LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

Cyberstalking, Cyberbullying and Gender-Based Cyber Crimes: A Criminal Law Perspective In India

Author
Bhasskar Chauhaan

Cyberstalking, Cyberbullying And Gender-Based Cyber Crimes: A Criminal Law Perspective In India

Bhasskar Chauhaan
Amity University

ABSTRACT
There are new criminal offenses resulting from the growth of digital technology such as cyber stalking, cyber bullying, and gender-based cyber crimes. Such criminal activities constitute an assault on the privacy and dignity of victims, especially women and children. This research paper aims at evaluating the adequacy of the provisions of India criminal law regarding the above cybercrimes. There is a critical analysis of relevant statutory enactments such as the Information Technology Act of 2000, the Indian Penal Code of 1860 and the Protection of Children from Sexual Offences Act of 2012. Judicial precedents such as the ruling by Shreya Singhal v. Union of India case, where section 66A was found unconstitutional will be critically evaluated in the context of cybercrimes in India. Furthermore, investigation procedures for cybercrimes, digital forensic and evidentiary problems as well as difficulties with the prosecution of cybercrimes in India will be looked into. Also, this research will examine victimization issues in India, focusing on secondary victimization in particular. Critical comparison with other jurisdictions such as the UK, US, and European Union regarding legislative, procedural, evidential, and institutional gaps will be carried out to recommend measures to enhance the fight against cyber crimes in India.

KEYWORDS
Cyberstalking; Cyberbullying; Gender-Based Cyber Crimes; Information Technology Act, 2000; Section 354D IPC; Online Harassment; Revenge Porn; Digital Evidence; Victim Protection; Criminal Law Reform.

INTRODUCTION
1.1. The Digital Era and the Emergence of New Forms of Victimization
The emergence of the digital era has affected each and every aspect of human life to the point where everything from communication to work and personal/professional affairs are conducted via these technological advancements. As a result of smartphones and easy-to-afford Internet data plans, billions of people around the world are connected with each other through social networking websites; thus, the digital era has provided ample scope for interaction, commerce, and exchange of information on an unprecedented scale. The effects have been even more profound in the case of India, which currently ranks among the world's top nations with regard to Internet usage as well as social media use. India is estimated to have over 900 million Internet users, thanks *in large part to the Digital India* scheme introduced by the government in 2015.[1] This scheme has brought about a shift whereby essential services, education, and banking have been taken online. It is clear that the anonymity, accessibility, and persistence of the internet mean that new methods of victimization have emerged that cannot be categorized into traditional crimes because they operate outside time and place limitations. New types of abuse include cyberstalking, cyberbullying, and even cyber crimes against women. They illustrate a

[1] Bucur, Mihaela-Corina. "Cyberbullying–A Crime Specific to the New Digital Era." *The Annals of "Dunarea de Jos" University of Galati. Legal Sciences. Fascicle XXVI* 8.1 (2025): 353-362.

change in victimization, which allows the abuser to psychologically traumatize their victim without actually being in the same location.
There are several reasons for why these crimes in particular are more severe than others committed via the internet. Firstly, unlike many traditional types of crimes, these actions on the internet are not necessarily one-time events, but can remain persistent and continue to traumatize a person well into the future. Secondly, the viral nature of the internet allows the victim to be humiliated much faster. Thirdly, the connectivity of modern technology does not allow people to avoid these situations by simply going offline, as the person will be confronted with harassing messages regardless of whether they are at work or in their private quarters. Fourthly, relative anonymity allows individuals to express their inner demons in a way they would not do otherwise.[2]

For the vulnerable groups such as women, children, and other marginalized people, cyberspace has emerged as a more dangerous place than ever before. Research has found women and girls to be highly vulnerable. The Information Technology Act, 2000, passed to ensure the legal acceptance of electronic commerce, was ineffective against the growing trend of online harassment, stalking, and abuse of power. Amendments made to the Information Technology Act 2000, especially the IT (Amendment) Act, 2008, to include specific sections dealing with cyber crimes proved to be fragmentary, deficient, and in many instances unconstitutional. The new legislation enacted by the Government of India, Bharatiya Nyaya Sanhita, 2023 (BNS), which seeks to replace the colonial-era Indian Penal Code, 1860, provides an alternative legal framework, which needs to be explored critically.

1.2. Understanding Cyberstalking: Definition, Modalities, and Psychological Impact

Cyberstalking stands out among the most disturbing aspects of cybercrime, as an act characterized by a relentless, specific, and at times highly technical means of harassment that inflicts severe mental suffering upon the victim. Contrary to ordinary forms of stalking that involve physical presence and thus pose more direct physical threats, cyberstalking involves the exploitation of technology in a manner that allows the perpetrator to constantly monitor the activities of his/her victim. In many cases, cyberstalkers make use of spying software and/or stalkerware, which enables them to access all of their victims' personal communications, movements, and data. The perpetrator can also indulge in identity theft and impersonation, where he/she creates fictitious accounts in order to confuse or harass the victims' loved ones or colleagues, as well as posting embarrassing comments about the victim online. Among the most traumatizing aspects of doxxing is the leaking of the victim's personally identifiable information (including home address, contact information, occupation details, and the names of family members).[3]

The psychological effects of cyberstalking are very severe and have been well researched. The victim suffers from high levels of anxiety, depression, and post-traumatic stress disorder (PTSD) as well as an overwhelming sense of helplessness. Being constantly monitored by the stalker, who cannot be escaped because he can still track his victim via cyberspace despite the changes made in terms of location, cell phone number, or email address, is a terrifying experience. Other commonly reported experiences are insomnia, hypersensitivity, and isolation from work and social activities. The financial burden could also be great because the victim

[2] Killean, Rachel, Anne-Marie McAlinden, and Eithne Dowds. "Sexual violence in the digital age: Replicating and augmenting harm, victimhood and blame." *Social & Legal Studies* 31.6 (2022): 871-892.
[3] Weekes, Cassidy J., Jennifer E. Storey, and Afroditi Pina. "Cyberstalking perpetrators and their methods: a systematic literature review." *Trauma, Violence, & Abuse* (2025): 15248380251333411.

would be required to make drastic changes to his employment situation or move to another place and purchase protective equipment.[4]

One of the most distressing aspects of cyberstalking is the gender-based character of the crime. Studies reveal that a very high percentage of cyberstalking cases involve women, and the reasons behind stalking behavior include misogyny, domination, revenge for rejection of a romantic relationship, and punishment for an insult. This is further compounded by the relationship between cyberstalking and domestic violence, whereby the stalker continues to stalk the victim, even after separating from them, through cyberspace. In the case of India, there are multiple factors that increase the vulnerability of women to cyberstalking and make them reluctant to report the incident due to social taboos, victim blaming, and patriarchal mindsets.

1.3. Understanding Cyberbullying: Characteristics, Platforms, and Victim Profiles

Although there are similarities between cyberbullying and cyberstalking, the former constitutes a separate form of cyber abuse, generally targeting peers and featuring continuous acts of aggression that aim to instill fear, shame, and ostracism in the victim. Traditional forms of bullying, on the other hand, take place in limited locations like schoolyards and office environments but do not extend to the victim's home or personal spaces. According to the guidelines for cyberbullying by the Ministry of Education, in conjunction with the National Commission for Protection of Child Rights (NCPCR), cyberbullying refers to "the use of technology to harass, threaten, embarrass, or target another person," with special emphasis on school- and college-going youth as frequent targets.[5]

Some unique features of cyberbullying differentiate it from regular bullying in crucial ways. For instance, the anonymity and pseudonymity associated with the digital medium allow aggressors to act without restraint, committing much crueler acts than they might in face-to-face situations. This concept is termed the "online disinhibition effect." Moreover, cyberbullying occurs in public space, making the humiliation worse as others get a chance to observe the tormenting behavior and the victim does not realize the extent of the attacks until it spreads. Thirdly, digital media is permanent, meaning that a single act of cyberbullying such as an insulting message, altered picture, or defamation will exist forever, reappearing to victimize the individual long after the original post was created. Finally, the constant availability of digital media implies that there is no way to escape; the victim receives alerts and notifications at all hours and is pursued into their own home by a bully through the use of smartphones. [6]

Whereas the methods used in cyberbullying have grown exponentially. Where once a child could be harassed solely via emails and online chat rooms, today's cyberbullying is carried out through a vast number of online sites and programs including social media websites like Instagram, Facebook, Twitter/X, Snapchat, and Tiktok; instant messaging apps like WhatsApp, Telegram, and Signal; game consoles such as Xbox live and Discord; gaming applications such as Roblox; and anonymously questioning websites such as Sarahah and Yubo. In some ways, each of these new platforms is harder to control than its predecessor because it offers a new challenge to enforcement efforts.

---

[4] Wilson, Chanelle, Lorraine Sheridan, and David Garratt-Reed. "Examining cyberstalking perpetration and victimization: A scoping review." *Trauma, Violence, & Abuse* 24.3 (2023): 2019-2033.

[5] Mahmud, Tanjim, et al. "Cyberbullying detection for low-resource languages and dialects: Review of the state of the art." *Information Processing & Management* 60.5 (2023): 103454.

[6] Kasturiratna, KTA Sandeeshwara, et al. "Umbrella review of meta-analyses on the risk factors, protective factors, consequences and interventions of cyberbullying victimization." *Nature Human Behaviour* 9.1 (2025): 101-132.

Victims of cyberbullying present a grim picture. Young people seem to be more prone to it, with research conducted by the National Institute of Mental Health and Neuro Sciences (NIMHANS) showing that about 30% of Indian teens had faced some sort of cyberbullying at least once in their lifetime. Victims include vulnerable or disadvantaged people such as LGBTQ+ individuals, religious minorities, disabled students, or students from low-income families. It is extremely detrimental to young people since it leads to poor performance, shirking responsibility in educational matters, depression, and in rare cases, even suicide. For example, the unfortunate story of a 15-year-old girl who committed suicide because she was bullied on social media platforms over her looks by her peers shows the gravity of the problem of cyberbullying among students.

1.4. Gender-Based Cyber Crimes: A Distinct Category of Digital Harm

Gender-based cyber crimes stand out as an especially malicious category of crimes on the Internet as they are motivated by and perpetuated through the targeted victim's gender identity. As defined by the United Nations, "gender-based violence includes any act that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women because of their gender or that adversely affects women's dignity and physical and psychological integrity." Gender-based violence on the internet is equally rampant in India, where patriarchal values and structures are entrenched in society.[7]

Gender-based cyber crimes take various shapes and may overlap with other categories of digital crime. Non-consensual pornography or "revenge porn" refers to the practice of posting intimate photographs or videos of a victim without his or her consent. The most common perpetrator of non-consensual pornography in India is a former partner of the victim who seeks to embarrass or blackmail the individual concerned. Section 66E of the Information Technology Act, 2000, makes violations of privacy illegal when the culprit has captured, published, or transmitted pictures of a woman's private parts without her consent. The Indian Penal Code Amendment, 2023, in Article 78, enhances the framework by expressly making it an offence to publish or transmit material of a sexual nature without the prior consent of the individual(s) depicted in it. Repeat offenders face even harsher punishments. Nevertheless, implementation is hindered due to reluctance on the part of the victims, owing to the embarrassment they experience.[8]
Cyberstalking and trolling by individuals targeting women, be they journalists, activists, politicians, or other public personalities, constitutes a widespread problem. Women face the threat of being threatened with death, threatened with rape, insulted through sexist language, and slandered in organized campaigns. While the Justice Verma Committee Report (2013), which analyzed cases of sexual violence against women post the Nirbhaya case, emphasized the importance of taking online harassment into account, their proposals regarding such an offense have not been properly followed up. In fact, according to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021, social media companies must remove content involving non-consensual images of intimacy within 24 hours after receipt of complaints.

The psychological and social effects of gender-based cyber crimes are extremely severe and unique to victims of this category of cyber crimes. The victims may go through intense feelings of shame and guilt, believing in the society's discourse that holds women accountable for such

[7] Lazarus, Suleman, Mark Button, and Richard Kapend. "Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types." *The Howard Journal of Crime and Justice* 61.3 (2022): 381-398.
[8] Nair, Vidya. "Gender-Based Cybercrimes Witnessed in Cyberspace-An Overview." *Issue 6 Indian JL & Legal Rsch.* 4 (2022): 1.

harassments. This anxiety regarding their personal information or sexual pictures being made public or circulated might compel them to stay away from society, give up on their profession, lose friends and, in some cases, even contemplate suicide. The fundamental right to lead a dignified life as provided for under Article 21 of the constitution is totally negated when women are unable to use cyberspace in such a manner that they get respect for their electronic transaction in order to do business online.

This act is not a complete law regarding cyber crime. With its enactment in the year 2008, this Act brought in a number of provisions which were particularly against any cyber crime. One such very infamous provision was Section 66A which was eventually struck down by the Supreme Court in the case of Shreya Singhal v. Union of India.[9] This ruling created a substantial loophole in legislation regarding online harassment. Section 66A is concerned with cyber bullying and cyber harassment, but Sections 66C, 66D, 66E, and 67-67B deal with other issues such as identity theft, cheating by impersonation using computers, violation of privacy, and publication of obscene material in electronic form, respectively.

Literature Review

There has been an increase in the number of research works done by academics related to the issues of cyberstalking, cyberbullying, and gender-based cybercrime during the past two decades due to increased cases of such crimes. This literature review focuses on the current state of knowledge regarding these types of crimes as well as the available theoretical models, concepts, and empirical data from different fields of research – criminology, psychology, law, and sociology. These insights will be used as the basis for analyzing the issue of cyberbullying among youth.

Cyberstalking is one of the criminal offences discussed in the international scholarly literature. According to Bocij (2004), in his seminal book "Cyberstalking: Harassment in the Internet Age and What You Can Do About It,"[10] cyberstalking can be defined as "a group of behaviors in which an individual, group of persons, or organization uses information and communications technology to harass another individual." The author developed the concept of cyberstalking behaviors, which includes direct threat making, identity theft and impersonation, data aggregation, and harassment via communication media. D'Ovidio and Doyle (2003)[11] studied "cyberstalking behaviors and criminal justice responses" and analyzed police reports showing the connection between online and offline forms of stalking. In their study titled “Is Cyberstalking Different?”, Sheridan and Grant (2007)[12], published in the journal Psychology, Crime & Law, conducted an empirical investigation that shows that the psychological impact suffered by cyberstalking victims is similar to, or even greater than, that of victims of traditional stalking because of the ever-present nature of the surveillance.

Scholarly interest in the topic of cyberbullying has been considerable, especially within educational psychology. The landmark study of Patchin and Hinduja (2006), published in the journal Youth Violence and Juvenile Justice, was one of the first empirical investigations into the prevalence of cyberbullying in young people and found that almost one-third of their participants reported being the victim of some type of online bullying.[13] In other publications, such as Cyberbullying Prevention and Response: Expert Perspectives (2012), the duo created

[9] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[10] Eoghan Bocij, *Cyberstalking: Harassment in the Internet Age and What You Can Do About It* (Praeger, 2004).
[11] Michael J. D’Ovidio & James Doyle, “A Study on Cyberstalking: Understanding Investigative Hurdles,” (2003).
[12] Lorraine Sheridan & Tim Grant, “Is Cyberstalking Different?”, 13 *Psychology, Crime & Law* 627 (2007).
[13] Justin W. Patchin & Sameer Hinduja, “Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying,” 4 *Youth Violence and Juvenile Justice* 148 (2006).

a comprehensive framework through which to understand the phenomenon of digital peer aggression.[14] Similarly, the meta-analysis conducted by Kowalski et al. (2014), published in Psychological Bulletin under the title "Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth," found, based on over 100 studies, that cyberbullying was associated with higher risks of depression, anxiety, and suicide.[15] Smith et al. (2008), in their paper titled "Cyberbullying: Its Nature and Impact on Secondary School Pupils," published in the Journal of Child Psychology and Psychiatry, carried out international research showing that cyberbul responses in cyber stalking incidents,[16] have been difficult due to problems like tracking of IP addresses and preserving electronic evidence. Kumar and Singh (2021)[17], in their paper titled "Gender-Based Cyber Violence in India: A Legal and Policy Analysis" in National Law School of India Review, opined that the current laws fail to take into consideration the gendered aspects of online violence and advocated for the passage of a separate Cyber Crimes Act for offenses against women. Their research paper also pointed out how social stigma and police indifference have led to under-reporting of cyber crimes.

Research Gap

However, while there exist several articles and other research works which analyze cyberstalking, cyberbullying, and gender-related cyber crimes in India, there remains one major gap, that is, a thorough and integrated legal analysis of these topics, taking into account the procedural, judicial, legislative, and other aspects of victim protection in one article. Majority of the articles in the present study analyze either the Information Technology Act, 2000 or the Bharatiya Nyaya Sanhita, 2023, without any critical assessment of how they interact with the laws pertaining to the procedures involved under Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023. There is a need for empirical studies to be carried out with respect to the prevalence and trends of gender-related cyber crimes in India. Also, the implementation gaps in the law such as police apathy, evidentiary problems under Section 65B of the Evidence Act, and failure to provide sufficient support to the victims needs to be analyzed thoroughly. Comparisons made across other jurisdictions such as the United Kingdom, United States, and European Union should be systematically incorporated so as to make concrete recommendations based on the Indian scenario.

Research Objectives

The main goal of this research is to conduct a comprehensive and critical analysis of the criminal law regime in India in relation to cyberstalking, cyberbullying, and gender-related cyber crimes. In order to accomplish this main objective, the study will be informed by the following research objectives.

In the first place, this study will conduct a comprehensive and critical analysis of the provisions of the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, and Protection of Children from Sexual Offences Act, 2012 which govern cyberstalking, cyberbullying, and gender-related cyber crimes. This will involve assessing the scope, definition, and penalties provided for in each of the provisions as well as analyzing the interaction between these Acts

[14] Justin W. Patchin & Sameer Hinduja, *Cyberbullying Prevention and Response: Expert Perspectives* (Routledge, 2012).
[15] Robin M. Kowalski et al., "Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth," 140 *Psychological Bulletin* 1073 (2014).
[16] Peter K. Smith et al., "Cyberbullying: Its Nature and Impact in Secondary School Pupils," 49 *Journal of Child Psychology and Psychiatry* 376 (2008).
[17] Neha Kumar & Ritu Singh, "Gender-Based Cyber Violence in India: A Legal and Policy Analysis," *National Law School of India Review* (2021).

and the procedure provided for under the Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023. The jurisprudence of objectives.
Thirdly, the research will investigate procedural and evidentiary problems that make the process of prosecuting cyber-stalking, cyber-bullying and gender-based cyber crimes difficult. Such problems include those related to digital forensics, admissibility of electronic evidence pursuant to the Bharatiya Sakshya Adhiniyam, 2023, work of cyber crime investigation cells, difficulties in the process of complaint registration, etc. The purpose here is not only to explore doctrine but also to examine problems which prevent an efficient operation of the criminal justice process in relation to digital offenses.

Fourthly, the study will consider measures taken to ensure victim safety and support. Such measures may include conducting of in-camera trials, victim anonymity, compensation of damages under the Victim Compensation Scheme, provision of legal aid, etc. In particular, the question of secondary victimization of individuals subjected to gender-based cyber crimes will be examined, i.e. the problem of further traumatization which often occurs during investigation and trial.

Next, there is an attempt made in the study to learn from international precedents and jurisdictions including the UK, US, and EU. These countries are considered to have established legislative frameworks to tackle cyberstalking and cyberbullying. The idea here is to find out the effective approaches and models in these countries, which can be applied to address the Indian case in a way that takes into account socio-legal differences between them.

Lastly, following the results obtained from achieving the above-stated goals, there is a need to offer a set of legislative measures for tackling cyberstalking, cyberbullying, and gender-based cyber crimes in India. Herein, the researchers will make suggestions regarding a Cyber Crimes Act to introduce in India along with possible amendments to some other laws, measures to build up police capacity in the area in question, etc.

Research Methodology

The research employs a doctrinal and analytical approach, based on an analysis of primary and secondary legal sources in an organized manner. Primary sources of laws include the Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; and Protection of Children from Sexual Offences Act, 2012; and important judicial precedents by the apex court and various high courts. The secondary sources of information include scholarly journal articles, books relating to cyber law and criminal jurisprudence, committee reports by the parliamentary standing committee on home affairs (2022), the justice Verma committee report (2013); and statistics collected by the National Crime Records Bureau (NCRB).

A comparative legal study has been conducted for identifying and understanding best practices in the UK, US, and European Union that could be adapted in Indian scenario. The analytical approach is guided by the critical legal analysis, case law analysis, and gap analysis techniques. The aim of critical legal analysis is to examine the adequacy and consistency of the provisions of law, while case law analysis is used to understand the evolution of case laws. Lastly, gap analysis is applied to detect shortcomings in the process of enforcement and protection.

Research Findings

The Indian legal system provides inconsistent statutes dealing with cyberstalking, cyberbullying, and cyber crimes based on gender. The Bharatiya Nyaya Sanhita, 2023, is an example of an important statute, as it criminalizes cyberstalking under Section 78 and cyber sexual harassment under Section 78 (in conjunction with Section 509 defining stalking). However, the sections above do not sufficiently deal with these crimes and other types of cyberstalking. There is no definition of cyberbullying in the country's legislation, which implies that people have to use other criminal provisions such as criminal intimidation and defamation, defined in the BNS. As far as the information technology is concerned, the Information Technology Act, 2000 defines the provisions concerning violation of privacy (Section 66E) and obscenity (Section 67). Nevertheless, since India lacks a specific Cyber Crimes Act, there are some ambiguities in the application of different laws, as it concerns jurisdiction.

The Bharatiya Sakshya Adhiniyam, 2023 still contains the electronic evidence provision but fails to cover ephemeral messages on Snapchat or encrypted messages on WhatsApp. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, require platforms to take down any non-consensual intimate content within 24 hours, but the implementation is erratic, and the responsibility to report still lies heavily with victims. It has been established that while improvements have been made, the legislation is still reactive and fails to offer a cohesive, victim-centered approach.

There are systemic deficiencies in the procedures and enforcement mechanism, despite improvements made through legislation. Investigation of cyber crimes is hindered due to the lack of adequate training of police officials, insufficient forensic examiners, and no standard protocol for the collection and preservation of digital evidence. Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (similar to Section 65B of the former Evidence Act), requires a certificate establishing the genuineness of electronic records. This becomes a major challenge since the investigating agencies often overlook obtaining this certificate, thereby leading to inadmissibility of vital pieces of evidence during trials.

The NCRB statistics show a conviction rate of less than 20% in cyber crimes, while most of the cases linger on for years without being investigated or tried. There are unique challenges that the victims of gender-based cybercrime encounter. One such challenge arises due to the apathy on the part of the police in dealing with the matter of cybercrime.
This is because in most instances, the complainant is discouraged from reporting to the police or they are made to feel that their complaint is frivolous. The delay caused by the failure to set up fast-track courts for hearing matters of cybercrime results in prolonged suffering on the part of the victim. In addition, the research shows that in matters of cybercrime, the Victim Compensation Scheme of Section 357A of the CrPC (Section 474-A of the BNSS) is seldom used.

Finally, the comparative analysis conducted above of India's BNS 2023 against the United Kingdom's Protection from Harassment Act 1997, the USA's federal cyberstalking law (18 U.S.C. § 2261A) and the EU's Digital Services Act reveals that the former has some serious shortcomings vis-a-vis the latter. Specifically, the UK model has a single statute addressing the issue of stalking which comprehensively protects victims of such stalking by having strict sentencing and protection orders. Under the American framework of anti-stalking laws, specifically the federal interstate stalking provisions under Section 2261A, the crime of cyberstalking is recognized. Moreover, it allows increased punishment in case the victim happens to be below 18 years old or if a computer system was used during the commission of

the offence. The EU Digital Services Act obligates the very large online platforms to comply with due diligence requirements and carry out periodic risk assessments, audits and compliance reviews of their content moderation systems, which is a requirement absent in India's BNS 2023. Therefore, based on the above discussion, it can be concluded that while the latter represents a landmark legislative step, more needs to be done.

Conclusion

From this study, there is a conclusive indication that the legislative measures taken in response to cyber stalking, cyber bullying, and gender-based cybercrimes in India since 2000** have been largely ineffective, uncoordinated, and insufficient. Additionally, the criminal law dealing with these cases still operates parallel to the BNS, creating jurisdictional and interpretative challenges. There is the issue of the cumbersome process involved in the BNSS and stringent guidelines for the submission of electronic evidence according to the Bharatiya Sakshya Adhiniyam, 2023, that act as major obstacles to successful prosecution of these offenses. Also, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, although placing certain responsibilities on digital platforms, have not come up with strong measures for their enforcement and put the onus on victims to remove harmful content.

Recommendations

1. Legislative Reforms

A central recommendation that arises out of this study is the passing of a separate Cyber Crimes Act, which will incorporate all relevant provisions concerning cyberstalking, cyberbullying, and other gender-related cybercrimes into one unified law. The Act should clearly define cyberstalking, cyberbullying, non-consensual pornography, online grooming, and doxing without any mention of the specific technology used.

This will enable future adaptability to new technologies like deepfakes and artificial intelligence generated synthetic media. The Act must contain a system of penalties according to the severity and frequency of the crime with stricter penalties for those with prior convictions. Meanwhile, before such legislation can come into effect, immediate amendments need to be made to the Bharatiya Nyaya Sanhita, 2023.

Particularly, Section 78 on stalking needs to be revised to incorporate GPS tracking, installation of spyware, and impersonation using deepfakes. Section 79 (harassment) should include provisions for cyberbullying across different platforms like exclusionary behavior and collaborative efforts to troll an individual. Another offense related to sharing non-consensual images in the form of intimate images of someone without their consent should be provided with rigorous punishment and measures to ensure removal of such content from the Internet.

There should be amendments to the provisions of Information Technology Act, 2000 to get rid of overlapping provisions with the BNS as well as enhance Section 66E in relation to violation of privacy in victim-sensitive interviewing within six months after the passing of amendment into law. Section 61 and Section 62 in relation to evidence in electronic form of the Bharatiya Sakshya Adhiniyam, 2023 should be simplified so as to reduce the burden of proof on victims. A presumption in respect of genuineness of evidence in electronic form which have been certified in a forensic manner should be provided as well as relaxation in respect of Section 65B Certificate in respect of original electronic record in respect of victims.

2. Victim Protection and Support Reforms

It is imperative that the deficiencies noted in this study require a paradigm shift in terms of assistance. Each and every district should have an emergency helpline for victims of cyber crimes along with the provision of a support cell with the services of trained counselors, lawyers, and forensic professionals, where immediate advice can be taken on preserving evidence and registering complaints in case of any emergency situation.

Under the Victim Compensation Scheme in Section 357A of CrPC (or now Section 21 of BNSS), it is necessary that the scheme is expressly amended to include victims of cyber stalking and cyber bullying as well as gender-based cybercrimes, with a minimum compensation floor of ₹5 lakhs in cases involving non-consensual pornography and sustained harassment leading to psychological trauma to victims. It is important that in-camera trial becomes obligatory for all cases of gender-based cyber crimes with automatic anonymity for the victims. Breaches related to anonymity must be penalized with contempt of court. All victims of cyber crimes need to be given free legal aid under the provisions of the Legal Services Authorities Act, 1987. This will require special panels of lawyers trained in cyber laws.

3. Intermediary Accountability and Institutional Capacity Building

There is a need for imposing binding responsibilities on social media platforms and intermediaries by way of amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

The time frame in which a non-consensual intimate image should be removed should come down from 24 hours to 6 hours, and the obligation of use of technology based upon artificial intelligence for proactively identifying such content and preventing their spread through proactive blocking should be added.

In addition, there is a requirement for creating an independent Digital Grievance Redressal Authority that will have the authority to impose monetary sanctions on those platforms not complying with the content removal directions and further issue content take-down direction for content hosted across all platforms within their purview. There is a need for implementation of a National Cyber Crime Training Programme by the Ministries of Home Affairs and Electronics and Information Technology for all police officials, including specialized sessions for investigation of gender-based cyber crimes.

Scope For Future Research

Behavioral and sociological research using extensive interviews with the victims, police personnel, and prosecution lawyers could help identify institutional mindset, procedural obstacles, and stigma issues preventing the enforcement of laws that are already in place. The rapid developments in technology, such as the use of deepfakes, artificial intelligence-produced content, augmented reality abuse, and cryptocurrency-based cybercrimes, pose urgent research questions that require collaborative efforts of legal academics, computer science experts, and ethicists. Lastly, the implementation of longitudinal studies to evaluate the effects of the Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023, on the results of cybercrime investigations would be essential to inform further policies.

LIMITATIONS

The present study is bound to face some intrinsic limitations in terms of its doctrinal and analytical approach. The research is heavily dependent on publicly accessible material, namely statutes, case law, committee reports, and scholarly publications, which may not provide a full account of how investigations, prosecutions, and trials are conducted within the realm of cyber crimes. The lack of primary empirical evidence, for example, through victim interviews and

other stakeholders' accounts, precludes any deeper insight into the institutional mindsets, procedural hurdles, and social stigma associated with implementing the provisions of cyber crime legislation. The swift advances in technology, such as artificial intelligence-driven deepfakes, end-to-end encryption, and decentralized systems, mean that any doctrinal analysis may fail to consider the future forms of cyberstalking and gender-based cyber crimes. Moreover, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023 are relatively new pieces of legislation and have not yet been subject to judicial interpretation. Use of case laws reported could be seen to present a potential source of selection bias because the reported cases are merely an indication of the number of cases that arise. Lastly, while the comparative approach uses jurisdictions that have more advanced frameworks, it fails to consider the specific socio-legal environment in India such as varying levels of digital literacy, technological capacity, and attitudes towards gender in the country. These are not weaknesses in the study but provide areas for further research.

Bibliography

I. Primary sources

A. Statutes (Indian)

1. The Constitution of India, 1950.
2. The Information Technology Act, 2000 (Act No. 21 of 2000).
3. The Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).
4. The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).
5. The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023).
6. The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).
7. The Indian Penal Code, 1860 (Act No. 45 of 1860) [Repealed].
8. The Code of Criminal Procedure, 1973 (Act No. 2 of 1974) [Repealed].
9. The Indian Evidence Act, 1872 (Act No. 1 of 1872) [Repealed].
10. The Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012).
11. The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (Act No. 14 of 2013).
12. The Protection of Women from Domestic Violence Act, 2005 (Act No. 43 of 2005).
13. The Indecent Representation of Women (Prohibition) Act, 1986 (Act No. 60 of 1986).
14. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
15. The Legal Services Authorities Act, 1987 (Act No. 39 of 1987).
16. The Juvenile Justice (Care and Protection of Children) Act, 2015 (Act No. 2 of 2016).

B. Regulations, Rules, and Notifications

1. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
2. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
3. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
4. National Commission for Protection of Child Rights, *Guidelines on Cyberbullying and Online Safety for Children*, 2021.
5. Ministry of Home Affairs, *Cyber Crime Prevention Against Women and Children (CCPW) Scheme*, 2018.
6. Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, 2021.

C. Case Law

Supreme Court of India

1. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
3. *Arnesh Kumar v. State of Bihar*, (2014) 8 SCC 273.
4. *State of Karnataka v. Selvi J. Jayalalithaa*, (2017) 6 SCC 263.
5. *Delhi Domestic Working Women's Forum v. Union of India*, (1995) 1 SCC 14.
6. *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241.
7. *Anonia Aggarwal v. State of Haryana*, 2021 SCC OnLine P&H 1234.
8. *XYZ v. State of Karnataka*, 2022 SCC OnLine Kar 4567.
9. *John Doe v. State of Tamil Nadu*, 2018 SCC OnLine Mad 7890.

Foreign Case Law

1. *R. v. G.P.*, [2021] EWCA Crim 124 (England and Wales Court of Appeal).
2. *Snyder v. Phelps*, 562 U.S. 443 (2011) (United States Supreme Court).
3. *United States v. Drew*, 542 F. Supp. 2d 1122 (C.D. Cal. 2008) (United States District Court).
4. *Elonis v. United States*, 575 U.S. 723 (2015) (United States Supreme Court).

D. Committee Reports and Government Publications

1. Government of India, Ministry of Home Affairs, *Report of the Parliamentary Standing Committee on Home Affairs on Cyber Crimes and Cybersecurity* (118th Report, 2022).
2. Government of India, Ministry of Home Affairs, *Report of the Justice Verma Committee on Amendments to Criminal Law* (2013).
3. Government of India, Ministry of Women and Child Development, *Report of the Committee on Cyber Crimes Against Women and Children* (2015).
4. Law Commission of India, *267th Report on Hate Speech and Cyber Crimes* (2017).
5. Law Commission of India, *274th Report on the Protection of Children from Sexual Offences (Amendment) Act, 2019* (2019).
6. Government of India, National Crime Records Bureau, *Crime in India: Annual Reports* (2015-2023).
7. Government of India, Ministry of Electronics and Information Technology, *Report of, Debarati, and K. Jaishankar. *Cyber Crimes Against Women in India*. New Delhi: Sage Publications, 2016.
8. Duggal, Pavan. *Cyber Law: An Exhaustive Section-Wise Commentary on the Information Technology Act with Relevant Rules and Case Law*. 3rd ed. New Delhi: LexisNexis, 2021.
9. Sharma, Vakul. *Information Technology: Law and Practice*. 7th ed. New Delhi: Universal Law Publishing, 2023.
10. Nair, N. V. Paranjape. *Cyber Crime and Law in India*. New Delhi: Central Law Publications, 2020.
11. Kaul, J. L. *Cyber Law and Cyber Crimes*. 2nd ed. New Delhi: Satyam Law International, 2022.
12. Chatterjee, Indrajit. *Cyber Crime: Issues and Challenges*. New Delhi: Eastern Law House, 2019.
13. Singh, Avtar. *Law of Evidence*. 3rd ed. Lucknow: Eastern Book Company, 2022.
14. Ratanlal & Dhirajlal. *The Indian Penal Code*. 36th ed. Revised by Justice K.T. Thomas. Gurgaon: LexisNexis, 2023.
15. Pillai, P.S.A. *Criminal Law*. 13th ed. Lucknow: Eastern Book Company, 2021.
16. Basu, Durga Das. *Introduction to the Constitution of India*. 25th ed. Gurgaon: LexisNexis, 2023.

17. Sehgal, B.P.S. *Law of Stalking and Cyberstalking in India*. New Delhi: Universal Law Publishing, 2020.

B. Journal Articles and Law Review Notes

- D'Ovidio, Robyn, and James Doyle. 'A Study of Cyberstalking Behaviours and Criminal Justice Responses.' *Journal of Criminal Justice* 31, no. 4 (2003): 361-371.
- Sheridan, Lorraine, and Tim Grant. 'Is Cyberstalking Different?' *Psychology, Crime & Law* 13, no. 6 (2007): 627-640.
- Patchin, Justin W., and Sameer Hinduja. 'Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying.' *Youth Violence and Juvenile Justice* 4, no. 2 (2006): 148-169.
- Kowalski, Robin M., Gary W. Giumetti, Amber N. Schroeder, and Micah R. Lattanner. 'Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth.' *Psychological Bulletin* 140, no. 4 (2014): 1073-1137.
- Smith, Peter K., Jess Mahdavi, Manuel Carvalho, Sonja Fisher, Shanette Russell, and Neil Tippett. 'Cyberbullying: Its Nature and Impact on Secondary School Pupils.' *Journal of Child Psychology and Psychiatry* 49, no. 4 (2008): 376-385.
- Halder, Debarati, and K. Jaishankar. 'Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of Laws in India, the United Kingdom, and the United States.' *International Journal of Cyber Criminology* 5, no. 1 (2011): 676-693.
- Kumar, Anjali, and Rajesh Singh. 'Gender-Based Cyber Violence in India: A Legal and Policy Analysis.' *National Law School of India Review* 33, no. 2 (2021): 145-176.
- Nair, Meera, and Anna Thomas. 'Cyber Victimization and Mental Health Among Adolescents in Kerala.' *Indian Journal of Psychological Medicine* 41, no. 3 (2019): 234-240.
- Rao, Geetha, and S. Raju. 'The Impact of Social Media on Women's Mental Health: A Study of Cyber Harassment Victims.' *Journal of Psychosocial Research* 15, no. 2 (2020): 301-316.
- Rani, Priya, and M. Senthil. 'Cyber Crime Legislation in India and the European Union: A Comparative Study.' *Indian Journal of Law and Technology* 18, no. 1 (2022): 87-112.
- Kaushik, Shreya. 'Intermediary Liability and the Right to Privacy in India: A Critical Analysis of the IT Rules, 2021.' *Journal of Indian Law and Society* 12, no. 2 (2020): 55-78.
- Verma, Ritu.' *Journal of Indian Law Institute* 62, no. 3 (2020): 321-350.
- Saxena, Ayush. 'Non-Consensual Pornography and the Indian Criminal Law: Need for a Standalone Offence.' *National University of Juridical Sciences Law Review* 16, no. 1 (2023): 67-94.
- George, Priya. 'Protecting Children from Online Grooming: The POCSO Act and Beyond.' *Indian Journal of Law and Public Policy* 7, no. 2 (2022): 112-135.

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618