INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER BULLYING AND SOCIAL MEDIA ABUSE IN INDIA: LEGAL CHALLENGES, EMERGING TRENDS, AND POLICY RESPONSES

AUTHORED BY - SHIREEN SULTANA
Assistant Professor of Law
Christ Academy Institute of Law, Bengaluru

Abstract

The unprecedented growth of digital technologies and social media platforms has transformed communication, education, commerce, and governance across the globe. In India, where internet penetration and smartphone usage continue to expand rapidly, social media has become an indispensable part of everyday life. However, alongside these technological advancements, a significant rise in cyberbullying and social media abuse, posing serious legal, ethical, and psychological challenges, has emerged. Cyberbullying encompasses repeated acts of harassment, intimidation, humiliation, and victimization conducted through digital platforms, while social media abuse includes a broader spectrum of unlawful online activities such as cyberstalking, identity theft, online defamation, dissemination of obscene content, hate speech, and the circulation of misinformation. These offences disproportionately affect women, children, adolescents, and marginalized communities, often resulting in emotional trauma, reputational harm, and violations of the constitutional rights to dignity and privacy. This chapter critically examines the evolving landscape of cyber bullying and social media abuse in India by exploring their conceptual framework, prevalence, legal implications, and societal impact. It further analyses the adequacy of the existing legal framework and identifies contemporary challenges associated with emerging technologies, including artificial intelligence and deepfakes. The chapter argues that a multidisciplinary approach involving legal reform, digital literacy, institutional accountability, and responsible platform governance is critical to creating a safe and inclusive digital environment.

Keywords: Cyberbullying, Social Media Abuse, Information Technology Act, Digital Privacy, Online Harassment, Cyber Law, India.

ISSN: 2582-6433

1. Introduction

The digital revolution has fundamentally reshaped the way individuals communicate, interact, and access information. Social networking platforms such as Facebook, Instagram, WhatsApp, X (formerly Twitter), Snapchat, and YouTube have become integral components of personal and professional life. India, with one of the largest internet user populations globally, has witnessed remarkable growth in digital participation due to affordable internet services, increasing smartphone penetration, and governmental initiatives promoting digital inclusion (Statista, 2024).

While these technological developments have democratized access to information and facilitated economic and social development, they have simultaneously created new opportunities for cybercrime. Among the most concerning manifestations are cyber bullying and social media abuse, which have emerged as persistent threats affecting individuals across all demographic groups. Unlike traditional forms of bullying, cyberbullying is not confined by geographical boundaries or time constraints. Harmful messages, manipulated images, defamatory content, and abusive comments can instantly reach a global audience and remain accessible indefinitely, amplifying their detrimental impact.

The anonymity that digital platforms afford often emboldens perpetrators, making it difficult for victims to identify offenders or seek effective legal remedies. Consequently, cyberbullying has evolved into a complex socio-legal issue requiring coordinated responses from legislators, law enforcement agencies, educational institutions, technology companies, and civil society organizations.

India has experienced a steady increase in cybercrime complaints over the past decade, with online harassment constituting a substantial proportion of reported incidents. Women and children remain particularly vulnerable to cyberstalking, revenge pornography, online sexual harassment, identity theft, and malicious dissemination of personal information. These offences not only infringe individual rights but also undermine public confidence in digital platforms as safe spaces for communication and participation.

2. Understanding Cyber Bullying and Social Media Abuse

Cyberbullying refers to the deliberate and repeated use of digital communication technologies to threaten, harass, intimidate, embarrass, or humiliate another individual. It differs from

ISSN: 2582-6433

isolated incidents of online conflict by involving a sustained pattern of aggressive behavior intended to inflict emotional, psychological, or reputational harm. Unlike conventional bullying, cyber bullying enables perpetrators to target victims anonymously, continuously, and on a large scale, thereby intensifying the consequences for those affected (Hinduja & Patchin, 2018).

Social media abuse encompasses a broader range of harmful online behaviors extending beyond cyberbullying. It includes the misuse of digital platforms to engage in unlawful or unethical activities such as cyberstalking, impersonation, identity theft, online defamation, dissemination of sexually explicit material without consent, hate speech, phishing, financial fraud, and the spread of misinformation. The rapid evolution of digital technologies has further facilitated sophisticated forms of abuse, including the creation and dissemination of AI-generated deepfakes capable of damaging reputations and manipulating public opinion.

The impact of cyber bullying extends far beyond temporary emotional distress. Victims frequently experience anxiety, depression, diminished self-esteem, academic decline, workplace difficulties, and social isolation. In severe cases, persistent online harassment has been associated with self-harm and suicidal ideation. The permanence and viral nature of online content distinguish cyberbullying from traditional bullying, as harmful material may remain accessible long after its initial publication, continuously revictimizing affected individuals.

The phenomenon also raises important constitutional and human rights concerns relating to the rights to equality, dignity, privacy, and freedom of expression. While digital platforms facilitate democratic participation and the free exchange of ideas, they also create environments in which these rights may be undermined through harassment, intimidation, and coordinated online abuse. Consequently, we must carefully balance safeguarding freedom of speech by protecting individuals from unlawful digital harm when addressing cyberbullying.

3. Constitutional Perspective

Although the Constitution of India does not explicitly recognize a right to protection from cyber bullying or online abuse, several fundamental rights provide the constitutional basis for safeguarding individuals in the digital environment. The interplay between the right to equality, freedom of speech, and the right to life and personal liberty forms the foundation of India's cyber jurisprudence.

ISSN: 2582-6433

Article 14, which guarantees equality before the law and equal protection of the laws, obligates the State to protect all individuals from arbitrary and discriminatory conduct, including harassment occurring in cyberspace. Cyberbullying often disproportionately affects women, children, individuals with disabilities, and members of marginalized communities, thereby raising concerns relating to substantive equality and equal access to digital spaces.

Article 19(1)(a) guarantees freedom of speech and expression, a cornerstone of democratic participation. Social media platforms have significantly expanded opportunities for public discourse and civic engagement. However, this freedom is not absolute. **Article 19(2)** authorizes the State to impose reasonable restrictions on the interests of sovereignty, security, public order, decency, morality, defamation, and incitement to an offence. Consequently, expressions that constitute criminal intimidation, defamation, hate speech, or targeted online harassment do not receive absolute constitutional protection.

The constitutional significance of privacy has expanded following the Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which recognized the **right to privacy** as an intrinsic component of **Article 21**. The unauthorized disclosure of personal information, cyberstalking, non-consensual dissemination of intimate images, and identity theft constitute serious infringements of informational privacy and personal dignity. Cyber bullying therefore implicates not only statutory protections but also fundamental constitutional guarantees.

The challenge before lawmakers and courts lies in balancing the constitutional commitment to free expression with the need to protect individuals from digital abuse. Excessive regulation may chill legitimate speech, whereas inadequate regulation leaves victims vulnerable to persistent online victimization.

4. Statutory Framework Governing Cyber Bullying

4.1 Information Technology Act, 2000

The **Information Technology Act, 2000** remains India's principal legislation regulating electronic communications and cyber offences. Although the Act does not specifically define "cyber bullying," several provisions address conduct commonly associated with online harassment.

Section 66C criminalizes identity theft involving the fraudulent use of passwords, digital

ISSN: 2582-6433

signatures, or other unique identification features.

Section 66D penalizes cheating by personation through computer resources, which frequently occurs through fake social media profiles and fraudulent online communications.

Section 66E protects individual privacy by criminalizing the intentional capture, publication, or transmission of images depicting private areas without consent.

The Act also regulates the dissemination of obscene and sexually explicit content through the following:

- **Section 67** – Publishing or transmitting obscene material in electronic form.
- **Section 67A** – Publishing sexually explicit material electronically.
- **Section 67B** – Publishing or transmitting material depicting children in sexually explicit acts or child sexual abuse material.

These provisions are particularly relevant where cyberbullying involves image-based abuse, revenge pornography, online sexual exploitation, or circulation of intimate content without consent.

A significant constitutional development occurred in *Shreya Singhal v. Union of India* (2015), where the Supreme Court declared **Section 66A** unconstitutional for being vague and disproportionately restricting freedom of speech. While the judgment strengthened constitutional protections for online expression, it also reaffirmed that offences involving criminal intimidation, obscenity, defamation, and incitement remain punishable under other statutory provisions.

4.2 Bharatiya Nyaya Sanhita, 2023

The enactment of the **Bharatiya Nyaya Sanhita, 2023 (BNS)** modernized India's criminal law framework. Although the legislation does not create a separate offence titled "cyberbullying," numerous provisions apply to online misconduct depending on the factual circumstances.

Cyberbullying may attract criminal liability where conduct amounts to the following:

- Criminal intimidation through electronic communications.
- Online defamation that causes reputational harm.
- Sexual harassment committed via digital platforms.
- Voyeurism involving unauthorized dissemination of private images.
- Stalking, including persistent online monitoring or unwanted electronic contact.
- Circulation of obscene or sexually explicit material.

The BNS reflects legislative recognition that traditional criminal offences increasingly occur through digital means. Consequently, electronic communications, digital evidence, and social

ISSN: 2582-6433

media interactions assume greater evidentiary significance during criminal investigations and prosecutions.

4.3 Digital Personal Data Protection Act, 2023

The **Digital Personal Data Protection Act, 2023 (DPDP Act)** represents a major development in India's privacy framework by regulating the processing of digital personal data.

Although the act primarily governs obligations of data fiduciaries and consent-based processing, it has major repercussions for cyberbullying and social media abuse. Unauthorized collection, disclosure, profiling, or misuse of personal information frequently facilitates online harassment, impersonation, financial fraud, and targeted abuse.

The legislation introduces principles such as the following:

- Lawful processing of personal data.
- Purpose limitations.
- Data minimization.
- Protection of children's personal data.
- Accountability of data fiduciaries.
- Rights of individuals regarding their personal information.

Effective implementation of these principles may substantially reduce opportunities for identity theft, doxxing, and misuse of personal information on digital platforms.

4.4 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Recognizing the growing influence of digital intermediaries, the government introduced the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**.

The Rules impose due diligence obligations upon intermediaries, including social media platforms. Significant responsibilities include:

- Appointment of grievance officers.
- Establishment of effective complaint-redressal mechanisms.
- Timely removal of unlawful content upon receiving valid legal directions.
- Preservation of digital records for investigative purposes.
- Cooperation with law enforcement agencies.

Large social media platforms are expected to adopt greater transparency regarding content moderation and user grievance mechanisms. While these obligations strengthen user

ISSN: 2582-6433

protection, they have also generated debates concerning intermediary liability, user privacy, and governmental oversight of online speech.

Critical Evaluation

India's statutory framework demonstrates a progressive attempt to address various manifestations of cyber abuse through multiple legislative instruments. However, the absence of a **specific statutory definition of** cyberbullying results in fragmented enforcement. Investigators frequently rely upon multiple provisions scattered across different enactments, creating uncertainty regarding jurisdiction, evidentiary standards, and prosecutorial consistency.

Furthermore, technological advancements—including encrypted messaging services, anonymous accounts, artificial intelligence-generated content, and cross-border digital platforms—continue to outpace legislative reforms. Consequently, legal regulation alone cannot effectively address cyber bullying without complementary measures involving digital literacy, technological safeguards, institutional cooperation, and responsible platform governance.

5. Judicial Responses to Cyber Bullying and Social Media Abuse

The Indian judiciary has played an important part in shaping the legal discourse on cyber law by balancing the constitutional guarantee of freedom of speech with the protection of individual dignity, privacy, and reputation. Although India lacks a dedicated statute specifically addressing cyber bullying, judicial interpretation has expanded the application of constitutional principles and statutory provisions to address online harms.

A landmark decision in this regard is *Shreya Singhal v. Union of India* (2015), where the Supreme Court invalidated Section 66A of the Information Technology Act, 2000, holding that its vague and overbroad language violated Article 19(1)(a) of the Constitution. The Court observed that restrictions on online speech must satisfy the constitutional requirements under Article 19(2) and cannot be based upon subjective interpretations of annoyance or inconvenience. While the judgment strengthened freedom of expression in cyberspace, it also reaffirmed that unlawful online conduct involving criminal intimidation, defamation, obscenity, incitement, and threats remains punishable under existing laws (Government of India, 2000; *Shreya Singhal v. Union of India*, 2015).

Equally significant is *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), in which the

ISSN: 2582-6433

Supreme Court recognized the right to privacy as a fundamental right under Article 21. The judgment emphasized informational privacy, autonomy, and personal dignity in the digital era. This constitutional recognition has profound implications for cyberbullying cases involving unauthorized disclosure of personal information, identity theft, cyberstalking, image-based abuse, and non-consensual dissemination of intimate content.

Indian High Courts have also increasingly recognized the importance of protecting individuals from online harassment by directing the removal of defamatory or obscene digital content and emphasizing the responsibility of investigative agencies to address cyber offences expeditiously. These judicial interventions demonstrate an evolving recognition that digital abuse causes real and lasting harm, warranting timely legal remedies.

6. Comparative Legal Perspectives

United Kingdom

The United Kingdom does not have a single comprehensive cyberbullying statute; instead, it addresses online abuse through a combination of criminal laws, including the **Malicious Communications Act 1988**, the **Communications Act 2003**, and the **Online Safety Act 2023**. The Online Safety Act imposes extensive duties on digital platforms to identify, mitigate, and remove harmful content while strengthening protections for children and vulnerable users. The regulatory approach emphasizes platform accountability, proactive risk assessments, and transparency in content moderation.

United States

The United States primarily regulates cyber bullying through state legislation rather than a unified federal law. Most states have enacted anti-bullying statutes requiring educational institutions to develop policies addressing cyberbullying among students. However, the strong constitutional protection afforded freedom of speech under the First Amendment limits governmental regulation of online expression unless it falls within recognized exceptions such as true threats, harassment, or defamation. Consequently, the American approach seeks to balance individual liberty with protection from digital abuse.

Australia

Australia has adopted a comparatively proactive regulatory framework. The establishment of the **e-Safety Commissioner** provides a specialized institutional mechanism for addressing

ISSN: 2582-6433

cyberbullying, image-based abuse, online safety complaints, and harmful digital content. The **Online Safety Act 2021** empowers the Commissioner to require removal of abusive material, investigate complaints, and promote digital safety education. Australia's model demonstrates the effectiveness of combining legal regulation with specialized administrative oversight.

Lessons for India

Comparative analysis reveals that effective regulation of cyber bullying extends beyond criminal sanctions. Successful jurisdictions integrate legal enforcement with digital literacy programs, platform accountability, specialized regulatory institutions, victim support mechanisms, and public awareness initiatives. India may benefit from adopting a similarly coordinated regulatory approach while respecting constitutional guarantees of free expression.

7. Emerging Challenges in the Digital Era

Rapid technological innovation continues to transform the nature of cyber bullying and social media abuse. Artificial intelligence, machine learning, and generative technologies have created new forms of digital victimization that challenge existing legal frameworks.

One of the most concerning developments is the proliferation of **AI-generated deepfakes**, which involve the creation of highly realistic, manipulated images, audio recordings, or videos depicting individuals engaging in conduct that never occurred. Deepfakes can facilitate political disinformation, financial fraud, revenge on pornography, reputational attacks, and cyber extortion. Existing legal provisions addressing obscenity, identity theft, and defamation may apply in certain situations, but they do not comprehensively regulate the unique harms created by synthetic media.

Another significant concern is **cyberstalking**, characterized by persistent monitoring, repeated messaging, online surveillance, and unwanted digital communication. The widespread availability of location-sharing technologies, facial recognition software, and publicly accessible personal information have increased the opportunities for perpetrators to continuously monitor victims.

The widespread use of **anonymous accounts** further complicates enforcement efforts. Perpetrators frequently exploit encrypted communication services, virtual private networks (VPNs), temporary accounts, and foreign-hosted platforms to conceal their identities and evade

ISSN: 2582-6433

legal accountability. These technological realities often create jurisdictional and evidentiary challenges for law enforcement agencies.

Algorithm-driven social media platforms present additional concerns. Recommendation systems designed to maximize user engagement may inadvertently amplify abusive content, misinformation, hate speech, and coordinated harassment campaigns. The rapid dissemination of harmful content can expose victims to repeated victimization before platforms respond to complaints or remove the offending material.

Another emerging issue involves the mental health consequences of sustained online harassment. Numerous studies indicate that cyber bullying contributes to anxiety, depression, academic disengagement, social withdrawal, and reduced psychological well-being, particularly among adolescents and young adults (Hinduja & Patchin, 2018). The permanence and public visibility of online abuse frequently intensify these harms compared with traditional forms of bullying.

These developments demonstrate that cyberbullying has evolved from an individual behavioral problem into a multidimensional legal, technological, and public policy challenge. Addressing these complexities requires adaptive legislation, improved cyber forensic capabilities, responsible platform governance, international cooperation, and continuous public education concerning responsible digital citizenship.

8. Recommendations

The increasing prevalence of cyber bullying and social media abuse necessitates a comprehensive legal and policy framework that extends beyond criminal sanctions. A multidimensional approach involving legislative reform, technological innovation, institutional accountability, education, and public participation is essential for ensuring digital safety.

8.1 Enact a Dedicated Law on Cyber Bullying

India currently addresses cyber bullying through provisions dispersed across the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and other statutes. Although these laws provide remedies against specific forms of online misconduct, they do not comprehensively define or regulate cyber bullying. A dedicated statute should clearly define cyber bullying, categorize various forms of online abuse, prescribe proportionate penalties, and

ISSN: 2582-6433

establish victim-centric remedies, particularly for children, women, senior citizens, and other vulnerable groups.

8.2 Strengthen Institutional Mechanisms

Cybercrime investigation requires specialized knowledge of digital evidence, cyber forensics, and cross-border cooperation. Therefore, dedicated cybercrime units should be adequately staffed and trained, while judicial officers and prosecutors should receive regular capacity-building programs on emerging technologies, digital evidence, and cyber jurisprudence. Efficient grievance and redressal mechanisms and fast-track procedures may significantly improve access to justice for victims.

8.3 Enhance Platform Accountability

Social media companies should implement robust mechanisms for identifying and responding to cyber bullying. Artificial intelligence-based moderation systems, transparent reporting procedures, timely removal of unlawful content, and independent grievance officers can substantially reduce online harm. However, automated moderation should remain subject to human oversight to prevent arbitrary restrictions on legitimate expression.

8.4 Promote Digital Literacy and Awareness

Preventive education remains one of the most effective strategies against cyber bullying. Schools, universities, and community organizations should incorporate digital citizenship, cyber ethics, online privacy, and responsible social media usage into educational curricula. Parents and educators should also receive training to identify early signs of online harassment and provide appropriate support to affected individuals.

8.5 Improve International Cooperation

Since digital platforms operate across national boundaries, cyber investigations often require cooperation between multiple jurisdictions. India should strengthen mutual legal assistance mechanisms, promote international information sharing, and actively participate in global initiatives addressing cybercrime and digital governance.

8.6 Address Emerging Technologies

Legislative frameworks should evolve to regulate emerging threats such as artificial intelligence-generated deepfakes, synthetic media, algorithmic manipulation, and identity-

ISSN: 2582-6433

based digital fraud. Periodic review of cyber legislation will ensure that legal responses remain consistent with technological developments while preserving constitutional freedoms.

9. Conclusion

The rapid expansion of digital communication has transformed Indian society by enhancing access to information, economic opportunities, and democratic participation. Nevertheless, these technological advancements have simultaneously facilitated new forms of harassment, intimidation, and abuse that threaten individual dignity, privacy, and psychological well-being. Cyber bullying has evolved into a significant socio-legal challenge requiring coordinated responses from governments, educational institutions, technology companies, civil society organizations, and individual users.

India possesses an evolving legal framework through the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Judicial decisions have further strengthened constitutional protections relating to freedom of expression and informational privacy while recognizing the need to protect individuals from unlawful online conduct.

Despite these developments, several challenges remain unresolved. The absence of a dedicated cyberbullying statute, inconsistent enforcement, jurisdictional complexities, anonymity of offenders, technological advancements, and the emergence of artificial intelligence-generated content continue to complicate legal regulation. Addressing these challenges requires not only legislative reform but also stronger institutional capacity, improved digital literacy, responsible platform governance, and greater international cooperation.

Ultimately, a secure digital ecosystem depends upon balancing technological innovation with constitutional values of liberty, equality, dignity, and privacy. As India continues its digital transformation, the law must evolve proactively to ensure that cyberspace remains an environment that promotes innovation while safeguarding fundamental rights and protecting individuals from emerging forms of online harm.

ISSN: 2582-6433

References

Hinduja, S., & Patchin, J. W. (2018). *Connecting adolescent suicide to the severity of bullying and cyberbullying*. Journal of School Violence, 18(3), 333–346.

Statista. (2024). *Number of internet users in India from 2015 to 2024*. https://www.statista.com

Government of India. (2000). *Information Technology Act, 2000*.

Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.

Government of India. (2023). *Bharatiya Nyaya Sanhita, 2023*.

Government of India. (2023). *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.

Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.

National Crime Records Bureau. (2023). *Crime in India 2023*. Ministry of Home Affairs. https://ncrb.gov.in

Patchin, J. W., & Hinduja, S. (2023). *Cyberbullying prevention and response: Expert perspectives*. Cyberbullying Research Center.

United Nations Children's Fund. (2021). *The State of the World's Children 2021: On My Mind —Promoting, Protecting, and Caring for Children's Mental Health*. UNICEF.

World Health Organization. (2022). *World mental health report: Transforming mental health for all*. World Health Organization.