and more convenient, it has also revealed its dark side as people have started to find loopholes to misuse these online means of communication to demean each other.

Bullying is more of "a psychosocial problem of intentionally and repeatedly harming others and creating an imbalance of power between the victim and the perpetrator, with negative consequences for both parties" [2] (M et al., 2024) Cyberbullying refers to the act of intimidating, defaming, or harassing any person online, usually with the help of technological devices such as mobile phones, computers through social media, group chats, or any other digital platforms. The purpose behind cyberbullying is to demean or insult the victim, which leaves an enduring traumatic effect on the victim.

This article delves into the different forms of crimes that people use digital media for, with special emphasis on Legal frameworks for cyberstalking and online harassment.

Cyberstalking, cyber harassment, and online harassment are relatively new crimes that are not yet recognized by state laws. Consequently, victims are often left in fear and without any adequate protection. In light of the growing number of Internet crimes, there is a desperate need to protect these victims and amend laws recognising these crimes as well.

Stalking is recognised under the Bharatiya Nyaya Sanhita, 2023, defined under Section 78, which criminalizes stalking, which includes repeatedly following, contacting, or monitoring a

[1] Michael Fertik & David Thompson, Wild West 2.0: How to Protect and Restore Your Online Reputation on the Untamed Social Frontier 2 (2010)
[2] M, V., Balamurugan, G., Sevak, S., Gurung, K., G, B., X, S., P, T., & S, T. (2024). Silent Screams: A narrative review of cyberbullying among Indian adolescents. Cureus

woman online despite her disinterest. Exceptions apply if the act is for crime prevention, fulfilling legal obligations, or for reasonable justification. The punishment is up to 3 years of imprisonment and a fine for the first offense, and up to 5 years and a fine for repeat offenders. This provision aims to curb harassment and protect women's safety.[3]

Online harassment involves sexual harassment, which is unwanted contact of a personal nature, or other conduct based on sex affecting the dignity of men and women at work. Sexual Harassment is also defined under section 75 of the Bharatiya Nyaya Sanhita, 2023. "Online harassment can be divided into two categories, namely "Direct Harassment," which includes "harassment through the use of pagers, cell phones, and email to send hate messages, obscenities, and threats to intimidate a victim."[4] "Second, being "Indirect Harassment" which includes the use of the internet to display hate messages, threats, or to spread false rumours about a victim."[5]

The first, Cyberstalking, on the other hand, is defined as the act of harassing another individual via electronic communication, leading to considerable emotional distress without any valid reason. It generally involves repeated communication through emails, blogs, group chats, online social networks, or other websites. Cyberstalking is considered to be one of the most dangerous cybercrimes.

Harassment is a form of discrimination when someone experiences unwanted, offensive, or humiliating comments or behaviour.[6] It refers to deliberate aggressive behavior directed at someone, regardless of whether the harasser has been harmed. Historically, harassment was defined as actions intended to intimidate or distress another person based on their gender, race, religion, or other characteristics. While this definition still applies, modern technology has created new ways for harassers to target individuals, often allowing them to hide their true identities.

Further, Cyberharassment, the National Conference of State Legislatures defines cyberharassment as "threatening or harassing email messages, instant messages, blog entries,

[3] Bharatiya Nyaya Sanhita, 2023, Universal Publications
[4] https://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf
[5] Id
[6] Human Rights Commission

or websites dedicated solely to tormenting an individual."[7] Cyberharassment involves the use of information and communication technology to deliberately humiliate, annoy, attack, threaten, alarm, offend, and/or verbally abuse individuals. Even a single act can constitute cyberharassment, although it can involve more than one incident. Further, Cyberharassment involves spreading false information or rumors about an individual to undermine their social standing, relationships, and reputation. This behavior can have significant personal and professional consequences. Though Cyberstalking and cyberharassment possess similar ingredients, they differ in the repetition of the incident. In the case of cyberstalking, it is a series of behaviours and actions over a period of time, whereas only one incident is needed for cyberharassment.

Moreover, Online Impersonation is the act of creating a fake social media profile, website, or email account with the intention of threatening or harming someone without their consent. In today's world, there are so many ways in which one person can impersonate another, and with the gradual advancement in technology and the invention of Artificial Intelligence, scammers have pretended to be victims through social media, reaching out to the victims' friends and family, fabricating stories about how the victim is in danger and urgently needs money.

As the exposure to technology increases and more and more people find new and innovative ways to scam people, the rate of cybercrimes is just going to rise. Consequently, there is a need for more stringent cyberlaws, and the state needs to acknowledge and identify the newly invented methods that scammers are developing in this fast-paced, techno-dependent world.

IMPLICATIONS OF CYBERSTALKING AND ONLINE HARASSMENT:

Online cyberstalking and harassment are ubiquitous behaviors with wide-ranging implications for victims and society at large. These behaviors can cause extreme emotional distress, mental illness, and a sense of fear in victims. Several studies with credibility identify the multi-faceted effects of these online offenses, depicting how they can ruin personal lives, harm reputations, and even cause long-term psychological trauma. Additionally, the social impacts are significant, as these harassment forms have the potential to destroy trust in online communities and provide a platform where individuals feel insecure about communicating. Identifying the

[7] State Cyberstalking and Cyberharassment Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-law s.aspx (last updated Dec. 5, 2013)

multifaceted effects of online harassment is imperative for developing effective prevention and intervention strategies.

1. Impact on Psychology and Emotion

Victims of cyber harassment and cyberstalking often suffer from significant mental health issues. Research published in Cyberpsychology, Behavior, and Social Networking indicates that these individuals may experience anxiety, feelings of hopelessness, panic attacks, and even suicidal thoughts. Repeated instances of cyber abuse can lead to chronic stress and a pervasive sense of helplessness.

2. The decline of privacy and personal safety:

The erosion of privacy and personal safety has become a pressing societal issue in today's digital age. Unauthorized monitoring, identity theft, and doxing—the act of publicly disclosing an individual's private information without their consent—are prevalent forms of cyberstalking. These intrusive behaviors not only invade a person's privacy but can also lead to profound psychological distress, undermining their sense of security and well-being.

Victims of cyberstalking often experience a debilitating fear as malicious actors exploit their personal information. This can manifest in various forms, including harassment or threats, both online and in the physical world. The alarming reality is that individuals can feel unsafe in their own homes or communities as the boundaries between online harassment and real-world threats become increasingly blurred. As technology continues to evolve, it is essential to address these issues to safeguard personal safety and preserve the integrity of privacy in our increasingly interconnected society.

3. Disruption of Routine Activities and Social Withdrawal

Cyberstalking has a profound and often devastating impact on victims, disrupting their social relationships and daily activities in both the digital and physical realms. A thematic analysis published on PubMed reveals that those affected by cyberstalking frequently feel compelled to modify their daily routines, often limiting their participation in social events and activities they once enjoyed. This heightened sense of vulnerability leads many victims to become hyper-aware of their surroundings, constantly on edge, and living in fear of potential harassment or further stalking incidents. Over time, this can result in significant social withdrawal, as victims

may isolate themselves to avoid confrontation or escalation, ultimately affecting their mental health and overall well-being.

4. Undermining Academic and Professional Pursuits

Cyber harassment is a grave danger for academic and professional work since it often leads to harsh consequences for individuals in these professions. A paper published on arXiv shows that concentrated online cyberbullying of researchers and academicians has the potential to drastically reduce their productivity. Apart from the immediate impacts on their work, such attacks are capable of harming their professional image, keeping them from securing funding, collaborating with other professionals, or publishing their work.

In the worst cases, such persistence of this harassment has the consequence of leading people to modify the direction of their career by retreating from specific projects, changing institutions, or even leaving academia. Psychological consequences of online abuse include anxiety, depression, and loss of confidence, which have the consequence of leading to a dramatic drop in levels of participation in academic and professional tasks. So, the repercussions of cyberbullying go much deeper than the victim, with potential suppression of innovation and progress within the whole field of study.

5. Institutional and Legal Challenges

Combating internet abuse and cyberstalking also presents significant legal challenges. Internet incidents often cross national and regional borders, making it challenging to determine which authority should prosecute cases. The anonymity of the criminals also makes it easy for them to use pseudonyms, and so identifying and prosecuting them is an uphill task.

The rapid pace of technological development also hinders legal responses, as new communication platforms tend to surpass existing legislation intended to protect victims. The majority of victims of internet abuse are not content with support from law enforcement and legal groups, which typically lack the necessary understanding of crimes on the internet. Such inadequate assistance erodes victims' confidence in the justice system, leading them to feel isolated and disheartened about seeking help.

6. Implications for Society and the Need for Policy Reform

Online harassment and cyberstalking are serious social problems affecting millions of

individuals each year. In order to counteract these widespread problems, wide-ranging legislative reform is required. This includes not only the passing of new laws specifically dealing with online harassment and protecting victims, but also the modification of existing regulations to fit the evolving digital landscape.

To effectively avert these issues, it is essential to advocate for digital literacy of all ages. This entails enrolling in education courses to teach individuals how to navigate cyberspaces securely, be capable of detecting the red flags of cyberstalking, and understand their rights. Moreover, strengthening legislation and regulations ensures there are definite policies and penalties for offenders and that they can be held accountable for what they do.

Instilling a sense of responsibility online is equally important. This may be achieved by engagement by the active role of governments, tech industries, and civic society actors to all cooperate towards the crafting of integrated measures designed to prevent ugly behavior as well as support its victims. In promoting a culture where responsible, safe online experiences are the norm, society may achieve tremendous improvements in securing humans online.

In a nutshell, the impact of cyberstalking and online harassment is far-reaching and not only for the immediate victims but also with a corrupting effect on digital spaces and the overall health of society. To address the issues effectively, an integrated approach with technological protections, policy changes, and cultural shifts towards online empathy and accountability is required.

KEY DIFFERENCES BETWEEN CYBERSTALKING AND HARASSMENT

Cyberstalking can be characterized by persistent and obsessive behaviour, where the perpetrator continuously monitors, follows, or contacts the victim online despite a clear interest. This repeated behaviour is generally fuelled by an intention to control, manipulate, or develop fear in the mind of the victim, making it a more severe and dangerous form of online abuse. Cyberstalkers often use advanced technical devices like GPS tracking, spyware, and social engineering tactics to keep tabs on the victims, slowly instilling a sense of vulnerability and distress.

Although both cyberstalking and cyberharassment involve harmful online behavior, they differ in terms of frequency and intent. Cyberharassment is more common and tends to be less

consistent. It encompasses actions such as defamation, public shaming, trolling, and sending inappropriate messages. Perpetrators of cyberharassment usually do not have a long-term obsession with their victims. However, cyberstalking is more calculated and driven by obsessive feelings or a desire for revenge. Although cyberharassment can cause emotional distress, it typically does not lead to the persistent psychological harm often associated with cyberstalking. Cyberharassment may stem from petty rage, ideological disagreements, or a desire to provoke a response from the victim.

From a legal perspective, cyberstalking is considered a serious criminal offense due to its threatening nature. It is regulated under strict anti-stalking laws and often involves overt threats of harm, coercion, or identity fraud. In contrast, cyber harassment may not always qualify for criminal prosecution unless it includes severe threats of violence, slander, or intimidation. Some forms of cyberbullying may not be illegal but could be categorized as civil offenses, such as cases of internet defamation or workplace harassment.

The psychological impact of cyberstalking is more profound and enduring than that of cyberharassment. Victims frequently experience heightened anxiety, paranoia, and emotional trauma from the constant sense of being monitored. While cyberharassment also does leave an impact, it is often viewed as less invasive unless it escalates into repeated victimization.

Therefore, in both crimes, the victims may confront mental health issues, social withdrawal, and a diminished sense of personal security. It is, therefore, crucial to enhance laws and support systems for individuals affected by these issues.

RECENT TREND OF CYBERSTALKING AND CYBERHARASSMENT[8]

The nature of cyberstalking and harassment has evolved significantly in recent years due to technological advancements, particularly the emergence of deepfake technology, data breaches, and misuse of artificial intelligence. One concerning development is the weaponization of artificial intelligence, where criminals employ voice cloning, chatbots, and deepfake manipulation to harass, impersonate, or blackmail their victims. There has been a notable increase in cases involving AI-generated sexual content, where deepfake software is used to create fake nude photos of individuals. This trend has significantly exacerbated the harm caused

[8] https://www.cybercrimejournal.com/pdf/mpittarojccjuly2007.pdf

by online harassment.

The rising use of digital tracking tools and spyware is a concerning trend in cyberstalking. Stalkers increasingly employ hacked cameras, social media analytics, and location-tracking applications to monitor their victims in real time. This situation has blurred the lines between online and offline harassment, resulting in a rise in cases where individuals are stalked both digitally and physically. Investigating these crimes poses significant challenges for law enforcement, as many offenders utilize encrypted communication platforms, VPNs, and anonymous accounts.

Coordinated cyber harassment campaigns have emerged as a serious issue, especially affecting public figures, journalists, and activists. Organized groups on social media and dark web forums employ tactics such as smear campaigns, mass reporting, and doxxing—revealing private information—to intimidate or silence these individuals. Due to the involvement of multiple perpetrators in this type of cyberbullying, victims often struggle to hold any one of them accountable.

To combat online abuse, social media companies have sought to enforce stricter moderation guidelines; however, significant challenges remain. Offenders frequently evade bans by creating new accounts, employing coded language, or transitioning to private networks. Although there has been progress in legal frameworks, cross-border cybercrimes continue to pose substantial difficulties. The fact that stalkers and harassers operate across multiple legal jurisdictions complicates the prosecution process.

Governments, IT corporations, and law enforcement agencies need to take proactive measures as cyberstalking and harassment evolve. Increasing digital literacy, utilizing AI-driven threat detection, and strengthening legal frameworks are some of the ways to address these issues. Victims should also have access to legal remedies, mental health care, and education on digital safety to empower them in combating this growing digital threat.

COMPARING ONLINE AND OFFLINE ABUSE

Harassment can manifest in both physical and digital environments, and while they may initially appear similar, the internet significantly magnifies the impact and intricacies of such abusive behaviours. Traditional harassment often occurs within defined locations or social contexts,

such as workplaces, schools, or public spaces, where the victim may have a sense of control or safety. In contrast, cyber harassment operates beyond geographical limitations, allowing offenders to target individuals anytime and anywhere, which greatly increases its prevalence. The permanence of online harassment is another critical factor; once harmful content is shared on the internet, it can be difficult to remove, creating a lasting digital footprint that continues to affect victims long after the initial incident. Additionally, the anonymity that the internet provides can embolden perpetrators, leading to more aggressive and harmful behaviours that further intensify the psychological distress experienced by victims. The combined effects of these factors—widespread reach, permanence, and heightened aggression—make cyber harassment a particularly complex and distressing issue in contemporary society.

In an era defined by digital connectivity, online interactions have become an integral part of daily life. However, this increased reliance on the internet has also given rise to cyberharassment and cyberstalking, which are distinct from traditional forms of physical abuse. Although they share some similarities, online harassment poses unique challenges that conventional legal frameworks, primarily designed for real-world offenses, often struggle to address. The global reach, anonymity, permanence, and psychological effects of cyber abuse require specialized legal measures to protect victims effectively.

The magnitude and reach of harm are some of the most notable contrasts between physical and online harassment. While traditional harassment is confined to certain sites and people, cyberharassment knows no geographical boundaries. Once published online, harmful content can be accessed by an infinite audience, shared many times, and remain available forever. Removal from one platform does not guarantee erasure; it is often cached or mirrored on other sites, so erasing it becomes almost impossible. This permanence aggravates the victim's suffering since they cannot recover control over their reputation or privacy.

Online offenders enjoy another basic difference: anonymity is granted to them. Unlike physical-world harassers, who are usually identifiable, cyber-abusers can readily hide their identities using fake profiles, encrypted communications, and offshore digital platforms. Perpetrators are encouraged by this anonymity to participate in more aggressive and continuous abuse with minimal concern for consequences. Legal proceedings are also made more difficult by this, as problems with jurisdiction and tracking digital footprints often impede law enforcement actions.

Furthermore, online abuse can be indirect yet very harmful. Though they might not always make explicit threats, offenders can use online material to provoke others to attack the target. This sets off a cycle of abuse in which third parties unwittingly take part in the victim's harassment. Cyber abusers, for example, might publish false personal information that causes unwanted contact, threats, or even physical harm. Unlike conventional harassment, where damage is often done face-to-face, cyber-abuse allows broad, untraceable victimisation with long-lasting consequences.

LEGAL FRAMEWORKS RELATING TO CYBERSTALKING AND ONLINE HARASSMENT IN INDIA AND THEIR CHALLENGES

India has witnessed a surge in concerns regarding cyberstalking and online harassment, coinciding with the increasing use of the internet and the expansion of digital platforms. Although technological advancements have enhanced communication and connectivity, they have also created new opportunities for abuse, particularly against women and minors. In response to these challenges, India has developed a legal framework that integrates provisions from various laws to tackle cybercrimes, including stalking, bullying, and online abuse.

The Legal Frameworks in India concerning Cyberstalking and Online Harassment are defined under the Bharatiya Nyaya Sanhita,2023, and the Information Technology Act, 2000.

I. Section 74 of Bharatiya Nyaya Sanhita, 2023[Section 354 of Indian Penal Code]-

Assault or use of criminal force on a woman with the intent to outrage her modesty:

Whoever assaults or uses criminal force to any woman, intending to outrage or knowing it to be likely that he will thereby outrage her modesty, shall be punished with imprisonment of either description for a term which shall not be less than one year but which may extend to five years and shall also be liable to a fine.[9]

II. Section 75 of Bharatiya Nyaya Sanhita, 2023[Section 354A of Indian Penal Code]-

Sexual Harassment:

The section on sexual harassment in the Bharatiya Nyaya Sanhita, 2023, clearly defines specific

[9] Bharatiya Nyaya Sanhita,2023, § Section 74, No.45, Acts of Parliament,2023(India)

acts that constitute an offense when committed by a man against a woman. These acts include unwelcome physical contact, sexually suggestive advances, demands or requests for sexual favours, coercion of a woman to watch pornography against her will, and making sexually inappropriate remarks. The law takes these offenses seriously and prescribes penalties: rigorous imprisonment of up to three years, a fine, or both for the first three categories, and imprisonment of up to one year, a fine, or both for making sexually inappropriate remarks.

This provision is especially relevant in cases of cyberstalking and harassment, as these crimes are becoming increasingly common on the Internet. They include sending unwanted sexual messages, posting inappropriate sexual comments on social media platforms, distributing explicit material without consent, and repeatedly requesting sexual favors through texts or emails. Addressing these behaviors in the law acknowledges that harassment has moved into the virtual space, protecting women not only in public places but also in online environments. This is especially important since the anonymity and accessibility of the Internet often encourage such criminal behavior.[10]

III. Section 77 of Bharatiya Nyaya Sanhita 2023 [Section 354C of Indian Penal Code]

Voyeurism:

Voyeurism is defined as the act of taking a picture of a woman engaged in a private act and/or sharing such a picture without her permission. For this behavior to qualify as voyeurism, the situation must be one in which the woman would typically expect not to be observed, either by the perpetrator or by any other person acting on the perpetrator's behalf. A person found guilty of voyeurism can face a fine and a maximum sentence of three years in prison for their first conviction, with a possible sentence of seven years for subsequent convictions**.**[11]

IV. Section 78 of the Bharatiya Nyaya Sanhita,2023[Section 354D of the Indian Penal Code]

Stalking:

This section addresses stalking, including cyberstalking, which has been implemented. Stalking is defined as the act of a man pursuing or communicating with a woman despite her clear

[10] Bharatiya Nyaya Sanhita, 2023, § Section 75, No.45, Acts of Parliament, 2023(India)
[11] Bharatiya Nyaya Sanhita, 2023, § Section 77, No.45, Acts of Parliament, 2023(India)

indifference or monitoring her online activities and electronic communications. A man found guilty of stalking may face imprisonment for up to three years for a first offense, along with a fine. For each subsequent conviction, the penalty may increase to imprisonment for up to five years and a larger fine.[12]

V. Section 351 of Bharatiya Nyaya Sanhita, 2023[Section 503 of Indian Penal Code, 1860]-

Criminal Intimidation:

(1) "Whoever threatens another by any means, with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

(2) Whoever commits the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with a fine, or with both.

(3) Whoever commits the offence of criminal intimidation by threatening to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or imprisonment for life, or with imprisonment for a term which may extend to seven years, or to impute unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

(4) Whoever commits the offence of criminal intimidation by an anonymous communication, or having taken precaution to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment of either description for a term which may extend to two years, in addition to the punishment provided for the offence under sub-section (1).[13]

VI. Section 66C of the Information Technology Act, 2000-

Punishment for identity theft:

[12] Bharatiya Nyaya Sanhita, 2023, § Section 78, No.45, Acts of Parliament, 2023 (India)
[13] Bharatiya Nyaya Sanhita, 2023, § Section 351, No.45, Acts of Parliament, 2023 (India)

"Whoever fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term that may extend to three years and shall also be liable to a fine that may extend to rupees one lakh."[14]

VII. Section 66E of the Information Technology Act, 2000-

Punishment for violation of privacy:

"Whoever intentionally or knowingly captures, publishes, or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment, which may extend to three years or with a fine not exceeding two lakh rupees, or with both.

Explanation. – For the purposes of this section–

(a) ―transmit - means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) ―capture, with respect to an image, means to videotape, photograph, film, or record by any means; (c) ―private area‖ means the naked or undergarment-clad genitals, public area, buttocks, or female breast:

(d) ―publishes means reproduction in the printed or electronic form and making it available for the public;

(e) ―under circumstances violating privacy means circumstances in which a person can have a reasonable expectation that–

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place."[15]

[14] Information Technology Act, 2000 § Section 66C, No. 21, Acts of the Parliament, 2000 (India)
[15] Information Technology Act, 2000 § Section 66E, No. 21, Acts of the Parliament, 2000 (India)

VIII. Section 67 of the Information Technology Act, 2000-

Punishment for publishing or transmitting obscene material in electronic form:

Section 67 of the Information Technology Act, 2000, addresses the publication or transmission of obscene material in electronic form. This provision states that anyone who publishes, transmits, or facilitates the publication or transmission of any material that is lascivious, sexually explicit, or appeals to prurient interests— and is likely to corrupt or deprave the minds of readers, viewers, or listeners of such material—is subject to punishment under the law. For a first conviction, the offender may face imprisonment for up to three years and a fine not exceeding five lakh rupees. In the case of a subsequent conviction, the penalties increase to imprisonment of up to five years and a fine of up to ten lakh rupees. This chapter aims to regulate and penalize the distribution of obscene material in cyberspace to protect societal morality and reduce exploitation through electronic channels.[16]

IX. Section 67A of the Information Technology Act, 2000-

Punishment for publishing or transmitting material containing sexually explicit acts, etc., in electronic form:

Section 67A of the IT Act, 2000, explicitly addresses the electronic publication or transmission of information that includes sexually explicit acts or conduct. It states that anyone who publishes, transmits, or causes such information to be published or transmitted in electronic form will be subject to legal penalties. Offenders may face a prison sentence of up to five years and a fine of up to ten lakh rupees for their first conviction. If an individual is convicted a second time or repeatedly thereafter, the penalties increase with a longer prison term and a higher fine. This provision aims to prevent the distribution of explicit sexual material on the internet and to uphold digital decency.[17]

Section 67B of the Information Technology Act, 2000-

Punishment for publishing or transmitting material depicting children in a sexually explicit act, etc., in electronic form.:

[16] Information Technology Act,2000 § Section 67, No. 21, Acts of the Parliament,2000(India)
[17] Information Technology Act,2000 § Section 67A, No. 21, Acts of the Parliament,2000(India)

"Whoever –

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in a sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges, or distributes material in any electronic form depicting children in an obscene or indecent, or sexually explicit manner; or

(c) cultivates, entices, or induces children to an online relationship with one or more children for and on a sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates the abuse of children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A, and this section do not extend to any book, pamphlet, paper, writing, drawing, painting, representation, or figure in electronic form–

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is the interest of science, literature, art, or learning, or other objects of general concern; or (ii) which is kept or used for bona fide heritage or religious purposes. Explanation–For the purposes of this section, ―children means a person who has not reached the age of 18 years."[18]

Thus, as per the saying, "Prevention is better than cure", there is a need for more active implementation of these cybersecurity laws in order to make sure that the public, individually and at large, do not suffer from cyberstalking and online harassment, and no harm should be imposed upon them.

[18] Section 67B, No. 21, Acts of the Parliament, 2000(India)

Existing legislation against abuse and harassment had primarily been framed to address in-person interaction with a focus on close physical proximity, direct threats, and tangible proof. Legislation that is not geared towards the online world, therefore, presents victims of cyberharassment with nothing better than legal recourse. Thinking of victims being able to just "log off" is from a bygone era and fanciful in times of hyper-connectedness, where all social, economic, and financial activity is almost entirely reliant upon online media. Besides, even when a victim exits online platforms, offending material can continue to spread and influence their professional and personal life without their awareness or consent.

A second issue is that cybercrimes cross national borders. Unlike traditional harassment, which typically occurs within a single jurisdiction, cyber-harassment can originate from anywhere in the world, making legal enforcement extremely challenging. Different countries have varying laws regarding online abuse, and processes like extradition or international cooperation between governments can be slow and ineffective. Without unified policies addressing online harassment, offenders may exploit loopholes by operating from jurisdictions with weak enforcement systems.

The gap between offline and cyber harassment highlights the inadequacy of traditional legal approaches in addressing the complexities of online abuse. The characteristics of online harassment—such as its pervasiveness, anonymity, global reach, and delayed impact—pose significant challenges that require tailored legal responses. As the online environment continues to expand, it is crucial for the legal framework to evolve in order to provide victims of cyber harassment with the same level of protection as those experiencing abuse in the physical world. Without proactive reforms, online harassment is likely to worsen, leaving victims vulnerable in a legal system that has not yet fully recognized the seriousness of digital abuse.

LEGAL FRAMEWORKS OF THE UNITED STATES AND UNITED KINGDOM:

UNITED STATES-

A cross-sectional national online survey in the USA was conducted involving 1,588 adolescents. The participants, aged between 10 and 15, were required to have accessed the Internet at least once in the past six months. The main focus of the survey was on unwanted sexual solicitation online, which includes unsolicited requests to discuss sex, disclose private sexual information, or engage in sexual activities. The findings revealed that 4% of all youths reported experiencing an incident on a social networking site, specifically on a site dedicated

to cyber harassment. Additionally, 15% of youths indicated experiencing unwanted sexual solicitation online within the last year. Approximately 33% of the participants stated that they were victims of online abuse in the past 12 months, with 9% of those incidents occurring specifically on social networking sites.

Among the youths who were targeted, harassment was reported more frequently via instant messaging (55%) compared to social networking sites (27% and 28%, respectively). In contrast, unwanted sexual solicitations were reported more often in chat rooms (32%). [19]

State and federal legislation addressing the issue of stalking is present in the United States because it is a federal system. State laws, in general, fall into one of three categories:

- Legislation that does not explicitly address cyberstalking and
- Legislation that deals with some of its features
- Legislation that specifically addresses the problem of cyberstalking

State statutes that require physical pursuit or do not recognize electronic means of communication as stalking do not cover cyberstalking. The quintessential example in this regard is Maryland's anti-stalking statute that requires actual pursuit. There could be laws against telephone harassment in certain states that are sufficient to encapsulate cyberstalking. Certain states have attempted to fill in this void by amending their current state legislation to include electronic communication. The second category of legislation includes provisions that address certain aspects of cyberstalking. While stalking laws may cover electronic communication, they often do not account for issues such as third-party harassment or instances where communications are not directly delivered to the victim. In New York state law, stalking involving electronic devices is recognized; however, two specific scenarios are not included:

1. When the stalker posts information on the internet instead of sending it directly to the victim (as seen in the case of Amy Boyer).

2. When the stalker uses someone else to harass the victim.

Additionally, some laws stipulate that stalking occurs whenever the "credible threat"

[19] Ybarra & Mitchell, 2007

requirement is fulfilled.

North Carolina and Louisiana laws require that victims of harassment receive electronic communications regarding their cases. Similarly, Florida and Mississippi laws mandate that such messages be sent to a specific individual. However, these provisions do not cover instances of stalking and harassment directed at third parties.

When it comes to cyberstalking, laws fall under a distinct category of state regulations. Only three states, Rhode Island, Ohio, and Washington, have laws specifically addressing third-party harassment resulting from cyberstalking. While there are numerous statutes related to offline stalking, these three states focus solely on cyberstalking cases.

In accordance with state laws concerning civil protection orders, victims can seek these orders against cyberstalkers. Protection orders, along with any other remedies the court may find appropriate, can prevent the stalker from further contact, possessing weapons, or engaging in harassment or abuse. Violating these orders can lead to the offender being held in contempt of court.

In Florida and New York, cyberstalking offenses can be grounds for obtaining civil protection orders.

Threats made across state lines to harm another individual are illegal under the Interstate Communications Act,1934[20]. However, the threat must involve harm or kidnapping, and the communication would be considered serious by a reasonable person under such circumstances.

It's important to note that cyberstalking, which involves harassment without any risk of physical harm, is not covered by this act. For instance, in the case of *United States v. Alkhabaz*[21] "The defendant posted violent sexual fantasies about the daughter of a classmate on the internet." Since there was no element of menace in the message, it was determined that he had not violated the Act.

In 2006, the Federal Telephone Harassment Statute of 1934 was amended to address the issue of cyberstalking. Under the new provisions, any hardware or software that transmits

[20] Interstate Communications Act,1934§, No. US Code § 875, Acts of Parliament, 1934 (USA)
[21] United States v. Alkhabaz, 104 F.3d 1492 (1997)

information over the internet is classified as a telecommunications device. The law makes it a crime to use telecommunications equipment to threaten, abuse, or harass another individual, with penalties of up to two years in jail.

However, there are several significant issues with the Act. One major concern is that it only applies to anonymous communication. Additionally, the Act does not address the solicitation of third-party harassment by the cyberstalker, as it only pertains to direct communication. Critics have also pointed out that the term "annoy" used in the Act is too vague.

Cyberstalking is further addressed by the Federal Interstate Stalking Punishment and Prevention Act of 1996. This Act prohibits the use of an interactive computer device to cause severe mental distress, injury, death, or harassment. Initially, the only requirement for prosecution was that the defendant had crossed state lines; however, this requirement was removed with the 2006 amendment. Because it does not depend on a true threat threshold or limit its application to anonymous messages, this Act is considered more effective than other federal statutes. Nonetheless, it does not include provisions for harassment of parties other than the direct victim.

2. UNITED KINGDOM:

There is no specific UK law that addresses cyberstalking directly; however, there are three main laws that are used to combat harassment, including stalking. The most significant laws related to stalking and cyberstalking are the Telecommunications Act of 1984, the Malicious Communications Act of 1988, and the Protection from Harassment Act of 1997.

Under the Telecommunications Act of 1984, it is illegal to send inappropriate, threatening, or obscene messages. The Malicious Communications Act of 1988 has a broader scope and penalizes individuals who distribute materials or send letters with the intention of causing distress or alarm.

Under Section 1 of the Protection from Harassment Act of 1997[22]An individual is prohibited from engaging in any actions that constitute harassment of another person. This includes actions that the individual knows, or has reasonable grounds to believe, amount to harassment.

According to Section 2A of the Act, three requirements must be met for stalking to be

[22] Participation, E. (n.d.). *Protection from Harassment Act 1997.*

considered an offense:

1. The Code of Conduct

2. Conduct that is contrary to Section 1 of the Act.

3. Code of Conduct that amounts to stalking.

The Harassment Act does not try to define stalking; instead,

"In Section 2A (3), certain activities that would amount to stalking are listed:

- Following a person
- Attempting to contact or contacting a person
- Publishing any statement or other material relating or purporting to relate to a person
- Monitoring the use of the internet or electronic communication of any person
- Watching or spying on a person
- Interfering with property in possession of a person."[23]

CASE LAWS OF INDIAN LEGISLATION

1. *Shreya Singhal v. Union of India*[24] In this landmark ruling, the Supreme Court of India struck down **Section 66A of the IT Act, 2000**, which allowed authorities to arrest individuals for posting "offensive" content online. While this case is not directly related to cyberstalking, it is highly relevant as it establishes a precedent for protecting free speech on the internet. Importantly, it clarifies that this protection cannot be used to justify harassment or abuse. These rulings lay the groundwork for future interpretations of free speech and online behaviour.

The significance of this case lies in its extensive implications for understanding online speech and digital rights in India. The Court emphasized the need to balance state authority with individual freedom. It clarified that while offensive speech may not be criminalized, individual

[23] Protection from Harassment Act,1997§ Section 2A (3), No. 40, Acts of Parliament,1997(UK)
[24] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523; Writ Petition (Criminal) No. 167 OF 2012

targeting or threats of harm, such as those related to cyberstalking, should be treated differently under the law. The ruling helps establish clearer boundaries between acceptable expression and criminal activity, thereby indirectly facilitating legal action for victims of cyberbullying.

2. *Kalandi Charan Lenka v. State of Odisha*[25] This case exemplified cyberstalking and cyber harassment. The victim, a student, faced issues such as manipulated images, threatening emails, and derogatory updates on social media. The Orissa High Court recognized the trauma caused by these actions and underscored the importance of invoking **Section 66E and Section 67 of the IT Act,** along with provisions from the **Indian Penal Code (IPC), such as Section 354D**, which addresses stalking.

The case highlighted the judiciary's acknowledgment of privacy rights in the online environment and emphasized that cyber harassment is a serious offense deserving of legal intervention.

3. *State v. Yogesh Prabhu (2016)*[26] This case focused on the continuous and unwanted online messaging by the accused toward the complainant, which was treated as cyberstalking. It emphasized the application **of IPC Section 354D (stalking) and Section 509 (insulting the modesty of a woman),** along with relevant sections **of the IT [Information Technology] Act, specifically Sections 66A and 67.** The court's conviction of the accused highlighted the seriousness of online stalking and its psychological effects, reinforcing the idea that online actions are subject to the same legal regulations as physical actions under Indian law.

4. *Saurabh Kumar v. State of Haryana (2021)*[27] This case highlighted the dangers of impersonation and anonymous accounts that are used for cyberstalking and cyber harassment. The accused created impersonation accounts to blackmail and harass a woman. The legal response involved the application of IPC Sections 354D and 506 (criminal intimidation), along with provisions from the IT Act, such as Section 66C (identity theft) and Section 67 (posting obscene content). The case emphasized the importance of virtual evidence and the judiciary's adaptability to new forms of harassment. The strong action taken by the court communicated a clear message:

[25] *Kalandi Charan Lenka v. State of Odisha, 2017 SCC OnLine Ori 52*
[26] *State v. Yogesh Prabhu, (2016)*
[27] *Saurabh Kumar v. State of Haryana, (2021)*

Gender-based internet crimes will not be tolerated.

5. *Manik Taneja v. State of Karnataka (2015)*[28] This case, although focused on police behaviour online rather than harassment, is significant for its examination of acceptable online conduct according to the law. The court upheld the petitioners' right to free expression but clarified that when communication exceeds the boundaries of abuse or targeted harassment, it becomes criminal. This case helped delineate the difference between legitimate expression on the internet and harassment, thus making a positive contribution to the emerging jurisprudence surrounding cyberstalking and online abuse.

Thus, it is evident from the aforementioned case laws that cyber abuse is a significant issue that remains largely unrecognized and underreported in India. Although the Information Technology Act of 2000 and the Bharatiya Nyaya Sanhita of 2023 include various provisions to address cybercrimes, many individuals in India are still unaware of their implications and consequences. Therefore, there is an urgent need to raise public awareness about what constitutes cybercrime, its impacts, and the processes for reporting such incidents. Additionally, it is essential to provide individuals with the necessary support to register these cases and seek justice effectively.

CONCLUSION

Cyberstalking and internet harassment are significant and growing threats in today's digitally networked world, impacting individuals of all age groups and backgrounds. These offenses not only create an invasion of privacy and dignity for victims but also significantly affect their mental health and well-being. Moreover, the pervasiveness of these offenses erodes public confidence in the safety of online communities so that an environment of fear and mistrust dominates. The psychological trauma, damage to professional and personal reputations, interference with daily routines, and intrusive nature of these offenses record the necessity for more adequate legal protections and responsive systems able to effectively address them.

In India, important legislation has been introduced to tackle online abuse, most notably through the Information Technology Act of 2000 and the Bharatiya Nyaya Sanhita, 2023. Although these acts are important steps in the right direction, there are a number of challenges preventing

[28] *Manik Taneja v. State of Karnataka, [2015] 1 S.C.R. 156 (2015)*

their proper implementation. Lingering problems include unclear jurisdiction, gaps in enforcement, and prevalent public unawareness regarding the legal recourse available contribute to the challenges presented by victims trying to seek redress. Besides, the legal system is generally lagging behind the speed of rapidly developing technology and the increasing complexity of cyber harassment, and victims are left without redress or support. There have been some significant cases and court rulings that have, however, emphasized the seriousness of cybercrimes and demanded reforms.

To counteract the impact of cyberstalking and online harassment, there must be a multi-dimensional and long-term approach. This strategy needs to involve comprehensive legislative reforms, technological advancements, and educational initiatives. A more robust legal system and courts that can respond promptly in instances of cyber harassment, and proactive police units that specialize in cyber safety are required. In addition, a culture of digital resilience and cyber literacy among users can empower users to utilize the online environment safely and responsibly. By arming people with the knowledge and tools to detect and combat cyberattacks, we can all contribute together towards a safer and more secure internet space.

SUGGESTIONS

1. *Strengthening Laws:* Implement specific cybercrime laws that clearly define and make cyberstalking and online harassment illegal. This should include newer forms of abuse, such as deepfake misuse, identity theft, and coordinated cyberattacks. To keep pace with advancing technology, current laws must be regularly reviewed and updated to ensure they remain effective.

2. Additionally, *establish specialized cybercrime tribunals or judicial benches* with a set timeframe for addressing cases of internet harassment. Justice delayed not only erodes public trust but also leaves victims vulnerable to further exploitation.

3. *Digital Literacy Programs:* Implement comprehensive national programs with the specific objectives of educating all age groups, particularly young people, about their rights under law in cyberspace, rules of safe internet usage, and protocol for reporting cybercrime. The programs will involve practical workshops, web-based training, and community activities to ensure universal availability and appeal to different segments. By prioritizing awareness and comprehension, we can allow individuals to navigate the digital domain responsibly and

assertively, which in turn ensures that instances of cyber-related issues are reduced.

4. *Facilitating Law Enforcement:* Invest in enhancing the operational efficiency of police forces and investigating agencies by the provision of state-of-the-art digital technologies, expertise, and skilled training that promote effective detection, tracing, and prosecution of cybercriminals. This will have to include access to the latest forensic tools, analytics capabilities, and cybersecurity frameworks. In addition, in order to effectively combat cross-border cybercrime, mutual legal assistance treaties (MLATs) and cross-agency cooperation at the global level need to be strengthened, facilitating timely sharing of information as well as best practices.

5. *Victim Support Systems:* Implement robust support mechanisms that offer multifaceted assistance to victims of cyber abuse. This may involve setting up specialized help desks and 24/7 helplines manned by trained professionals who can offer instant psychological support and advice. Collaborating with nongovernmental organizations (NGOs) will increase the provision of legal aid and services for victims going through the aftermath of cyberattacks. Moreover, by using a victim-centered approach that considers the personal needs and experiences of each victim, recovery and rehabilitation can greatly be improved to help victims gain confidence and establish their lives.

6. *Platform Responsibility:* Mandate social media and online platforms to implement proper and efficient content moderation systems with the intent to stifle the spread of offensive content. The platforms must incorporate rapid reporting systems where users can report abusive content or perform rapid identification of abusive content or behavior. They must accelerate the process of deleting the content for safeguarding users. Platforms must also have welldefined procedures for sharing pertinent user data with law enforcement agencies in a way that is compliant with current privacy laws and regulations to safeguard user rights.

7. *International Cooperation:* Promote a collaborative approach among global cyber law enforcement agencies to create a unified response to cybercrime. Convergence of the cybercrime laws of different jurisdictions to seal loopholes that are exploited by global cybercriminals must be accomplished. The authorities may enhance their capacity to investigate and prosecute transborder cybercriminals through the exchange of intelligence, best practices, and resources. Cybersecurity will be boosted globally.

REFERENCES

1. https://www.jstor.org/stable/3312990?read-now=1&seq=23
2. https://www.jstor.org/stable/24118683?read-now=1&seq=29
3. https://www.jstor.org/stable/24395601?read-now=1&seq=22
4. https://pmc.ncbi.nlm.nih.gov/articles/PMC11376467/pdf/cureus-0016-00000066292.pdf
5. https://cyberbullying.org/cyberstalking
6. https://www.myjudix.com/post/cybercrime-punishments-under-bnsbharatiya-nyaya-sanhita
7. Bharatiya Nyaya Sanhita, 2023
8. https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html
9. https://www.cybercrimejournal.com/pdf/mpittarojccjuly2007.pdf
10. https://fire.kerala.gov.in/wp-content/uploads/2022/08/journal-vol10.pdf
11. https://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf
12. https://core.ac.uk/download/pdf/228084254.pdf
13. https://www.researchgate.net/profile/Erum-Hafeez/publication/270342188_Cyber_Harassment_its_implications_on_youth_in_Pakistan/links/54a8c2de0cf256bf8bb7e584/Cyber-Harassmentits-implications-on-youth-in-Pakistan.pdf
14. https://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf
15. https://core.ac.uk/download/pdf/228084254.pdf
16. https://pubmed.ncbi.nlm.nih.gov/24875706/
17. https://pubmed.ncbi.nlm.nih.gov/33181026/
19. Information Technology Act, 2023
20. Protection from Harassment Act, 1997