INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 4 | Issue 1 Art. 17

2025

Preventing Online Harassment: Legal approaches to Cyberstalking, Cyberbullying and Defamation in Cyberspace

Sarah Kikon and Jyotirmoy Banerjee

Recommended Citation

Sarah Kikon and Jyotirmoy Banerjee, *Preventing Online Harassment: Legal approaches to Cyberstalking, Cyberbullying and Defamation in Cyberspace*, 4 IJHRLR 230-248 (2025).

Available at www.humanrightlawreview.in/archives/.

Preventing Online Harassment: Legal approaches to Cyberstalking, Cyberbullying and Defamation in Cyberspace

Sarah Kikon and Jyotirmoy Banerjee

LLM Student, Amity Law School, Amity University, Bengaluru
Assistant Professor, Amity Law School, Amity University, Bengaluru

Manuscript Received	Manuscript Accepted	Manuscript Published
09 Jan. 2025	11 Jan. 2025	14 Jan. 2025

ABSTRACT

The rapid growth of digital technology has revolutionised communication, enabled global connectivity while also facilitated harmful behaviours like online harassment. Cyberstalking, cyberbullying, and online defamation have become widespread threats, exploiting the anonymity and far-reaching nature of the internet. These forms of harassment severely impact individuals' mental health, privacy, and reputations, underscoring the need for comprehensive legal and social responses. This paper explores legal approaches to addressing online harassment across various jurisdictions, examining both successes and shortcomings. While countries such as the United States, India, and Australia have implemented laws targeting cybercrimes, challenges persist in enforcement due to jurisdictional issues, the anonymity of the internet, and technological limitations. The paper also addresses the delicate balance between protecting free speech and preventing harm, especially in cases of online defamation. In addition to legal frameworks, technological solutions play a critical role in combating online harassment. Innovations in artificial intelligence, content moderation, and real-time monitoring offer promising tools for detection and intervention. However, these technologies also raise concerns regarding privacy, potential misuse, and the limitations of automated systems. International collaboration is key to tackling cross-border cybercrimes, but differing legal standards and resource constraints present significant obstacles. The paper calls for harmonized laws and data-sharing agreements to overcome these barriers. Finally, educational and social interventions are crucial

in preventing online harassment. Promoting digital literacy, raising awareness of the issue, and fostering empathy in online interactions can reduce harmful behaviours. Schools, workplaces, and communities must work together to build safer digital spaces. By combining strong legal frameworks, technological innovation, and social education, this paper advocates for a comprehensive, multi-pronged approach to preventing online harassment and safeguarding individuals in the digital era.

KEYWORDS

Cyber Harassment, Online Defamation, Digital Privacy, Legal Frameworks, Cybersecurity, Digital Literacy

- ***INTRODUCTION***

The internet has fundamentally transformed human interaction, becoming an essential part of everyday life. From social networking and e-commerce to education, digital platforms offer unparalleled opportunities for communication, collaboration, and the exchange of information. However, this digital revolution has also brought about significant challenges, notably the rise of online harassment.

Online harassment encompasses various forms of abusive behaviour, including cyberstalking, cyberbullying, and online defamation. These actions take advantage of the unique aspects of cyberspace anonymity, global reach, and permanence to inflict psychological, emotional, and social harm on victims.[1]The effects can be devastating, leading to anxiety, depression, repetitional damage, and, in extreme cases, self-harm or suicide.[2]

Cyberstalking involves ongoing, intrusive behaviours like monitoring or threatening individuals through digital means. Cyberbullying, which often targets vulnerable groups such as minors, uses online platforms to intimidate, shame, or harass victims. [3]

[1] Alice E. Marwick & Ross Miller, *Online Harassment, Defamation, and Hateful Speech: A Primer of the Legal Landscape*, (2014), https://papers.ssrn.com/abstract=2447904 (last visited Jan 7, 2025).

[2] SocialMedia And Defamation: Legal Implications, http://legalserviceindia.com/legal/article-18213-social-media-and-defamation-legal-implications.html (last visited Jan 7, 2025).

[3] Chanelle Wilson, Lorraine Sheridan & David Garratt-Reed, What Is Cyberstalking? A Review of Measurements, 37 J Interpers Violence NP9763 (2022), https://journals.sagepub.com/doi/ 10.1177/0886260520985489 (last visited Jan 6, 2025).

Online defamation involves spreading false information to harm an individual's reputation, with the viral nature of social media amplifying its impact. While many countries have acknowledged the need for legal responses to online harassment, enforcing these laws remains difficult due to the constantly evolving nature of cybercrimes, jurisdictional issues, and the anonymity of perpetrators.

In addition to legal measures, technological solutions, international collaboration, and public education are crucial in fostering safer online environments.

This paper examines legal approaches to combating cyberstalking, cyberbullying, and defamation in cyberspace. It assesses the effectiveness of current laws, identifies challenges in enforcement, and explores the potential of complementary strategies, such as technology and education, to mitigate online harassment. By adopting a comprehensive approach, the paper aims to contribute to the ongoing efforts to make cyberspace a safer and more inclusive space for all users.

UNDERSTANDING CYBERSTALKING: LEGAL DEFINITION AND KEY ELEMENTS

Cyberstalking is a form of online harassment where an individual uses electronic communication to intimidate, threaten, or cause distress to another person or group. This behaviour, which can be difficult to track, often involves repeated unwanted contact through emails, text messages, phone calls, social media posts, or other digital platforms. Stalkers may also use hacking or spyware to access victims' personal information or monitor their online activities.[4] What makes cyberstalking particularly harmful is its ability to occur 24/7, leaving victims feeling trapped and unable to escape. Common tactics include sending threatening messages, spreading false rumours, posting explicit content, creating fake profiles, and impersonating the victim online to damage their reputation. The psychological toll on victims can be severe, leading to anxiety, depression, and social isolation, while physical symptoms like headaches and fatigue are also common.

Cyberstalking is illegal in many countries, including India, where it is addressed under the Information Technology Act, 2000, and the Indian Penal Code (IPC). In one case, a woman from Delhi was repeatedly harassed by an acquaintance through threatening emails and fake profiles. The stalker was eventually arrested after using spyware to monitor her online activity, reflecting India's

[4] Louise Ellison, Cyberstalking: Tackling Harassment on the Internet, in Crime and the Internet (2001).

growing efforts to combat digital harassment.

- ***PREVENTING CYBERSTALKING***

There are several proactive steps individuals can take to protect themselves from cyberstalking. One of the most effective measures is to keep personal information secure by using strong, unique passwords, limiting what is shared online, and being cautious about who they interact with on digital platforms. It's also essential to adjust privacy settings on social media to control who can access personal information and posts.

In addition to safeguarding themselves, individuals can play a key role in preventing cyberstalking by reporting suspicious or harassing behaviour to law enforcement or the relevant online platforms. Most social media sites have reporting tools to flag abusive behaviour, and local authorities can assist with serious cases of cyberstalking. By taking these precautions and staying vigilant, individuals can reduce the risk of cyberstalking and contribute to creating a safer digital environment. [5]Understanding the nature and impact of cyberstalking, along with the legal consequences for perpetrators, empowers people to protect themselves and help prevent this harmful behaviour from spreading.

CYBERBULLYING: LEGAL FRAMEWORKS AND SOCIAL IMPLICATIONS

Bullying, in any form, is an act of humiliation that can occur anywhere whether in schools, workplaces, homes, or even online. While traditional bullying happens face-to-face, cyberbullying, which occurs in the virtual world, presents a different challenge. In the physical world, victims may have the option to escape or avoid the bully, but in the online realm, the harassment can be [6]relentless, with no clear escape and limited control over the situation.

In India, cyberbullying has become a significant concern, particularly among students, as digital services and social media usage have surged. 6However, there is no specific law in India that directly addresses cyberbullying, although various sections of

[5] Ameema Miftha, The Social, Legal, and Technical Perspectives of Cyberstalking in India (2024), https://uobrep.openrepository.com/handle/10547/626190 (last visited Jan 6, 2025).

[6] Manpreet Kaur & Munish Saini, Indian Government Initiatives on Cyberbullying: A Case Study on Cyberbullying in Indian Higher Education Institutions, 28 Educ Inf Technol 581 (2023), https:// doi.org/10.1007/s10639-022-11168-4 (last visited Jan 6, 2025).

existing laws, like the Information Technology Act, 2000, are used to tackle related issues such as cyberstalking and harassment. While the IT Act was initially established to deal with e-commerce, Indian courts have applied it to address cyberbullying, as well.

Cyberbullying is defined as any aggressive, intentional behaviour using electronic means to harm or intimidate a victim who cannot easily defend themselves. It can involve communication via computers, mobile phones, or other devices, through text messages, social media, emails, or group chats. [7]Examples include spreading harmful rumours, sharing humiliating photos or videos, creating defamatory websites, issuing online threats, and impersonating others to spread false information. Such behaviours can escalate to serious consequences, including threats of violence or suicide.

Understanding the different forms of cyberbullying is crucial for parents, young people, and educators to recognize and report it. Some common forms of cyberbullying include posting degrading comments or rumours online, publishing embarrassing photos or videos, making slanderous websites, threatening harm or suicide, spreading hate speech, and falsifying identities online. The internet, while offering opportunities for connection and awareness, also has a darker side, where individuals can engage in harassment while hiding behind the anonymity of screens. This has led many young people to experience confusion and fear, often not realizing that what they are enduring is a form of bullying.'

- ***Forms of Cyberbullying***

Cyberbullying can take many forms, but all involve the use of the internet and electronic devices like cell phones or computers, with the common aim of causing harm to the victim.

One common form is flaming, which occurs when the bully and the victim exchange angry, threatening, or abusive messages often through emails, texts, or social media designed to intimidate or distress the victim. [8]Another form, exclusion, happens when the victim is deliberately left out of online

[7] Christian Licoppe & Zbigniew Smoreda, Are Social Networks Technologically Embedded?: How
Networks Are Changing Today with Changes in Communication Technology, 27 Social Networks 317 (2005), https://www.sciencedirect.com/science/article/pii/S0378873304000619 (last visited Jan 6, 2025).

[8] Cyberbullying and Legal Remedies, LAW Notes (Mar. 21, 2024), https://lawnotes.co/cyberbullying-and-legal-remedies/ (last visited Jan 7, 2025)

groups or chat rooms, with the bully and other group members sending harmful messages, sharing the victim's private photos, or spreading malicious rumours to isolate and humiliate them. Outing involves intentionally posting or sharing someone's private information or photos online, often on social media, to embarrass or retaliate against them. The individual whose information is exposed is said to be "outed." Lastly, impersonation occurs when a bully creates a fake online profile or pretends to be someone else to damage the victim's reputation or manipulate their online presence. While these methods vary, all share the common goal of inflicting emotional, psychological, or social harm on the victim, often leaving them feeling humiliated, vulnerable, or powerless.

- ***Remedies Provided Under Indian Laws IT Act, 2000***

The Information Technology Act, 2000, amended in 2008, is a law established by the Government of India to address cybercrimes and outline penalties for such offenses. Although this legislation defines various forms of cybercrime, including cyberbullying, and provides penalties for them, India currently lacks a specific law that directly addresses cyberbullying.[9]

Cyberbullying can have a severe and lasting impact on victims, sometimes leading to tragic consequences like suicide. While cyberstalking was criminalized in the 2013 amendment to the Act, cyberbullying remains unaddressed as a standalone offense[10]. However, certain provisions in the Act, particularly in Chapter XI, offer recourse for victims of cyberbullying:

The provision deals with the transmission of offensive, derogatory, or harmful content via electronic platforms such as social media or group chats[11]. The Supreme Court of India has struck down Section 66(A) for being vague and unconstitutional, as it was seen to unnecessarily limit the right to free expression[12].

This provision addresses the use of technology to impersonate or blackmail someone online. Offenders face up to three years in prison and a fine of at least one lakh rupees

[9] Sesha Kethineni, Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms, in The Palgrave Handbook of International Cybercrime and Cyberdeviance 305 (Thomas J. Holt & Adam M. Bossler eds., 2020), https://doi.org/10.1007/978-3-319-78440-3_7 (last visited Jan 6, 2025).
[10] Sabrina S. Rapisarda & Kimberly R. Kras, *Cyberstalking*, *in* Handbook on Crime and Technology 303 (2023), https://www.elgaronline.com/edcollchap/book/9781800886643/book-part-9781800886643-27.xml (last visited Jan 7, 2025).
[11] Information Technology Act, 2000, Sec 66A
[12]Shreya Singhal v. Union of India, 2015 AIR SCW 1989 AIR 2015 SC

if they mislead or harm someone through impersonation on social media[13].Further the act penalizes the breach of privacy, including the unauthorized use of a person's images or personal information for malicious purposes, with fines of up to 3 lakh rupees or imprisonment for up to three years[14]. In case of publication or transmission of obscene content over the internet. Violators can face up to five years in prison and fines of up to 10 lakh rupees[15].

- ***Indian Penal Code, 1860***

The Indian Penal Code (IPC), which governs criminal offenses in India, does not have explicit provisions for cyberbullying but does include sections that address behaviors often linked to cyberbullying. Section 507 criminalizes threats made anonymously, including online threats. Offenders can face up to two years in prison for threatening or coercing someone without revealing their identity, a common tactic in cyberbullying[16]. Section 354(C) punishes the act of secretly photographing or watching a woman in a private situation without her consent. This can apply to cyberbullying cases where such images are taken or shared online without the victim's permission, with penalties ranging from one to three years in prison for the first offence[17].

According to Section 354(D) makes stalking, including monitoring someone's online activities or movements without their consent, a criminal offence. Cyberstalkers can face up to three years in prison under this section[18]. Section 499 addresses defamation, including sending derogatory messages or posts via email or social media. If the content damages the victim's reputation or mental well-being, it may be considered a form of cyberbullying and carry legal consequences.

DEFAMATION IN CYBERSPACE: CHALLENGES IN ENFORCEMENT

The internet has transformed communication by offering a fast and cost-effective platform for sharing text, sound, and images. With minimal political or content restrictions, it provides an open space for information exchange, limited only by the willingness of providers to share their resources. 12As a result, informational websites are multiplying, many hosted by ISPs or IT departments

[13] Information Technology Act, 2000, Sec 66D
[14] Information Technology Act, 2000, Sec 66E
[15] Information Technology Act, 2000, Sec 66F
[16] Indian Penal Code, Sec Section 507
[17] Indian Penal Code, Sec Section 354(C)
[18] Indian Penal Code, Sec Section 354(D)

and indexed by search engines[19]. However, businesses often overlook the risks associated with website hosting, particularly regarding defamatory content. If an employee posts racist, sexist, or defamatory statements about a competitor on a company website, liability becomes a significant concern[20].

What sets the internet apart from traditional media is its interactivity and the sense of freedom it offers users. This sense of freedom, however, can lead to misuse. The accessibility of the internet has contributed to a dramatic rise in defamation cases, as the low cost of website creation and internet access makes it easier for anyone to publish content and face potential legal consequences.[21] Additionally, the anonymity provided by email and bulletin board postings allows individuals to make defamatory statements without revealing their identity, exacerbating the issue. As the internet continues to permeate daily life, the risks associated with defamation grow, highlighting the need for a reassessment of how defamation laws apply in the digital age[22].

- ***Cyber Defamation - A Socio-Economic Offences*:**

  Cyber law covers a wide range of issues, including cybercrimes, electronic commerce, freedom of expression, intellectual property, privacy, and jurisdiction. Cybercrimes include fraud, unauthorised access, cyberstalking, and defamation. While defamation, obscenity, and censorship are part of free speech, the rapid spread of defamatory content online presents unique challenges. The anonymity of the internet enables harmful information to spread quickly, making it difficult to control or prevent. Cyber defamation can severely damage an individual's reputation or a company's financial standing, affecting the broader economy as well.

  Unlike traditional crimes, cyber defamation involves indirect

[19] Sheeraz A. Alvi et al., *Internet of Multimedia Things: Vision and Challenges*, 33 Ad Hoc Networks 87 (2015), https://www.sciencedirect.com/science/article/pii/S1570870515000876 (last visited Jan 7, 2025).

[20] Manpreet Kaur & Munish Saini, *Indian Government Initiatives on Cyberbullying: A Case Study on Cyberbullying in Indian Higher Education Institutions*, 28 Educ Inf Technol (Dordr) 581 (2023), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9251041/ (last visited Jan 7, 2025).

[21] A Companion to Media Studies, (Angharad N. Valdivia ed., 1 ed. 2003), https:// onlinelibrary.wiley.com/doi/book/10.1002/9780470999066 (last visited Jan 6, 2025).

[22] Ishan Atrey, Cybercrime and Its Legal Implications: Analysing the Challenges and Legal Frameworks Surrounding Cybercrime, Including Issues Related to Jurisdiction, Privacy, and Digital Evidence, (2023), https://papers.ssrn.com/abstract=4789133 (last visited Jan 6, 2025).

harm, often committed in secrecy by skilled individuals using advanced technology. The law must adapt to address these challenges, as the damage is often done before legal action can be taken. Jurisdictions worldwide face the difficulty of handling such cases, with potential defendants liable for defamation across multiple countries. The consequences of cyber defamation extend beyond the victim, impacting public welfare and economic stability. As cybercrimes evolve, so too must the legal framework to mitigate their impact.

- ***Liability Under Cyber Defamation***

Legal liability for cyber defamation varies by jurisdiction, with individuals potentially facing both civil and criminal penalties. Civil liability typically involves a lawsuit seeking damages for harm caused by defamation, where the plaintiff must prove that the statement was false, harmful, and communicated to a third party. Criminal liability, where applicable, involves prosecution by the state, with a higher burden of proof, requiring evidence of malicious intent or recklessness. Additionally, individuals may face disciplinary action from employers or professional bodies if the defamation relates to their professional conduct.[23]

- ***Provisions Governing Cyber Defamation In India***

According to Section 499 of the Indian Penal Code (IPC) defines defamation as an act where someone intentionally harms another's reputation through false statements, knowing it may cause damage. This includes acts of public slander, physical abuse, or any behaviour that tarnishes an individual's image. [24]For instance, if two people have a disagreement and one of them spreads harmful content on social media, it could be considered defamation under this section. Online platforms are often misused for defamatory purposes, with such actions falling under this category[25].

The provision prescribes the punishment for defamation, stating that anyone found guilty under Section 499 can be punished with a fine or imprisonment for up to two years[26]. Further this provision addresses forgery, which involves

[23] Defamation Laws And Judicial Intervention: A Critical Study - ProQuest, https:// www.proquest.com/openview/275515b31553f97943ba77d9749f2c24/1?pqorigsite=gscholar&cbl=2035897 (last visited Jan 6, 2025).
[24] Ankit Valdaya, Legal Consequences of Online Defamation in India, (2014), https:// papers.ssrn.com/abstract=2386983 (last visited Jan 6, 2025).
[25] Indian Penal Code, 1860, Sec 499
[26] Indian Penal Code, 1860, Sec 500

creating false documents with the intent to harm someone's reputation. Anyone found guilty of forging documents in this manner can face up to three years in prison or a fine[27].

Criminal intimidation as threatening harm to someone's reputation, property, or someone closely associated with them. The intent is to cause fear and coercion to make the victim act in a particular way. Anyone committing criminal intimidation can be punished with up to three years of imprisonment, a fine, or both[28].

- ***Case Studies***

In the case of *SMC Pneumatics (India) Pvt. Ltd. vs Shri Jogesh Kwatra on 12th February 2014*, a Delhi Court took jurisdiction over a matter involving online defamation, where the reputation of a company was being tarnished through electronic messages. This case marked India's first significant instance of legal action against digital defamation, with the court issuing a major ex-parte order in favour of the aggrieved party. [29]

In the case of *Rajiv Dinesh Gadkari vs Smt. Nilangi Rajiv Gadkari on 16th October 2009*[30], the respondent filed a lawsuit against her husband after receiving a divorce notice. She accused him of sending obscene images and defaming her. The wife sought a monthly maintenance of Rs. 75,000 as compensation for the offense. In the case of *Kalandi Charan Lenka vs State of Odisha*[31], the victim was repeatedly stalked by the accused, who created a fake profile of her and sent inappropriate messages to her friends. Additionally, a manipulated photo of the victim was posted on the walls of a hotel. The court held the offender accountable for these actions.

ROLE OF TECHNOLOGY IN PREVENTING CYBER

[27] Indian Penal Code, 1860, Sec 469
[28] Indian Penal Code, 1860, Sec 503
[29] Cyber Law Case Analysis of SMC Pneumatics (India) Pvt. Ltd. VS Shri Jogesh Kwatra - IA1 SUBMISSION Studocu,https://www.studocu.com/in/document/jagran-lakecity-university/cyber-law-and-cyber-security/cyber-law-case-analysis-of-smc-pneumatics-india-pvt-ltd-vs-shri-jogesh-kwatra/26666670(last visited Jan 7, 2025).
[30] Rajiv Dinesh Gadkari vs Smt. Nilangi Rajiv Gadkari, AIR 2010 (NOC) 538 (BOM.)
[31] Kalandi Charan Lenka Petitioner v. State Of Odisha Opposite Party, Orissa High Court, Judgment, Law, casemine.com, https://www.casemine.com, https://www.casemine.com/judgement/in/5b1a327c4a932631a5a0c01f (last visited Jan 7, 2025).

HARASSMENT

Technology plays a critical role in preventing and addressing cyber harassment by providing a range of tools for detection, intervention, and legal action. Al-powered systems are used by social media platforms to automatically detect harmful content such as hate speech, cyberbullying, and threats, often flagging or removing abusive material before it escalates.[32]

These platforms also feature reporting and blocking options, allowing users to quickly flag harassment and limit communication with perpetrators. Enhanced privacy settings further empower individuals by giving them control over who can access their profiles or send them messages. Additionally, end-to-end encryption on messaging apps ensures that communication remains secure and prevents misuse of personal data. [33]Tools for monitoring one's digital footprint also alert users when their information is being misused, such as in cases of doxing.

Sentiment analysis and machine learning help identify subtle forms of abuse by analysing text and online interactions for harmful patterns, which can lead to quicker intervention. Technology also supports law enforcement by enabling data sharing and tracking offenders, while digital evidence can be preserved for legal purposes. Moreover, online platforms are adopting stricter policies and working with authorities to prevent and punish cyber harassment. Educational campaigns and digital safety programs raise awareness about how to recognize and protect oneself from online abuse. While technology is a powerful tool, it works best in conjunction with cultural changes toward greater accountability and responsibility in online spaces.23

- ***Role of Social Media Platforms and ISPS In Enforcement***

Social media platforms and Internet Service Providers (ISPs) play vital roles in combating cyber harassment. Social media platforms use Al, content moderation, and reporting systems

[32] Seema Babusing Rathod, Anita G. Khandizod & Rupali A. Mahajan, Cybersecurity Beyond the
Screen: Tackling Online Harassment and Cyberbullying, in AI Tools and Applications for Women's Safety 51 (2024), https://www.igi-global.com/chapter/cybersecurity-beyond-the-screen/www.igiglobal.com/chapter/cybersecurity-beyond-the-screen/337755 (last visited Jan 6, 2025).

[33] Greg Nojeim & Namrata Maheshwari, Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth, 17 Indian J. L. & Tech. 1 (2021), https:// heinonline.org/HOL/Page?handle=hein.journals/indiajoula17&id=43&div=&collection=.

to detect and remove harmful content, suspend abusive accounts, and provide tools like blocking or restricting access to prevent further harassment. Platforms also cooperate with law enforcement to track down offenders involved in serious criminal activities.[34]

ISPs help by monitoring internet traffic, blocking harmful websites, and potentially identifying perpetrators through IP addresses when harassment occurs. They cooperate with authorities to share data for legal investigations and often have policies in place to prevent abuse on their networks. While both platforms and ISPs are crucial in addressing online harassment, challenges remain, such as distinguishing between free speech and harmful content and dealing with jurisdictional issues. Ongoing collaboration among platforms, ISPs, law enforcement, and policymakers is essential to enhance enforcement and protect users.

LEGAL REMEDIES AND PUNISHMENTS FOR ONLINE HARASSERS

The growth of the internet and social media platforms has revolutionized communication, offering numerous benefits. However, it has also given rise to a troubling new form of abuse online harassment. In today's digital era, individuals are increasingly vulnerable to various forms of online abuse, including cyberbullying, cyberstalking, hate speech, and the non-consensual sharing of intimate images, commonly referred to as "*revenge porn*".

As internet use in India continues to rise, online harassment has become an escalating concern, especially for women and marginalized groups. Beyond its emotional and psychological toll, online harassment can have serious impacts on a person's personal and professional life. If you are experiencing online harassment in India, there are several steps you can take to seek help and report the abuse.

- ***Case Studies and Precedents in Cyber Harassments***

In 2022, a deeply troubling incident of online harassment occurred in India, where several Muslim women journalists were targeted in a campaign of humiliation. Their photos were uploaded to GitHub, a Microsoft-based platform, accompanied by text that implied these women were being auctioned, not for

[34] Ritu Pareek, Cyber Crime in India: An Indian Perspective, in Cyberfeminism and Gender Violence in Social Media 252 (2023), https://www.igi-global.com/chapter/cyber-crime-in-india/ www.igi-global.com/chapter/cyber-crime-in-india/331910 (last visited Jan 6, 2025).

sale, but for the purpose of public degradation. [35]Unlike the impersonation of journalist Rana Ayyub, these photos, taken from various online sources, were paired with degrading and sexually explicit comments.

The police responded by filing charges under Section 67 of the Information Technology Act, which deals with obscenity, as well as provisions of the Indian Penal Code for promoting religious enmity and insulting women's modesty. Two cases were filed, one in Delhi and one in Mumbai, but in both instances, the accused were granted bail. [36]The courts cited the perpetrators' ages, their intent (mens rea), and their non-criminal family backgrounds as justifications for the bail. There was no indication that the courts recommended counselling for the offenders or took measures to prevent further harassment against these women or others in the future.

While the Information Technology Act, 2000, prescribes penalties for creating sexually explicit content under Section 67A, it fails to specifically address the issue of image morphing, a practice central to this case. On the other hand, the Indian Penal Code includes provisions under the Section 354 series that cover sexual harassment in both physical and digital spaces, such as sexual assault, voyeurism, stalking, online stalking, and acts that insult a woman's modesty (Section 509). However, the Penal Code lacks detailed provisions to prevent and punish the trafficking and misuse of images for sexual harassment, exposing significant gaps in the legal framework designed to address the full scope of online abuse and exploitation.

The case of Rana Ayyub in 2018 highlights significant gaps in the legal response to advanced forms of digital identity harassment. Her experience with online predators who created cloned profiles and deepfake pornography demonstrates the sophisticated and malicious tactics employed by cyber harassers. The Indian legal system's slow and ineffective response only rectified after substantial international pressure reveals a troubling disconnect between the evolving methods of cybercriminals and the outdated legal frameworks in place[37].

[35] Ayesha Bhimdiwala, Krishna Akhil Kumar Adavi & Ahmer Arif, Fighting for Their Voice: Understanding Indian Muslim Women's Responses to Networked Harassment, 8 Proc. ACM Hum.Comput. Interact. 166:1 (2024), https://dl.acm.org/doi/10.1145/3641005 (last visited Jan 6, 2025).

[36] Mayur R. Suresh, Terror Trials: Life and Law in Delhi's Courts (2023).

[37] Delhi Police To Close Case On Violent Abuse And Threats Against Rana Ayyub, HuffPost (2020), https://www.huffpost.com/archive/in/entry/delhi-police-threats-against-rana-ayyub_in_5f2d22f2c5b6b9cff7f05ba5 (last visited

This disparity emphasizes the urgent need for a more robust, adaptive legal structure capable of keeping up with the rapidly changing landscape of cybercrime. While the current laws serve as a foundation, they must be regularly reviewed and updated to address the increasingly complex and inventive nature of digital harassment.

CHALLENGES IN PROSECUTING ONLINE HARASSMENT CASE

Even with the most carefully crafted legislation, enforcing laws in a virtual environment presents unique challenges never before encountered by law enforcement agencies. These challenges are largely tied to the global nature of the internet. As a medium accessible worldwide by anyone with a computer and internet connection, the potential offender may be outside the jurisdiction where the offence occurs. The anonymity the internet offers, while beneficial in some cases, also complicates law enforcement efforts.

The internet, being borderless, opens up new opportunities for cyberstalkers. With affordable and easy access to the web, distance becomes irrelevant to a cyberstalker. Victims can be targeted in various ways-through email, instant messaging, chat rooms, social media, or even by the stalker gaining access to the victim's computer to monitor their online activities. While the internet is not a "lawless space," applying national laws, such as those against harassment and stalking, to online actions is complex and challenging, as these laws are designed for specific jurisdictions.

STRENGTHENING LEGAL FRAMEWORKS: SUGGESTIONS AND RECOMMENDATIONS

India currently lacks specific regulations to address online hate speech. While provisions in the Indian Penal Code (IPC) and the Information Technology (IT) Act offer some legal recourse, they face significant challenges. For instance, Section 153A of the IPC criminalizes promoting enmity between different groups, while Section 295A penalizes acts intended to outrage religious sentiments. However, these laws are often criticized for being vague and prone to misuse, potentially stifling legitimate free speech.[38]

Additionally, Section 66A of the IT Act, which allowed for the removal of "offensive" content, was struck down by the Supreme

Jan 7, 2025).

[38] Li-ann Thio & Jaclyn L. Neo, Religious Offences in Common Law Asia: Colonial Legacies, Constitutional Rights and Contemporary Practice (2021).

Court in 2015 for violating free speech principles.[39] In recent years, India has seen a sharp rise in online hate speech, driven by factors such as religious tensions, political polarization, and the rapid growth of social media. Acknowledging the severity of the issue, the Indian government has begun taking steps to reform its legal frameworks and address the societal impact of hate speech on social media platforms.

- ***Legal Reforms***

India's legal system has undergone significant reforms to address the growing issue of online hate speech. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, introduced by the Ministry of Electronics and Information Technology, hold social media intermediaries accountable for the content shared on their platforms. These guidelines require platforms to implement mechanisms for identifying and removing unlawful content, including hate speech, within strict timelines.

In addition to these regulations, existing laws such as the Indian Penal Code and the Code of Criminal Procedure have been amended to include provisions specifically targeting online hate speech. For example, Section 153C of the IPC criminalizes the incitement of hatred between communities based on religion, race, caste, or ethnicity, especially when such incitement leads to violence. These legal reforms reflect a concerted effort to tackle the rising threat of online hate speech in India.

- ***Social Impact on Social Media Legal Framework***

The legal reforms in India have had a significant impact on the social media legal framework, affecting both platforms and users. Social media platforms now face increased pressure to monitor and regulate content effectively. To comply with the new guidelines, many platforms have implemented automated content moderation tools and employed teams of moderators. However, this has raised concerns about censorship and the potential suppression of free speech, as platforms struggle to balance the need to curb hate speech with the protection of freedom of expression.

These legal changes have also heightened awareness among social media users regarding the consequences of engaging in

[39] Siddharth Narrain, Social Media, Violence and the Law: 'Objectionable Material' and the Changing Countours of Hate Speech Regulation in India, 10 Culture Unbound 388 (2018), https:// cultureunbound.ep.liu.se/article/view/212 (last visited Jan 6, 2025).

hate speech online. With stricter penalties in place, people are becoming more cautious about the content they share and the language they use on social media. This heightened awareness has led to some self-regulation among users, though others continue to test the limits of acceptable speech, often facing legal consequences.

Civil society organizations have played a vital role in advocating for stronger legal measures to combat online hate speech. They have called for greater transparency and accountability from social media platforms, urging them to implement robust policies to address hate speech more effectively. Civil society engagement has helped amplify the voices of marginalized communities impacted by online hate and has contributed to fostering a more inclusive discourse on social media platforms.

These legal reforms represent a significant step towards creating a safer and more inclusive online environment in India. By holding social media platforms accountable and raising awareness among users, the reforms have the potential to reduce the spread of hate speech and mitigate its harmful societal effects. However, challenges remain in striking the right balance between freedom of expression and protecting vulnerable groups from online abuse. Continued collaboration between the government, social media platforms, civil society, and users is essential to addressing these challenges and fostering a culture of respect and tolerance in the digital space.

- ***Effectiveness of Legal Framework***

Despite existing laws, enforcement has proven to be a significant challenge. Key difficulties include the complexities of identifying and defining hate speech, inadequate training for law enforcement, and limited resources to tackle the issue effectively. Furthermore, social media platforms often struggle to strike a balance between protecting freedom of expression and fulfilling their responsibility to curb harmful content. This creates a complex and evolving landscape where decisive action against hate speech remains difficult to achieve.

- ***Social Impact***

Online hate speech has a profound chilling effect, silencing marginalized voices and creating an atmosphere of fear and anxiety. It can escalate into real-world violence, as seen in several instances of mob lynchings triggered by online rumours. Social media platforms often become echo chambers, amplifying existing prejudices and deepening societal divides.

40

Despite existing legal provisions, enforcing laws against online hate speech remains a significant challenge. The sheer volume of online content and the difficulty in identifying perpetrators make it hard to take effective action. Additionally, the lack of coordination between law enforcement agencies and social media platforms further complicates the enforcement process.

Need for Transparency and Accountability: Strengthening transparency and accountability mechanisms within social media platforms is essential in the fight against online hate speech. This includes setting clearer content moderation guidelines, improving reporting systems, and ensuring swift action against violators.

CONCLUSION

Today addressing online harassment necessitates a comprehensive approach that combines legal, technological, and social strategies. By fostering collaboration between governments, tech companies, and civil society, we can create a safer, more equitable digital environment. Future research should focus on emerging threats and innovative solutions to adapt to the rapidly changing dynamics of the online world. Online harassment encompassing cyberstalking, cyberbullying, and defamation has become a critical issue in the digital age, with significant implications for individual rights, social well-being, and the rule of law. The research underscores the challenges posed by anonymity, jurisdictional complexities, and the rapid pace of technological advancement, which often outstrips the ability of legal frameworks to keep up. While existing laws provide some protection, gaps remain in enforcement, victim support, and international cooperation.

The study highlighted the need for a multifaceted strategy to address these challenges effectively. Strengthening legal frameworks at both national and international levels is essential for ensuring justice for victims and holding offenders accountable. Technological solutions, such as Al-driven content moderation, must be developed and deployed ethically to complement legal efforts. Social interventions, including public awareness campaigns and victim support systems, are also vital for addressing the psychological and societal impact of online harassment. Furthermore, it is crucial to strike a balance between

[40] Ritika Singh et al., "Online Hate Speech in India: Legal Reforms and Social Impact on Social Media Platforms," (2024), https://papers.ssrn.com/abstract=4732818 (last visited Jan 6, 2025).

protecting freedom of expression and ensuring digital safety, to avoid overregulation or censorship. International cooperation is key to tackling cross-border issues and harmonizing legal responses in the global digital landscape.