LEGAL ASPECT OF CYBER CRIME IN INDIA: AN ANALYSIS

Saumya Shil, Research Scholar; Faculty of Law; Deen Dayal Upadhyaya University; Gorakhpur
Dr. TN Mishra, Assistant Professor; Faculty of Law; Deen Dayal Upadhyaya University Gorakhpur

ABSTRACT

The swift proliferation of digital communication technologies has transformed cyberbullying into a significant socio-legal challenge in India. The increasing use of social media platforms, instant messaging applications, and online communities has contributed to the growing incidence of digital harassment, identity fraud, defamation, cyberstalking, online intimidation, and the unauthorized dissemination of private or intimate images. Although Indian law does not recognize cyberbullying as a distinct and standalone offence, different manifestations of such conduct are addressed through various provisions of the Information Technology Act, 2000, the Indian Penal Code, 1860, and, particularly in cases involving children, the Protection of Children from Sexual Offences Act, 2012. With the enactment of the Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code from 1 July 2024, the legal framework governing cyber-related misconduct has undergone significant transition. This research examines the statutory framework regulating cyberbullying in India and analyses significant judicial decisions concerning online harassment, privacy, reputation, and digital abuse. It further identifies major challenges in effective enforcement, including difficulties in identifying perpetrators, jurisdictional complications, technological barriers, under-reporting, delays in investigation, inadequate victim-support mechanisms, and the rapidly evolving nature of digital platforms. The study finds that, although existing legislation provides remedies for several forms of cyberbullying, the absence of a comprehensive statutory definition creates gaps in prevention, enforcement, and victim protection. The research therefore advocates clearer legislative recognition of cyberbullying, strengthened institutional mechanisms, effective cybercrime investigation, greater digital literacy, and improved cooperation among law-enforcement agencies, educational institutions, technology platforms, and civil society. A comprehensive, rights-based, and victim-centric approach is essential to protect individual dignity, privacy, reputation, and digital liberties in

India's rapidly evolving cyberspace and to ensure timely and effective remedies for affected individuals and communities.

Key Words: *- Electronic Bullying, Information Technology Act, Bharatiya Nyaya Sanhita, Web-based Harassment, POCSO, Virtual Liberties, Confidentiality, Liberty of Expression.*

Introduction

Electronic Bullying, Information Technology Act, Bharatiya Nyaya Sanhita, Web-based Harassment, POCSO, Virtual Liberties, Confidentiality, Liberty of Expression.

Online harassment involves leveraging digital communication tools—including social media, electronic mail, messaging apps, and internet forums—to bully, menace, frighten, or slander others. Diverging from conventional bullying methods, cyberbullying is not restricted by physical locations and can happen around the clock, frequently enabling aggressors to hide behind anonymity. Within India, the swift expansion of digital networks, low-cost connectivity, and the ubiquity of mobile devices have markedly boosted digital engagement, especially among teenagers and the youth population. Although digital integration offers many advantages, it has simultaneously triggered a significant increase in internet-based hostility, turning cyberbullying into a critical social and legal issue.

Online harassment presents itself through various methods, such as sending hostile or intimidating communications, digital stalking, provocative trolling, identity fraud, pretending to be someone else, distributing malicious or untrue information, and the unauthorized dissemination of private, sexually explicit photos (frequently termed "revenge porn"). This can furthermore involve doxing, a practice where private details are exposed to the public to torment or frighten an individual. Even though Indian legislation lacks a specific definition for cyberbullying as an independent crime, the different elements of such behavior are subject to penalties under current legal frameworks.

The primary legal framework governing cybercrime in India is the Information Technology Act, 2000 (IT Act), which underwent revisions in 2008. Under Section 66C, identity theft is penalized, whereas Section 66D focuses on fraud committed through electronic impersonation. Section 66E imposes penalties for privacy breaches, which is especially significant in instances involving the illicit recording or sharing of intimate photos. Furthermore, Sections 67, 67A, and 67B establish criminal offenses for the distribution or dissemination of lewd imagery, sexually

explicit media, and child sexual abuse material via digital channels. [1]Taken together, these stipulations tackle numerous actions linked to online harassment.

"The government is prohibited from withholding legal equality or equivalent legal safeguards from any individual residing within the borders of India".

Article 14 ensures two core principles: Equality before the law, meaning no individual possesses immunity from legal authority, and Equal protection of laws, which mandates that legal statutes must be applied uniformly across comparable circumstances. Regarding Article 14 and cybercrime: within the realm of digital offenses, cybercriminals are subject to the same legal consequences as any other lawbreakers. Legislative frameworks, including the Information Technology Act, 2000, are required to be enforced consistently upon every person. State authorities are prohibited from randomly restricting web access, detaining citizens, or initiating legal action against people lacking legitimate justification and equitable treatment. Every piece of cyber legislation must refrain from practicing unjust bias against specific persons or demographics.

Article 19 – Guarantee of Liberty – Section 19(1)(a) stipulates that every citizen is entitled to: The liberty of speech and communication, the liberty of gathering, the liberty of establishing organizations, the liberty of travel, the liberty of settlement, and the liberty to pursue any occupation. Within the digital realm, Article 19(1)(a), which guarantees the Freedom of Speech and Expression, holds the highest significance. Regarding the intersection of Article 19 and cyberspace, the internet serves as a vital medium for various activities, including social media commentary, blogging, web-based journalism, and digital advocacy. The Supreme Court has affirmed that these constitutional protections for free speech extend to the online environment.

Significant Precedent: Shreya Singhal v. Union of India (2015) resulted in the invalidation of Section 66A of the IT Act. The judiciary determined that this provision breached Article 19(1)(a) due to its ambiguous nature and its tendency to suppress digital freedom of expression. However, liberty is not unlimited, as it remains subject to the legitimate constraints outlined in Article 19(2). The government is permitted to enforce justifiable limitations for the purposes of: India's sovereignty and unity, national security, maintaining public tranquility, upholding decency or ethical standards, preventing defamation, and stopping the provocation of criminal acts.

Within the realm of cybercrime, authorities possess the power to prosecute various offenses,

[1] Information Technology Act, 2000, Section 66C, 66D, 66E, 67, 67A, 67B.

including digital hate speech, cyber terrorism, the dissemination of misinformation leading to civil unrest, online slander, and the distribution of explicit material. Regarding the legal framework in India, the Information Technology Act, 2000, addresses several key areas: unauthorized computer access (Section 66), identity fraud (Section 66C), acts of cyber terrorism (Section 66F), the digital publication of lewd content (Section 67), as well as breaches of data security and privacy.

The intersection of privacy rights and digital offenses was highlighted in the landmark case of Justice K.S. Puttaswamy v. Union of India (2017), where the Supreme Court established the Right to Privacy as a Fundamental Right under Article 21. This protection is critical in addressing cyber-related crimes such as data leaks, hacking, identity theft, digital stalking, unlawful monitoring, and web-based harassment. When an individual's private information is exploited online, it constitutes a breach of their Article 21 privacy rights.

Furthermore, cybercrimes represent a direct assault on personal liberty. These offenses can compromise one's Right to Reputation through online defamation, the creation of fraudulent profiles, or the manipulation of images that harm personal dignity. They also threaten the Right to Safety, as cyberbullying and digital intimidation can severely impact mental health. Finally, they infringe upon the Right to Freedom, as illegal spying or the use of spyware undermines individual autonomy. Consequently, various digital crimes act as an indirect violation of the protections guaranteed under Article 21.

Significance of the IT Act, 2000: In an effort to shield citizens within the digital realm, the Indian government implemented the Information Technology Act, 2000. This legislation: penalizes unauthorized system access (Sec 66), criminalizes identity fraud (Sec 66C), addresses cyber terrorism (Sec 66F), and provides security for private and sensitive information. Furthermore, the IT Act functions in conjunction with Article 21 to uphold and defend digital liberties.

Government Surveillance & Article 21

Government monitoring is required to adhere to the following: it must follow legally mandated protocols, be equitable, impartial, and sensible (as established in the 1978 Maneka Gandhi ruling), and satisfy the proportionality standard (per the Puttaswamy judgment). Any unauthorized electronic spying constitutes a breach of Article 21.

While the IT Act, 2000 focuses on specific cybercrimes such as data violations, identity theft,

hacking, and digital terrorism, the BNS, 2023 is utilized when conventional criminal acts are executed via digital or electronic interfaces. Since numerous BNS offenses now specifically mention actions performed through "digital means" or "electronic communication," legal proceedings for cyber-related crimes frequently involve the simultaneous application of both the BNS and the IT Act.

BNS Clauses Pertaining to Cybercrime

Deception and Web-based Scams: Activities like investment scams, UPI fraud, OTP deception, phishing, and various online con games are prosecuted using:

Deception clauses (comparable to the former IPC Section 420), where fraudulent acts carried out through electronic channels are punishable by both monetary penalties and incarceration. Such clauses are frequently utilized in instances of electronic payment scams.

Regarding identity theft and impersonation: while the IT Act (specifically Sections 66C and 66D) addresses identity theft directly, BNS regulations concerning forgery, impersonation, and cheating by personation are invoked when fraudulent digital personas are employed to execute scams.

Digital Defamation: Character assassination conducted via social media updates, YouTube content, blogs, or direct messaging is governed by: The BNS defamation clauses (which supersede IPC Sections 499/500): Disseminating untrue claims through digital channels that damage a person's standing is a punishable offense.

Electronic Criminal Intimidation and Threats: Distributing menacing emails, texts, or social media posts is subject to prosecution under: The criminal intimidation statutes of the BNS (comparable to IPC Section 506).

Vulgarity and Ethics: Distributing or sharing indecent material via the internet can trigger: BNS statutes concerning lewd conduct and writings, in addition to Section 67 of the IT Act (which addresses obscene content in digital formats).

Acts of sexual harassment and cyberstalking, including the transmission of lewd communications, the manipulation of photographs, and digital intimidation, are subject to legal penalties under the following categories: regulations concerning stalking, sexual harassment, and the outraging of women's modesty. Such violations now explicitly encompass actions carried out through digital messaging.

Abolishing Sedition – National Security and Online Expression. The former sedition statute

(IPC 124A) has been substituted within the BNS by a fresh clause regarding: Conduct that threatens the sovereignty, unity, and cohesion of India. Such provisions might be relevant to specific types of digital material that promote unrest or secessionist movements.

Regarding National Security and Cyber Terrorism, major digital crimes—including the unauthorized infiltration of state networks and strikes against essential infrastructure—are primarily addressed by Section 66F of the IT Act (Cyber Terrorism). Nevertheless, BNS statutes concerning the instigation of war, acts of terrorism, and criminal conspiracies might also be invoked, contingent upon the specific circumstances.

Significant Cybercrimes under the IT Act

Section 43 – Harm to Computing Infrastructure: Establishes civil accountability for: Illicit entry, Extracting or replicating information, Injecting malware, Interfering with network operations. Affected parties are entitled to seek financial restitution.

Section 65 – Manipulation of Computer Source Code: Penalizes the deliberate modification or wiping of source code. Penalty: A prison term of up to 3 years, a financial penalty, or both.

Section 66 – Technology-Linked Crimes: When actions described in Section 43 are carried out through deceit or fraud, they are classified as criminal acts. Penalty: Up to 3 years in jail or a fine.

Section 66C – Identity Theft: The illegal utilization of someone else's digital signature, password, or unique identifying data; frequently seen in phishing attacks and OTP-based scams. Penalty: A fine along with up to 3 years of imprisonment.

Section 66D – Impersonation-based Fraud: This pertains to digital deception where individuals pose as others through electronic means. It encompasses various schemes such as UPI-related scams, fraudulent employment opportunities, and deceptive online investment plots.

Section 66E – Breach of Privacy: Recording or disseminating intimate imagery without permission. This includes instances involving surreptitious filming and non-consensual sexual content distribution.

Section 66F – Cyber Terrorism: Encompasses the hacking of essential infrastructure and the deployment of digital threats against national security. Offenders face a potential sentence of life imprisonment.

Part 67 – Indecent Material: The electronic distribution or dissemination of obscene content.

More rigorous penalties for: Sexually explicit content (Section 67A), Child pornography (Section

67B).

Middleman Responsibility (Section 79): Digital facilitators (such as internet service providers and social media networks) receive "safe harbour" immunity provided that: They neither start nor alter the data transfer, and they adhere to prescribed due diligence protocols.

Following the Shreya Singhal v. Union of India (2015) ruling: These platforms are required to take down material solely when instructed by a judicial mandate or state authority.

Restrictions on Access (Section 69A): The state possesses the authority to restrict websites or digital material to protect national sovereignty, maintain security, or uphold public stability. Such actions are required to adhere to established procedural protections. The Supreme Court has validated this legal clause.

Legal Resolution and Cyber Appeal Framework: Designated Adjudicating Officers manage requests for compensation, while appeals are submitted to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

Responsibilities of CERT-In: Under this legislation, the Indian Computer Emergency Response Team (CERT-In) is established to oversee digital threats, distribute official protocols, and manage the synchronization of incident reactions.

This legal matter began when two young females in Maharashtra were taken into custody in 2012 under Section 66A of the Information Technology Act, 2000, for sharing remarks on Facebook that challenged a shutdown triggered by the passing of a political figure. These apprehensions sparked widespread condemnation across the country. Following this, Shreya Singhal initiated a Public Interest Litigation via Article 32 in the Supreme Court to contest the constitutional legitimacy of: Section 66A (concerning derogatory messages sent through communication services), Section 69A (regarding the restriction of websites), Section 79(3)(b) along with the Intermediary Rules, 2011.

The central question was whether Section 66A infringes upon Article 19(1)(a), which guarantees the right to freedom of speech and expression; if it falls within the scope of reasonable restrictions mandated by Article 19(2); whether Section 66A is capricious and contravenes Article 14; the legitimacy of Section 69A (the authority to block content); and the constitutionality of Section 79 and the regulations governing intermediary liability.

The Extent of Free Expression: The Judiciary reiterated that: The right to free speech is equally valid within the digital realm. The specific channel used for expression (whether through print,

verbal discourse, or web-based platforms) has no bearing on the level of constitutional safeguard provided.

Digital connectivity facilitates: Broader dissemination, immediate interaction, and civic engagement. Consequently, electronic communication is granted comprehensive constitutional rights.

Section 66A targeted content deemed to be: “Extremely insulting”, “Threatening”, inducing “irritation”, generating “trouble”, or inciting “animosity” or “hostility”.

The judiciary determined that such phrases were: Vague, Predicated on personal opinion, and Susceptible to capricious construction.

Any legislation that limits expression needs to be unambiguous and exact. Ambiguous statutes infringe upon constitutional protections, as individuals are unable to grasp with certainty which specific actions are forbidden. Consequently, Section 66A did not meet the criteria for justifiable limitations.

An examination of Article 19(2) reveals that this provision allows constraints only on particular foundations, including: India's sovereignty and unity, national security, maintenance of public order, standards of decency or morality, defamation, and the provocation of criminal acts.

The judiciary determined that Section 66A failed to align with any of those specific justifications, penalized verbal expressions simply for creating irritation or discomfort, and vastly exceeded acceptable constitutional boundaries.

In its ruling, the Court established a vital doctrine: restrictions on expression are only justifiable when the speech triggers immediate unrest or violent disturbances. By penalizing mere debate and support, Section 66A was deemed unconstitutional.

The judiciary acknowledged the phenomenon known as a “chilling effect.” When legal statutes are imprecise and overly expansive, individuals refrain from voicing their perspectives, as the dread of prosecution stifles lawful discourse. This cooling of expression undermines the fundamental principles of democracy.

Due to the absence of precise benchmarks and the potential for capricious application, Section 66A simultaneously breached Article 14 regarding the Right to Equality. Consequently, the Supreme Court ruled the entire provision unconstitutional and invalidated it. The ruling determined that the provisions infringed upon Articles 14 and 19(1)(a).

However, the Court affirmed the constitutionality of Section 69A, noting that it incorporates

necessary procedural protections. Specifically, blocking actions are permitted only under the justifications outlined in Article 19(2), a formal review process exists, and all directives must be supported by clear reasoning. Consequently, Section 69A was deemed to be legally sound.

Under Section 79, intermediaries such as Facebook and Google are granted safe harbor immunity. Nevertheless, Rule 3(4) mandates that these platforms delete specific content within a 36-hour window once they have been notified.

The judiciary narrowed the scope of this clause: Platforms are obligated to delete material solely in response to: A judicial mandate, or an official state directive issued via Section 69A. They are under no obligation to comply based on individual grievances alone.

A monumental ruling safeguarding digital expression, reinforcing constitutional legal principles regarding ambiguity and the suppression of speech. Extended the safeguards of Article 19 to the digital realm. Restrained unjustified government interference. Set incitement as the primary standard for censoring expression.

The ruling underscored several key principles: democratic systems rely on the unrestricted flow of thought, the government is prohibited from silencing expression simply due to its controversial nature, and any limitations imposed must be highly precise, limited in scope, and balanced.

Shreya Singhal v. Union of India stands as a landmark achievement in the constitutional jurisprudence of India. To safeguard free expression within the digital landscape, the Supreme Court invalidated Section 66A, though it simultaneously affirmed legitimate oversight tools such as Section 69A. This legal precedent continues to serve as a cornerstone for internet liberties, constitutional protections, and the boundaries of government authority.

A major legal milestone within this domain was the Supreme Court's ruling in Shreya Singhal v. Union of India (2015).[2] The Court invalidated Section 66A of the IT Act, ruling it unconstitutional due to its ambiguous nature. It was determined that this clause breached Article 19(1)(a) of the Constitution, which protects the fundamental right to freedom of speech and expression. Although this ruling bolstered safeguards for freedom of expression, it simultaneously sparked contention concerning whether existing legal mechanisms are sufficient to combat offensive digital discourse.

Beyond the IT Act, conventional criminal statutes are also applicable to instances of cyberbullying. Within the framework of the Indian Penal Code, 1860 (IPC)—which has been

largely superseded by the Bharatiya Nyaya Sanhita (BNS), 2023—legal provisions regarding criminal intimidation (Section 503 IPC), defamation (Sections 499–500 IPC), stalking (Section 354D IPC), and violating a woman's modesty (Section 509 IPC) are commonly cited during proceedings related to digital harassment.[3] Such stipulations prove that cyberbullying falls within the boundaries of criminal legislation, even in the absence of a specific designation.

The Protection of Children from Sexual Offences (POCSO) Act, 2012 serves a vital function in shielding young individuals from digital sexual abuse, grooming, and predatory behavior.[4] Since youngsters and adolescents represent some of the most susceptible targets of online harassment, POCSO offers a critical dimension of judicial safeguarding.

Even with these statutes in place, numerous obstacles prevent successful implementation. Primarily, frequent underreporting occurs because of societal prejudice, dread of reprisal, and insufficient knowledge concerning available legal recourse. Furthermore, the masked identity of wrongdoers and the employment of fraudulent profiles hinder both inquiry and the gathering of proof. Additionally, legal authority dilemmas emerge when criminals function across various regional or international borders. Furthermore, digital crime units across numerous areas struggle with inadequate funding and skill gaps, which hinders the pace and effectiveness of their inquiries.

A further major complication is the lack of a thorough, specialized legal framework specifically targeting cyberbullying. Existing methods depend on the implementation of disjointed clauses from various statutes, a practice that risks creating discrepancies in legal proceedings and penalties. Consequently, legal experts have advocated for more precise legislative terminology, robust assistance frameworks for victims, enhanced digital education initiatives, and expert instruction for police and judicial officials.

To summarize, digital harassment within India signifies a complicated overlap of technological advancement, legal systems, and fundamental human liberties. Although the Information Technology Act, various IPC/BNS statutes, and the POCSO Act together tackle numerous dimensions of web-based mistreatment, the absence of a dedicated statutory structure for cyberbullying underscores an urgent requirement for legislative updates. It is vital to adopt a proportional method that upholds the right to free speech guaranteed by Article 19, while simultaneously defending personal privacy and human dignity as mandated by Article 21 of the

Constitution. Enhancing enforcement, public consciousness, and organizational capabilities will be essential for successfully tackling cyberbullying within India's shifting digital environment.

References

- Constitution of India, 1950.
- Digital Personal Data Protection Act, 2023.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- Indian Penal Code, 1860, Section 499, 500, 503, 354D, 509 (now reflected in Bharatiya Nyaya Sanhita, 2023).
- Protection of Children from Sexual Offences Act, 2012.
- Ministry of Electronics and Information Technology, Government of India.
- Nayak, Ameya Avadhut, The DPDP Act, 2023 & Puttaswamy Judgment: At the Constitutional Crossroads.
- Rohan S., Consent, Control, and the Constitution: Deconstructing India's Digital Personal Data Protection Act, 2023.