IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Digital Abuse In India: A Legal Examination Of Cyber Stalking And Online Harassment Under The It Act, 2000

Name of 1st Author Ms. Ankita, Name Of 2nd Author Dr. Parvinder Kaur

Designation of 1st Author Student of LLM 2nd Sem, Designation of 2nd Author Assistant Professor Of Law

UNIVERSITY SCHOOL OF LAW,

RAYAT BAHRA UNIVERSITY, KHARAR (PB), INDIA

Abstract: The Information Technology Act, 2000, was enacted to regulate cyber activities in India and to provide legal remedies for various forms of cybercrime. The Act includes provisions related to unauthorized access, data breaches, and electronic transactions, as well as specific sections dealing with online harassment and cyber stalking. One of the most debated provisions was Section 66A, which was initially intended to prevent online abuse but was later struck down by the Supreme Court of India in 2015 due to concerns over its vague and broad wording that led to misuse. Despite this, the IT Act continues to be the primary legal tool to address digital abuse, along with supplementary provisions in *Bharatiya Nyaya Sanhita, 2023* (*BNS*), such as Sections *77* (stalking), *354* (defamation), and *349(4)* (criminal intimidation).

Index Terms **- Cyber Crime, Digital Abuse, Legal Provision, Online Harassment.**

I. INTRODUCTION

Digital abuse has emerged as a significant challenge in the modern world, where technology and the internet have become integral to daily life. With the rapid advancement of digital communication, individuals now interact, share, and engage on online platforms more than ever before. While these technological innovations have brought numerous benefits, they have also given rise to various forms of online abuse, including cyber stalking and online harassment. In India, digital abuse has escalated significantly in recent years, necessitating a strong legal framework to combat these issues. The Information Technology (IT) Act, 2000, serves as the primary legislation governing cyber-related offenses in the country, including provisions to address cyber stalking and online harassment. However, despite the existence of legal measures, challenges persist in effectively curbing digital abuse and ensuring justice for victims.

Cyber stalking and online harassment refer to persistent, unwanted, and threatening behavior conducted through digital means. Cyber stalkers often exploit online anonymity to intimidate, harass, or exert control

over their victims. Online harassment can take multiple forms, including sending abusive messages, posting defamatory content, hacking into personal accounts, and spreading misinformation.

Despite legal provisions under the IT Act and *BNS*, enforcing laws against cyber stalking and online harassment remains a complex task. Many victims hesitate to report digital abuse due to fear of retaliation, lack of awareness about legal remedies, or skepticism regarding law enforcement's ability to act. Moreover, jurisdictional challenges arise in cybercrime cases since perpetrators can operate from different geographical locations, sometimes even outside India. The absence of clear policies for cooperation between international law enforcement agencies further complicates the prosecution of cybercriminals.

II. BACKGROUND OF DIGITAL ABUSE

Digital abuse encompasses a wide range of harmful activities perpetrated through electronic communication, social media platforms, messaging applications, and other digital means. It includes cyber stalking, online harassment, cyberbullying, identity theft, defamation, and the non-consensual distribution of explicit content. The proliferation of the internet and advancements in technology have facilitated seamless communication, but they have also provided perpetrators with new tools to exploit, harass, and intimidate individuals. In India, the increasing reliance on digital platforms has led to a surge in cybercrimes, necessitating the development of a comprehensive legal framework to address digital abuse effectively.

The primary legislation governing cybercrimes in India is the Information Technology (IT) Act, 2000, which was enacted to regulate digital transactions and cyber-related offenses. The Act provides a legal structure to tackle crimes committed using computers, networks, and digital platforms. Among its key provisions, Section 66C criminalizes identity theft, which is often used in cases of cyber stalking whereperpetrators impersonate victims to deceive, defame, or manipulate them. Similarly, Section 66D penalizes cheating by impersonation using electronic resources, addressing cases where digital identities are misused for fraudulent or malicious purposes.

Online harassment, which includes sending abusive, threatening, or obscene messages through electronic means, falls under Section 67 of the IT Act. This provision criminalizes the publishing or transmission of obscene material in electronic form, imposing penalties for individuals who distribute explicit or offensive content to harass or harm others. Furthermore, Section 67A imposes stricter punishment for transmitting sexually explicit content electronically, which is particularly relevant in cases of revenge porn and image-based sexual abuse. The increasing instances of deepfake technology and unauthorized circulation of private images have amplified the need for stringent enforcement of these provisions.

Apart from the IT Act, provisions under *Bharatiya Nyaya Sanhita, 2023* (*BNS*), *2023*, supplement the legal measures against digital abuse. Section *77* criminalizes stalking, including cyber stalking, by penalizing repeated attempts to contact or monitor a person through digital means without their consent. This provision is particularly significant in addressing persistent online harassment faced by women and vulnerable individuals. Additionally, Section *78* of the *BNS* punishes any act, word, or gesture intended to insult the modesty of a woman, which extends to digital spaces where offensive messages or content are directed at individuals to harass or demean them.

Defamation in the digital sphere is also covered under Section *354* of the *BNS*, which prescribes punishment for publishing false statements intended to harm an individual's reputation. With the rise of social media platforms, instances of online defamation have become widespread, often leading to severe personal and professional consequences for victims. Similarly, Section *349(4)* of the *BNS* addresses criminal intimidation by anonymous communication, a tactic frequently used in cyber harassment where perpetrators hide their identities to threaten or coerce victims.

Recognizing the risks posed to minors in the digital space, the Protection of Children from Sexual Offences (POCSO) Act, 2012, includes provisions to safeguard children from online sexual exploitation and abuse. Section 11 of the Act defines sexual harassment, including sending sexually explicit messages to minors through digital platforms, and Section 15 penalizes the storage and distribution of child sexual abuse material (CSAM). These provisions are crucial in addressing the growing concerns of online child exploitation and grooming.

To ensure accountability among digital platforms, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose obligations on social media intermediaries and online platforms to implement grievance redressal mechanisms, remove harmful content, and prevent the spread of offensive material. These rules enhance the regulatory framework for digital abuse by placing the onus on intermediaries to act against online harassment and cyber stalking.

III. Emergence of Cyber Stalking And Online Harassment

The digital revolution has transformed the way individuals communicate, interact, and conduct business. While the internet has provided immense opportunities for connectivity and information sharing, it has also created new avenues for criminal activities, including cyber stalking and online harassment. These offenses have evolved with the increasing penetration of social media, instant messaging applications, and online forums, allowing perpetrators to exploit digital platforms for harassment, intimidation, and control over victims. Unlike traditional forms of stalking and harassment, which require physical presence, cyber stalking and online harassment occur in virtual spaces, often leaving victims feeling vulnerable and powerless. The emergence of these digital offenses has necessitated a strong legal framework in India, primarily governed by the Information Technology (IT) Act, 2000, supplemented by relevant provisions of *Bharatiya Nyaya Sanhita, 2023* (*BNS*), *2023*, and other legislative measures aimed at regulating digital crimes.

Cyber stalking refers to the persistent and unwanted pursuit of an individual using electronic communication, such as emails, social media messages, or tracking through GPS-enabled devices. This form of digital abuse often includes threats, blackmail, identity theft, and unauthorized surveillance. Section 66C of the IT Act criminalizes identity theft, which is a common tactic used by cyber stalkers to impersonate victims or gain unauthorized access to their personal information. Similarly, Section 66E penalizes the violation of privacy by capturing, transmitting, or publishing images of a person's private areas without their consent, which is frequently used by stalkers to humiliate and intimidate victims. Section 66D criminalizes cheating by impersonation through electronic communication, addressing situations where cyber stalkers create fake profiles to deceive and harass individuals.

In addition to the IT Act, *Bharatiya Nyaya Sanhita, 2023* (*BNS*), provides specific provisions to tackle cyber stalking and online harassment. Section *77* of the *BNS* directly addresses stalking, including its digital form, by penalizing any person who persistently follows, contacts, or attempts to monitor a woman through electronic communication despite her disinterest. The provision prescribes imprisonment of up to three years for first-time offenders and up to five years for repeat offenders, along with a fine. Online harassment also falls under Section *78*, which criminalizes words, gestures, or acts intended to insult the modesty of a woman. This section is particularly relevant in cases where individuals are subjected to sexually suggestive comments, derogatory messages, or offensive content on social media platforms.

Defamation is another form of online harassment that has gained prominence with the widespread use of digital platforms. False accusations, character assassination, and public shaming through social media have become common tactics used to harass and intimidate individuals. Section *354* of the *BNS* deals with criminal defamation, prescribing punishment for any individual who makes false statements with the intent to harm another person's reputation. Additionally, Section *349(4)* criminalizes criminal intimidation through anonymous communication, which is a frequently used method in online harassment cases where perpetrators hide behind fake profiles or encrypted messaging services to threaten their victims.

The harassment of minors in digital spaces has also become a growing concern, prompting the need for stringent legal protections. The Protection of Children from Sexual Offences (POCSO) Act, 2012, contains provisions to address online sexual harassment involving children. Section 11 of the POCSO Act defines sexual harassment, including sending sexually explicit messages or making inappropriate advances through digital platforms. Additionally, Section 15 criminalizes the storage and distribution of child sexual abuse material (CSAM), ensuring strict legal action against individuals who exploit minors through online platforms.

Despite the presence of legal provisions, cyber stalking and online harassment continue to rise due to several challenges in enforcement and awareness. Many victims hesitate to report digital abuse due to fear of retaliation, social stigma, or a lack of trust in law enforcement authorities. Additionally, the anonymity provided by digital platforms allows perpetrators to evade legal consequences, making it difficult for law enforcement agencies to track and apprehend offenders. Cyber stalkers and online harassers often operate from different geographical locations, further complicating jurisdictional issues in prosecution.

.

IV. Definition Of Digital Abuse

Digital abuse refers to any form of harassment, intimidation, control, or exploitation carried out through electronic communication or digital platforms. It includes actions such as sending threatening messages, unauthorized access to personal information, public shaming, stalking through digital means, and the spread of false or malicious content. Digital abuse often involves a violation of privacy, psychological harm, and reputational damage, making it a serious offense under various legal provisions in India.

The IT Act, 2000, provides the primary legal framework for dealing with digital offenses. Section 66E criminalizes the violation of privacy by capturing, transmitting, or publishing private images without consent. Section 67 prohibits the publication or transmission of obscene material in electronic form, while Section 67A deals with sexually explicit content. In addition, Section 66C penalizes identity theft, which is often used in

cases of cyber stalking and impersonation. *Bharatiya Nyaya Sanhita, 2023* (*BNS*), also addresses digital abuse through provisions such as Section *77*, which criminalizes stalking, including cyber stalking, and Section *354*, which punishes defamation. These legal provisions establish a foundation for defining and addressing digital abuse in India.

V. Types Of Digital Abuse

Digital abuse takes various forms, each with distinct legal implications. The most common types include:

i. **Cyber Stalking** – This involves repeated and unwanted surveillance, communication, or threats directed at an individual through digital means. Cyber stalking is addressed under Section *77* of the *BNS*, which penalizes persistent online monitoring and harassment.

ii. **Online Harassment** – This includes sending abusive, threatening, or obscene messages, making derogatory remarks, or spreading false information with the intent to harm an individual's mental well-being. Section 67 of the IT Act penalizes the publication of obscene material, while Section *78* of the *BNS* criminalizes words, gestures, or acts intended to insult a woman's modesty.

iii. **Identity Theft and Impersonation** – Perpetrators may misuse a victim's personal information or create fake profiles to deceive, harass, or defame them. Section 66C of the IT Act criminalizes identity theft, and Section 66D penalizes cheating by impersonation using digital means.

iv. **Cyber Defamation** – The digital space has become a platform for spreading false information or defamatory content. Section *354* of the *BNS* provides punishment for defamation, and Section 66A of the IT Act (before its repeal) dealt with offensive online content.

v. **Revenge Porn and Image-Based Sexual Exploitation** – The non-consensual sharing of intimate images is a serious form of digital abuse. Section 67A of the IT Act criminalizes the electronic transmission of sexually explicit content, while Section 354C of the *BNS* penalizes voyeurism.

vi. **Doxxing (Unauthorized Disclosure of Personal Information)** – This involves publicly revealing personal details of an individual, such as home addresses, phone numbers, or private conversations, often leading to harassment. **Section 72** of the IT Act penalizes unauthorized disclosure of information obtained through electronic means.

vii. **Cyberbullying** – The use of digital platforms to intimidate, threaten, or humiliate individuals, especially minors, is a growing concern. The Protection of Children from Sexual Offences (POCSO) Act, 2012, provides safeguards against online sexual harassment involving minors.

viii. **Hate Speech and Online Threats** – The spread of communal, caste-based, or gender-based hatred on digital platforms is a serious issue. **Section *194*** and **Section *297*** of the *BNS* penalize acts that promote enmity between different groups based on religion, race, or place of birth.

VI. CAUSES AND CONSEQUENCES OF CYBER STALKING AND ONLINE HARASSMENT:

- **Causes of Cyber Stalking and Online Harassment**

The rise of cyber stalking and online harassment can be attributed to multiple factors:

1. **Anonymity of Digital Platforms** – The internet allows perpetrators to hide their identities, making it easier to engage in abusive behavior without fear of immediate consequences.

2. **Lack of Digital Literacy** – Many internet users are unaware of the risks associated with sharing personal information online, making them vulnerable to cybercrimes. The issue of cyberstalking and online harassment has emerged as a significant challenge in the digital age, necessitating a comprehensive legal response.

3. **Inadequate Law Enforcement Mechanisms** – The lack of specialized cybercrime units and delays in legal action often allow perpetrators to continue their offenses unchecked.

4. **Social and Cultural Factors** – Gender-based discrimination, misogyny, and victim-blaming discourage individuals from reporting digital abuse.

5. **Technological Advancements** – The development of artificial intelligence, deepfake technology, and encrypted messaging services has enabled more sophisticated forms of cyber abuse.

- **Consequences of Cyber Stalking and Online Harassment:**

The impact of digital abuse extends beyond the virtual realm, affecting victims psychologically, socially, and economically. Some consequences include:

1. **Mental and Emotional Trauma** – Victims often experience anxiety, depression, and post-traumatic stress due to constant digital harassment.

2. **Reputational Damage** – False accusations, defamatory content, and revenge porn can severely harm an individual's personal and professional reputation.

3. **Privacy Violations** – Unauthorized access to personal information can lead to identity theft, financial fraud, and stalking.

4. **Social Isolation** – Victims may withdraw from online and offline interactions to escape harassment, leading to a loss of social connections.

5. **Legal and Financial Burdens** – Pursuing legal action against perpetrators can be costly and time-consuming, discouraging victims from seeking justice.

VII. Conclusion

The issue of cyberstalking and online harassment has emerged as a significant challenge in the digital age, necessitating a comprehensive legal response. The evolution of technology, particularly the rise of social media, digital communication platforms, and artificial intelligence-driven content, has facilitated the proliferation of digital abuse. While the Information Technology (IT) Act, 2000, serves as the primary legislation governing cyber offenses in India, there remain critical gaps in its implementation, enforcement, and alignment with global best practices. The legal framework must evolve to address emerging threats, ensure stronger victim protection mechanisms, and impose stricter accountability on digital intermediaries.

The legal definition of cyberstalking and online harassment under the IT Act, 2000, and relevant provisions of *Bharatiya Nyaya Sanhita, 2023* (*BNS*), *2023*, offer a broad yet insufficient foundation to tackle digital abuse. Section 66A of the IT Act was previously used to penalize online harassment, but its revocation has created a legal vacuum, necessitating alternative provisions such as Sections 66C, 66D, and 67 of the IT Act, alongside *BNS* Sections *77* (stalking), *78* (outraging a woman's modesty), and 503 (criminal intimidation). However, these provisions do not comprehensively address the nuances of digital abuse, especially in cases involving AI-generated deepfakes, anonymous cyber threats, and cross-border digital harassment. The lack of a uniform legal definition further complicates enforcement, leaving law enforcement agencies and judiciary with inconsistent interpretations of cyber offenses.

REFERENCES

[1] Ashar, "Social Media Impact: How Social Media Sites Affect Society," American Public University, May 2, 2024.

[2] Victims Commissioner. "Impact of Online Abuse and Harassment Revealed in New Research from the Victims' Commissioner." 2022. Available at: https://victimscommissioner.org.uk/news/impact-of-online-abuse-and-harassment-revealed-in-new-research-from-the-victims-commissioner (last visited March 22, 2025).

[3] Mahawar Sneha, "Information Technology Act, 2000," iPleaders, 2022. Available at: https://blog.ipleaders.in/information-technology-act-2000/ (last visited March 22, 2025).

[4] Protecting Childhood: Legal Safeguards Against Online Child Exploitation, Legal Service India. Available at: https://legalserviceindia.com/legal/article-19738-protecting-childhood-legal-safeguards-against-online-child-exploitation.html (last visited March 22, 2025).

[5] Esafety Commissioner. "Cyber Stalking." Available at: https://www.esafety.gov.au/key-topics/staying-safe/cyberstalking (last visited March 23, 2025).

[6]Drishti Judiciary. "Defamation and Social Media: Protecting Your Reputation Online." Available at: https://www.drishtijudiciary.com/blog/defamation-and-social-media-protecting-your-reputation-online (last visited March 23, 2025).

[7] Ahmed, Rashed. "Cyber Harassment in the Digital Age: Trends, Challenges, and Countermeasures." Preprints.org, 2024. Available at: https://www.preprints.org/manuscript/202409.1882/v1 (last visited March 23, 2025).

[8]Vikaspedia. "Definition of Digital Abuse." Available at: https://en.vikaspedia.in/viewcontent/education/digital-litercy/information-security/being-safe-online-1/cyber-harassment (last visited March 23, 2025).

[9] Cyber Lawyer. "Section 67 of Information Technology Act: Punishment for Publishing or Transmitting Obscene Material in Electronic Form." Info. Technology Law, 2014. Available at: https://www.itlaw.in/section-67-punishment-for-publishing-or-transmitting-obscene-material-in-electronic-form/ (last visited March 24, 2025).

[10] Ossa, Francisca. "The Role of Anonymity in Online Harmful Conducts: Is Regulation the Answer?" Universidad de Chile, 2024. Available at: https://www.researchgate.net/publication/379971586_The_role_of_anonymity_in_online_harmful_conducts_is_regulation_the_answer (last visited March 24, 2025).

[11] NCBI. "WWW Error Blocked Diagnostic." Available at: https://www.ncbi.nlm.nih.gov/books/NBK207191/ (last visited March 24, 2025).