
DIGITAL ABUSE AND HUMAN RIGHTS: LEGAL PROTECTION OF WOMEN AND CHILDREN IN ONLINE SPACES

Nidhi Yadav & Anushka Singh, Aligarh Muslim University, Aligarh, Uttar Pradesh.

ABSTRACT

The rapid development of digital technologies has changed the way we communicate, learn and interact with each other, but has also created new opportunities for abuse and exploitation. Women and children are among the most vulnerable groups affected by online violence, facing threats that extend beyond the virtual world and significantly impact their dignity, privacy, security, and overall well-being. This study examines digital abuse against women and children as a serious human rights issue rather than just a cybercrime issue. It uses a human rights-based approach to examine various forms of online violence, including cyber harassment, cyberstalking, image-based sexual abuse, non-consensual sharing of intimate content, deepfake technology, online grooming and technology-facilitated exploitation.

The paper examines the ways in which these forms of abuse violate internationally recognized human rights, including the rights to dignity, equality, privacy, freedom from discrimination, and protection from violence. It looks at key international human rights instruments, and evaluates the obligations of States to prevent, investigate and remedy digital harms. The study also examines the role and accountability of digital platforms in making safer online environments through content moderation, transparency and accountability measures. It also highlights the intersectional nature of digital abuse, emphasizing the ways in which gender, age, socio-economic status, disability and marginalization can increase vulnerability and hinder access to justice.

The paper critically analyses existing criminal and civil legal frameworks, highlighting major gaps in the protection, enforcement and victim support mechanisms. It calls for a change from a purely punitive approach to a rights-based, survivor-centred and child-sensitive approach. The study concludes with a call for comprehensive legal reforms, increased institutional responses, improved digital literacy initiatives, and greater platform accountability to ensure digital spaces are safe, inclusive, and respectful of fundamental human rights for all users.

1. GROWTH OF DIGITAL SPACES AND THEIR INTERACTION

The rise of digital spaces has fundamentally reshaped the "public space," expanding it from traditional physical locations like parks and cafes into virtual domains that constitute a "digital public space".¹ This change has transformed human connectivity by facilitating a high level of global interaction that goes beyond geographical and temporal boundaries, regardless of physical location. As digital platforms such as social media become the centre of social life, they foster a unique "digital culture" characterised by immediate information exchange.² This shift offers individuals with physical disabilities or those living in remote locations to participate in community discourse, access e-governance services, and mobilise global support for social movements like "Black Lives Matter" and "MeToo". Furthermore, technology-mediated interaction has introduced significant flexibility in professional and personal life through video conferencing and instant messaging.³

1.1 Why women and children are disproportionately affected in online spaces

Women and children are disproportionately affected in online spaces because digital violence are common cases, of a systemic extension of structural sexism and offline inequalities. Digital spaces have become an extension of the unsafe environments women already face in homes, schools, and workplaces. Harms that begin online, such as grooming or stalking, frequently lead to physical violence, kidnapping, or murder in offline settings. The technology-facilitated violence, particularly image-based sexual abuse, is used as a tool for extortion, forcing survivors to face sexual harassment or engage in further sexual acts.

Children face distinct risks because their developmental stage which makes them emotionally vulnerable. Abusers often lure children on public social media platforms and then use "off-platforming" tactics to move the conversation to private, end-to-end encrypted messaging apps where abusive exchanges are nearly impossible for parents or platforms to detect. Children are often seen more susceptible to Ai algorithm systems that inadvertently serve them dangerous content, such as materials promoting self-harm, eating disorders, or extremist ideologies. And in regions like India, entrenched patriarchal norms create specific layers of vulnerability that

¹ Johni Eka Putra, Dedah Ningrum, *et al.*, "Transforming Public Spaces in the Digital Age: How Technology Changes the Face of Social Interaction" 2(10) *International Journal of Society Reviews* 2711–2724 (2024).

² "Intersection of Environmental Law and Climate Justice in India: A Critical Analysis" Vol. V (Issue II) *Research in Law* (National Law University and Judicial Academy, Assam).

³ *Id* at 1.

restrict women's agency. Survivors often under-report online violence because they fear that disclosure will lead to further restrictions on their device ownership and digital participation.⁴

1.2 Digital abuse as a human rights issue, not merely a cyber offence

The shifting phase of digital abuse from a technical cyber offence to a core human rights issue marks a significant change in legal and philosophical thought. Earlier, cybercrime was viewed as a matter of protecting computer systems and data from unlawful access. However, as digital technologies now dominate almost every human interaction, the virtual environment has become a primary site for both the exercise and the violation of fundamental human rights.⁵

Under Social Contract Theory, the state has a reciprocal obligation to safeguard individuals from digital threats while balancing public safety against personal liberty. This duty becomes a legal necessity because digital abuse directly assaults the right to privacy, often cited as the cornerstone of digital dignity.

The impact of digital abuse is particularly devastating in the context of gender-based violence, often referred to as leaving "invisible wounds" in the digital world. Existing legal frameworks, such as India's Information Technology Act, 2000 are sometimes criticized for using non-gender-specific language that fails to capture the unique, targeted nature of these human rights violations.⁶

The role of the judiciary is critical in ensuring that the digital environment remains a safe space for human rights. Courts have increasingly intervened to bridge the "digital divide," recognizing internet access as a fundamental right necessary for full social and political participation, as seen in the *Anuradha Bhasin* and *Faheema Shirin* cases. Addressing these issues requires more than technical security.⁷

⁴ Syed Faraz Akhtar and Moumita Datta Bhowmik, "Digital Violence: The Rise of Online Gender-Based Violence Against Women in the Age of Social Media" *International Journal for Multidisciplinary Research (IJFMR)*.

⁵ Swarupa Dholam and Aditi Sawant, "The Impact of Cybercrime on Human Rights" 3(1) *International Journal of Legal Studies and Social Sciences* 488–514 (2025).

⁶ Sapnaben Pruthvisinh Zala, "Invisible Wounds in a Digital World: A Legal Dissection of Cyber Victimization of Women in Contemporary India" 5(3) *Indian Journal of Integrated Research in Law* (2025).

⁷ Tatiana Tropina, "'This Is Not a Human Rights Convention': The Perils of Overlooking Human Rights in the UN Cybercrime Treaty" 9(2) *Journal of Cyber Policy* 200 (2024).

1.3 Research Problem

Digital platforms have enlarged opportunities for expression and participation, but they have also become sites of abuse targeting women and children. Online harassment, cyberstalking, image-based abuse, grooming, and technology-facilitated sexual exploitation continue to rise. Existing frameworks such as the Information Technology Act, 2000 and relevant provisions of the Bharatiya Nyaya Sanhita, 2023 were not designed to address the scale, anonymity, and cross-border nature of digital abuse. This creates a protection gap that undermines human dignity, equality, privacy, and access to justice.

Objectives of the Study

1. To examine the nature and forms of digital abuse faced by women and children in online spaces.
2. To analyse digital abuse through a human rights framework, focusing on dignity, privacy, equality, and freedom from violence.
3. To critically assess the adequacy of existing Indian legal mechanisms addressing online abuse.
4. To identify institutional and enforcement challenges in providing effective legal protection.
5. To propose rights-oriented legal and policy reforms for stronger protection in digital environments.

1.4 Thesis Statement

This study argues that digital abuse against women and children constitutes a violation of fundamental human rights, and that India's current legal framework is insufficiently equipped to address the complexities of online harm. It contends that a rights-based, victim-centric, and technologically responsive legal approach is essential to ensure meaningful protection, accountability, and access to justice in digital spaces.

2. MEANING AND SCOPE OF DIGITAL ABUSE AND VIOLENCE

Digital abuse refers to the misuse of digital technology by an individual to monitor, stalk, harass, threaten, control, or impersonate another person. Such abuse may take various forms, including tracking someone through social media platforms, repeatedly sending abusive or intimidating messages, or publicly shaming a person by sharing private images or videos without consent.⁸

‘Technology facilitated violence’ is the term used by UN to describe the violence taking place against women and children through technological tools where these tools are being used to inflict harm both in virtual spaces and in technological world. The pre-existing forms of gender-based violence have been intensified-including sexual harassment, stalking, defamation etc.⁹

2.1 Forms of Digital Abuse

Cyber Threats- It refers to the unwanted and nonconsensual behaviour carried out through digital or online platforms that is intended to annoy or harass any person. It typically includes the act of sending abusive and threatening messages with the sole purpose of targeting and tormenting an individual.¹⁰ India is one of the top countries globally for email-related threats, with over 1 billion email-based threats detected in recent reporting.¹¹ Around 46% of women who experienced online abuse described it as misogynistic or sexist in nature.¹²

Cyber Stalking- It denotes a sustained pattern of unwanted and intrusive digital monitoring and communication. This may involve closely observing a person’s media presence, repeatedly sending messages or using technological tools to follow their online behaviour. The stress is

⁸ Police.uk, “Digital Domestic Abuse”, available at: <https://www.police.uk/advice/advice-and-information/daa/domestic-abuse/digital-domestic-abuse/> (last visited on Jan. 14, 2026).

⁹ UN Women, “FAQs: Digital Abuse, Trolling, Stalking and Other Forms of Technology-Facilitated Violence Against Women and Girls” (UN Women Knowledge Hub, Nov. 13, 2025), available at: <https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women> (last visited on Jan. 14, 2026).

¹⁰ Michigan Technological University, “Cyber Harassment”, available at: <https://www.mtu.edu/deanofstudents/policies-resources/intervention/cyber-harassment/> (last visited on Jan. 14, 2026).

¹¹ Trend Micro, “Cyber Risk Report 2025: India’s Cyber Risk Profile Intensifies with AI-Driven Threats” (Press Release, June 10, 2025), available at: <https://www.trendmicro.com/en/about/newsroom/local-press-releases/in/2025/2025-06-10.html> (last visited on Jan. 14, 2026).

¹² Amnesty International, *Online Violence against Women: Global Survey Results* (IPSOS MORI Poll, 2017), available at: <https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women> (last visited on Jan. 14, 2026).

on the repletion of the activity and invasion of privacy. *Ritu Kohli Case (2001)*¹³ became the 1st reported cyber stalking case prosecuted under section 509 of IPC, where Manish Kathuria impersonated Ritu Kohli on mlrc.com, shared her phone number, set obscene messages. Leading harassing calls from India and abroad, causing the victim much mental distress.

Deepfakes-The rapid advancement of Artificial intelligence has led to emergency of the deepfakes, synthetic media in which a person's voice, or actions are digitally manipulated to appear real. Deepfakes have become a powerful tool for sexual exploitation and psychological abuse raising grave human rights concerns. These systems analyse large sets of images, video or audio recordings to generate highly realistic fake contents. Deepfakes are often used to

- create non-consensual sexual images or videos
- Impersonate individuals for fraud or blackmail
- Spread misinformation or defamatory content¹⁴

Reports mention that around 550 percent increase in deepfake cases have been reported since 2019.65 percent of deepfake cases go unreported. Jamtara 2.0 refers to an advanced evolution of cyber fraud in India, leveraging deepfake technology to target video KYC processes and impersonate individuals, involving over 11 lakh daily KYC video calls.¹⁵

High profile incidents include deepfakes of celebrities like Rashmika Mandana have sparked the harassment concerns. The national cyber-crime reporting portal noted increasing complaints against women in 2025, while a Rati Foundation report revealed a 92 percent of deepfake against women often involving modify apps for extortion and doxing.

Online Grooming - It refers to deliberate and systematic behaviour by an adult who uses digital communication to befriend, emotionally manipulate, and gain the trust of a minor to prepare them for sexual exploitation or abuse. Research shows that the advent of social networking sites, messaging apps, and online gaming has significantly increased opportunities for such

¹³2023:PHHC:056020

¹⁴ Furizal and others, 'Social legal and ethical. Implications of AI generated Deepfake pornography on Digital platforms: A systematic literature review (2025) 12 Social Sciences and Humanities open 101882 <https://doi.org/10.1016/j.ssaho.2025.101882> last visted on June 21,2026

¹⁵ ET Edge Insights, "India to Lose Rs. 70,000 Crore in 2025 Due to Deepfake Fraud: Study", *ET Edge Insights*, Dec. 4, 2024, available at: <https://etedge-insights.com/trending/india-to-lose-rs70000-crore-in-2025-due-to-deepfake-fraud-study> (last visited on Jan. 17, 2026)

predatory behaviour, as offenders can establish anonymous profiles and maintain prolonged contact with children without immediate detection.¹⁶

Studies indicate that between 9% and 19% of minors experience attempts at online grooming, with older adolescents at greater risk due to increased independent internet use and engagement on social platforms. Risk factors associated with grooming victimisation include high screen time, limited parental supervision, emotional vulnerability, and disadvantaged socio-economic backgrounds. The grooming process is typically gradual and non-explicit initially. Predators often begin with harmless conversations to establish rapport and trust, progressively introducing sexually charged content or requests, which can lead to coercion or exploitation. Offenders use coded or indirect language that challenges detection by automated systems and complicates real-time identification.¹⁷

2.2 Why Digital abuse is Gender and age specific

Children and adolescents do not face online grooming risk equally; gender and age significantly influence vulnerability because of developmental and behavioural patterns documented in empirical research. Adolescents are commonly identified as the age group most susceptible to grooming because increased autonomy, identity exploration, and expanding social media use coincide with heightened curiosity about relationships and sexuality, which predators exploit for manipulation and sexual solicitation. Systematic reviews show that older youth, especially those in mid-to-late adolescence, report higher rates of grooming exposure than younger children, likely due to more frequent and unsupervised online interaction.¹⁸ Gender differences also emerge: while both boys and girls are at risk, many studies find girls are targeted more often for sexual solicitations online, reflecting broader patterns in sexual victimisation and behaviours related to online communication.¹⁹ For example, research indicates that among adolescents, girls are more likely to encounter risky solicitations and exploitative contact,

¹⁶ Kim-Kwang Raymond Choo, *Online Child Grooming: A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences* (Australian Institute of Criminology Research and Public Policy Series No. 103, 2009).

¹⁷ Sarah Wefers, [Second Author's Name], *et al.*, "Understanding and Detering Online Child Grooming: A Qualitative Study" *Sex Offending* e13147 (2024).

¹⁸ Juliane A. Kloess, Anthony R. Beech, *et al.*, "Online Child Sexual Exploitation: Prevalence, Process, and Offender Characteristics" 15 *Trauma, Violence & Abuse* 126 (2014).

¹⁹ Kimberly J. Mitchell, David Finkelhor, *et al.*, "Risk Factors for and Impact of Online Sexual Solicitation of Youth" 1 *Journal of Adolescent Health* 116 (2007).

though boys may accept advances at comparable rates in some contexts.²⁰ These patterns suggest that both age-related developmental factors and gendered social dynamics influence how predators select and engage with young people online, making tailored prevention efforts essential.²¹

3. UNDERSTANDING THE HUMAN RIGHTS-BASED APPROACH (HRBA)

An HRBA aims to align policy and practice with international standards grounded in human dignity without discrimination.²² In the context of protection against digital abuse, the approach would be structured as follows:

A. The Core Relationship: Duty-Bearers and Rights-Holders

The HRBA identifies two primary groups:

- **Duty-Bearers:** These are bodies with legal and moral obligations to respect, protect, and fulfil human rights. In a digital context, this would include governments and digital platform providers who must ensure users are protected from harm.
- **Rights-Holders:** These are the individuals guaranteed fundamental rights regardless of race, gender, or religion. The HRBA seeks to empower these individuals to know and claim their rights and to hold duty-bearers accountable for digital violations.²³

B. Participation and Accountability

A central theme of HRBA is that the views and concerns of affected populations must be considered when designing programmes or policies.

- **Accountability:** Organisations and duty-bearers must be held responsible for fulfilling their obligations to prevent harm.

²⁰ Tatiana R. Ringenberg, John D. Lanza, *et al.*, “A Scoping Review of Child Grooming Strategies: Pre- and Post-Internet” 124 *Child Abuse & Neglect* 105392 (2022).

²¹ *Id* at 16

²² Raoul Wallenberg Institute of Human Rights and Humanitarian Law, “What Is a Human Rights Based Approach (HRBA)”, available at: <https://rwi.lu.se/human-rights-based-approach-hrba/> (last visited on Feb. 2, 2026).

²³ *Supra* note 133.

- **Monitoring and Reporting:** A HRBA is used to watch, report, and shed light on human rights violations. In cases of digital abuse, this involves identifying specific rights being violated to create powerful cases for policy change and to put pressure on duty-bearers to take action.

3.1 Applicable international human rights norms

The international human rights framework applicable to digital technologies is anchored in several key instruments, including the Universal Declaration of Human Rights (UDHR), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), and the Convention on the Rights of the Child (CRC). These norms, originally developed for the offline world, apply necessarily to the digital sphere.²⁴ The following sections provide a detailed examination of these norms:

A. Universal Declaration of Human Rights (UDHR)

The UDHR is described as the "normative road map" for the international human rights movement. It serves as a foundation for the legal framework that protects individuals from the abuse of power.

- **Article 19 and Information Flow:** A critical component in the digital age is Article 19, which protects the right to receive and impart information "through any media". The sources affirm that this protection naturally extends to social media and other digital platforms.
- **Adaptation to Technology:** While the 1948 Declaration addressed challenges of its time, such as media access across frontiers and technical education it provides the abstract moral ideas that are now being translated into "digital rights" through modern law-making and interpretation.²⁵

B. Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)

²⁴ International Commission of Jurists, *Digital Technologies and Human Rights: A Legal Framework* (Briefing Paper, May 2022).

²⁵ Yuval Shany, "Digital Rights and the Outer Limits of International Human Rights Law" 24 *German Law Journal* 461 (2023).

CEDAW is a specific treaty containing detailed provisions regarding the non-discrimination of women and girls.

- **Non-Discrimination in Tech:** The observance of non-discrimination is vital in the design and development of artificial intelligence (AI) to ensure that historical biases against women are not reproduced in algorithmic decision-making.
- **Extraterritorial Obligations:** The Committee on the Elimination of Discrimination against Women has made affirmations regarding the extraterritorial application of the Convention. This means states have obligations to ensure that business enterprises under their jurisdiction do not nullify or impair women's rights abroad.²⁶

C. Convention on the Rights of the Child (CRC)

The CRC is frequently cited to address the unique vulnerabilities of children in the digital environment.

- **Rights in the Digital Environment:** A primary standard identified is General Comment No. 25 (2021), which specifically details children's rights in relation to the digital environment. This includes protecting children from being recruited by non-state armed groups through online spaces.
- **Freedom of Association:** The sources explicitly link Article 15 of the CRC, which concerns the right to freedom of association and peaceful assembly, to the positive obligations of states in the digital age.

4. DIGITAL ABUSE AGAINST WOMEN

Gender-based digital abuse against women refers to online harassment, stalking, image-based sexual exploitation, deepfakes, cyberbullying and sextortion that disproportionately target women because of their gender. Globally, about 38 % of women report having personally experienced online violence and 85 % have witnessed it; up to 95 % of deepfake pornographic content targets women, and fewer than 40 % of countries have legal protections against cyber harassment. Women human rights defenders and journalists face especially high abuse, with

²⁶ ET Edge Insights, "India to Lose Rs. 70,000 Crores in 2025" *ET Edge Insights*.

around 70 % reporting online violence and 41 % experiencing related offline attacks. This form of abuse curtails freedom of expression and can have severe psychological impacts.²⁷

Between 16 % and 58 % of women worldwide have experienced some form of technology-facilitated violence such as cyberstalking, harassment or image-based abuse.²⁸

A report from SHE Teams, Hyderabad's women-safety police unit, shows that over 92 % of complaints relate to digital blackmail, often involving harassment, stalking and threats using personal images or intimate content. Multiple arrests were made in cases where victims were harassed by ex-partners, colleagues, or acquaintances via online platforms.²⁹

4.1 Online abuse silences women in politics

A study by the Inter-Parliamentary Union (IPU) across 33 Asia-Pacific countries found that 60 % of women MPs have been targeted with online gender-based violence (hate speech, disinformation, image-based abuse). 76 % reported psychological violence and sexual violence was also common, showing how digital harassment undermines women's political participation.³⁰

UN agencies report that technology-facilitated violence abuse, doxxing, threats and manipulated content is used to silence women leaders, journalists and activists, undermining democratic discourse and press freedom.³¹

Research in India found that about 1 in 7 tweets mentioning women politicians were abusive or problematic, with sexist or misogynistic content discouraging women from engaging

²⁷ Economist Intelligence Unit, "Measuring the Prevalence of Online Violence Against Women" (Economist Intelligence Unit, 2021).

²⁸ UN Women, "AI and Anonymity Fuel Surge in Digital Violence against Women" (Nov. 20, 2025), available at: <https://www.unwomen.org> (last visited on Feb. 11, 2026).

²⁹ "92% of SHE Teams Complaints Linked to Digital Blackmail", *The Times of India*, Feb. 9, 2026, available at: <https://timesofindia.indiatimes.com/city/hyderabad/92-of-she-teams-complaints-linked-to-digital-blackmail/articleshow/128082079.cms> (last visited on June 21, 2026).

³⁰ Inter-Parliamentary Union, "60% of Women MPs in Asia-Pacific Report Online Gender-Based Violence" (Press Release, Mar. 2025), available at: <https://www.ipu.org/news/press-releases/2025-03/60-women-mps-asia-pacific-report-online-gender-based-violence> (last visited on June 21, 2026).

³¹ United Nations Development Programme, "Unite to End Digital Violence against All Women and Girls" (2025), available at: <https://www.undp.org/stories/unite-end-digital-violence-against-all-women-and-girls> (last visited on June 21, 2026).

politically online.³²

In a UNESCO-commissioned global survey of women journalists, 73% experienced online violence, with many reporting psychological impacts; some retreated from visibility, quit jobs or avoided audience engagement because of this abuse.³³

Research shows women report greater fear of online harms and reduced comfort expressing political opinions online compared with men with only ~23–24% of women comfortable posting political views online.³⁴

In the Arab States, 49% of women internet users feel unsafe from online harassment and 12% reported suicidal thoughts related to digital violence showing serious psychological harm and barriers to participation.³⁵

5. DIGITAL ABUSE AGAINST CHILDREN

The digital environment has become an integral part of modern civilisation. While providing greater opportunities for education and social connectivity, it also exposes children to significant risks that many digital technologies were not made to mitigate.³⁶ Approximately one in three internet users worldwide is a child under the age of 18, rendering them a disproportionately vulnerable demographic in the digital space. The dependency on internet was further hastened up by COVID-19 pandemic, leading to increase in digital violence and a 32% increase in cybercrimes against minors between 2021 and 2022.³⁷

³² Shocking scale of abuse on Twitter against women politicians in India' Amnesty International (Press Release, 2018) <https://www.amnestyusa.org/press-releases/shocking-scale-of-abuse-on-twitter-against-women-politicians-in-india/> last visited on june21,2026

³³ International Center for Journalists, "Online Violence, Fuelled by Disinformation and Political Attacks, Deeply Harms Women Journalists" (ICFJ-UNESCO Study, Oct. 12, 2020), available at: <https://www.icfj.org/news/icfj-unesco-study-online-violence-deeply-harms-women-journalists> (last visited on june21, 2026)

³⁴ Francesca Stevens et al, 'Women are Less Comfortable Expressing Opinions Online than Men...' (2024) arXiv

³⁵ United Nations Development Programme, "Empowering Women in the Arab States Region: Raising Awareness on Digital Violence and Building Safer Online Spaces", available at: <https://www.undp.org/arab-states/stories/empowering-women-arab-states-region-raising-awareness-digital-violence-and-building-safer-online-spaces> (last visited on June 21., 2026).

³⁶ Jaya Thapa, "The Protection of Children from Cyber Crimes in India" 6 *International Journal for Multidisciplinary Research (IJFMR)* 22957 (2024).

³⁷ Daniel Manoj, Ranjit Immanuel James, et al., "Behind the Screens: Understanding the Gaps in India's Fight against Online Child Sexual Abuse and Exploitation" 4 *Child Protection and Practice* 100088 (2025).

5.1 Online grooming and sexual exploitation of children

Online grooming is a misleading practice where an adult builds friendship with a child to establish an emotional connection, with an intention to exploit. Exploiters often use social media, gaming websites, and chat rooms to build common interests and build trust with unsuspecting minors. This practice led to the creation and sharing of Child Sexual Abuse Material (CSAM), or "live streaming" where abuse is shared in real-time to remote spectators.³⁸

There is a critical distinction between child sexual abuse and exploitation as sexual exploitation involves a third party benefiting from the activity, often through monetary, social, or political gains. As the term "pornography" inappropriately implies consensual activity, which is never the case for children, the international standards advocate for replacing the term "child pornography" with Child Sexual Exploitation Material (CSEM). In India, the Information Technology Act 2000 (Section 67B) and the POCSO Act 2012 are the primary legislations used to penalise these offences, though gaps remain regarding in-person meetings following online solicitation.³⁹

5.2 AI-facilitated grooming and manipulation

The emergence of AI-driven technology has introduced complex new avenues for digital abuse.⁴⁰ Accusers can now use AI tools to analyse a child's online behaviour and emotional state to tailor highly effective grooming strategies. Deepfake technology allows for the creation of realistic images of children used for sexual extortion.⁴¹

Furthermore, AI-powered recommendation algorithms on social media platforms, designed to maximise views and fame can unintentionally lead children toward dangerous or inappropriate content. Exploiters have also been known to use AI chatbots to simulate human-like conversations to trick children into providing sensitive personal details.

³⁸ UNICEF, *Handbook on Digital Safety for Children* (Internet Safety Alliance for Indians (SAFE) and Cyber Peace Foundation, in collaboration with NCERT).

³⁹ *Id* at 20

⁴⁰ UNICEF, "Protecting Children from Violence and Exploitation in Relation to the Digital Environment".

⁴¹ Vajirao Institute UPSC IAS Current Affairs, "Digital Child Abuse, the Dangers of AI-Based Exploitation & How to Protect Kids" (Apr. 5, 2025), available at: <https://www.vajiraoinstitute.com/upsc-ias-current-affairs/digital-child-abuse-the-danger-of-ai-based-exploitation.aspx> (last visited on Feb. 12, 2026).

5.3 Application of the “best interests of the child” principle

International human rights standards, led by the UN Convention on the Rights of the Child (CRC), dictate that all actions concerning children in the digital environment must be steered by the child's "best interests". This principle requires governments to balance the child's right to protection from violence with their rights to privacy, freedom of expression, and access to information.⁴²

In India, the judiciary has taken active approach to apply this principle by interpreting cyber laws to safeguard children's privacy. For instance, in the case of *Jayesh S. Thakkar v. State of Maharashtra*⁴³, the Bombay High Court established a committee to propose measures for managing minors against offensive online content. Furthermore, the Supreme Court of India has emphasised that the term "child pornography" should be avoided because it belittles the gravity of the crime and the trauma experienced by the child.⁴⁴

6. LEGAL PROTECTION MECHANISM AGAINST DIGITAL ABUSE

Information Technology Act, 2000 (IT Act)

- Section 66E criminalises voyeurism capturing, publishing or transmitting private images without consent (up to 3 years' imprisonment and fine).
- Section 67A prohibits publishing/ transmitting sexually explicit material online without consent (up to 5 years' imprisonment and fine, more for repeat offences).
- Section 67B addresses child sexual abuse material online.⁴⁵

Avni Chaturvedi v. State of Maharashtra (Bombay High Court, 2020)⁴⁶

The court dealt with online bullying through Instagram, including sexualized comments, threats, and sharing of private photos without consent. It invoked IPC Sections 354D (stalking), 509 (modesty), 503/506 (intimidation) and IT Act Section 66E (privacy violations). It

⁴² *Id* at 16.

⁴³ (2009) 7 SCC 104

⁴⁴ *Id* at 20.

⁴⁵ Information Technology Act, 2000.

reinforced the viewpoint that online harassment should be treated with the same gravity as offline harassment.

Kirti Vashisht v. State of Delhi (2019-Delhi High Court)⁴⁷

A revenge-porn case where the accused shared intimate images without consent and malicious intent. The court upheld charges under the IT Act (including Sections 67 & 67A concerning obscene content online) and emphasized significant punishment for non-consensual distribution of sexual material.

Bharatiya Nyaya Sanhita, 2023 (BNS)

- Section 74 criminalises stalking which includes persistent online contact and monitoring.
- Section 77 penalises voyeurism and private image dissemination without consent (revenge porn type conduct).
- Section 78 covers dissemination of private acts/images digitally.⁴⁸

Expansion of Privacy as a Civil Right

After Justice K.S. Puttaswamy v Union of India⁴⁹(2017), privacy was recognised as a fundamental right under Article 21. This judgment strengthened civil claims in digital abuse cases involving

- Non-consensual intimate image sharing
- Deepfake pornography
- Doxing and exposure of personal data

Victims can now seek:

- Injunctions

⁴⁷ 2019 Del 1940.

⁴⁸ Bharatiya Nyaya Sanhita 2023

⁴⁹ (2017) 10 SCC 497.

- Damages for mental trauma
- Protection orders

Research shows that privacy-based civil claims are increasingly being used in technology-facilitated abuse litigation.

UN Women and UNESCO reports show that digital abuse causes:

- Severe psychological harm
- Loss of employment opportunities
- Withdrawal from public participation
- Long-term reputational damage
- Because of these measurable harms, courts increasingly recognise:
- Emotional distress damages
- Reputational damages
- Aggravated damages in cases of sexualised abuse⁵⁰

7. STRUCTURAL AND INSTITUTIONAL FAILURES

The legal landscape surrounding cybercrime in India is currently facing complexities involving jurisdictional, enforcement, and evidentiary challenges. The borderless nature of cyberspace often renders traditional legal principles, designed for physical territories, inadequate for the digital age.

7.1 Jurisdictional Challenges

The primary hurdle in cybercrime adjudication is the "borderless" nature of the internet, which

⁵⁰ UNESCO, "Momentum to Meaningful Change: Addressing Tech-Facilitated Gender-Based Violence" (Jan. 17, 2026), available at: <https://www.unesco.org/en/articles/momentum-meaningful-change-addressing-tech-facilitated-gender-based-violence> (last visited on Feb. 14, 2026).

ignores geographical boundaries. While crimes can be committed in one jurisdiction, the effects are often felt in another, leading to significant conflicts of laws.⁵¹

- **Territoriality vs. Effects Doctrine:** Indian courts have attempted to navigate this through different interpretations. For instance, in *State of Maharashtra vs. Sandeep Atre*, the court asserted jurisdiction over a foreign-hosted website because the crimes effects were felt in India. Conversely, in *Google Inc. vs. Equustek Solutions Inc.*, the Delhi High Court refused to enforce a global removal order, citing concerns over territorial jurisdiction and freedom of speech.⁵²
- **Data Sovereignty and MLATs:** Data is often stored on servers located in foreign countries, placing it outside the reach of Indian law. Obtaining such evidence through Mutual Legal Assistance Treaties (MLATs) is often described as lengthy, slow, and bureaucratic process, which can lead to the loss of critical, volatile evidence.⁵³
- **Emerging Technologies:** Technologies like cloud computing and blockchain further complicate jurisdiction as they distribute data across multiple virtual and physical locations, making it difficult to determine which laws apply.⁵⁴

7.2 Enforcement Challenges

Enforcing cyber laws is hindered by a significant expertise gap and infrastructural limitations within law enforcement and judicial bodies.

- **Resource Constraints:** Many local law enforcement agencies are the first responders but they lack manpower and limited budgets, and outdated technology. There is a noted shortage of dedicated cybercrime cells, especially in rural and semi-urban areas.⁵⁵
- **Technical Barriers:** The widespread use of end-to-end encryption (e.g., on WhatsApp

⁵¹ Srinivas Katkuri, "Legal Challenges and Lacunas in the Digital Forensics Jurisprudence in India" 10(3) *International Journal of Law* 23–29 (2024).

⁵² Ishan Atrey, "Cybercrime and Its Legal Implications: Analysing the Challenges and Legal Frameworks Surrounding Cybercrime, Including Issues Related to Jurisdiction, Privacy, and Digital Evidence" 10(3) *International Journal of Research and Analytical Reviews* 245 (2023).

⁵³ M.K. Sil, "Jurisprudential Challenges in Cybercrime Adjudication" (Presentation, Apr. 25, 2025).

⁵⁴ Francesca, "Women are Less Comfortable Expressing Opinions Online than Men", available at: [URL] (last visited on Feb. 13, 2026).

⁵⁵ Meenakshi Tyagi, T.N.V.R. Swamy, et al., "Digital Evidence and Local Law Enforcement: Challenges in Cybercrime Prosecution" 2(5) *Advances in Consumer Research* (2025).

or Signal) creates significant barriers for investigators attempting to access lawful evidence. Additionally, the rapid evolution of technology, such as AI-driven deepfakes, often outpaces the development of legislative frameworks.⁵⁶

8. INTERSECTIONAL AND SOCIO LEGAL DIMENSIONS

- Digital abuse is not experienced uniformly; rather, it reflects and reproduces existing structural inequalities of caste, class, sexuality and political marginalisation. Kimberlé Crenshaw's theory of intersectionality explains how multiple identities, such as gender combined with race, caste or sexuality create compounded forms of discrimination that cannot be understood in isolation.⁵⁷
- In the digital sphere, this means that marginalised women often face layered harassment: sexist abuse combined with casteist slurs, homophobic threats, or communal targeting. Scholars argue that online violence mirrors offline hierarchies, transforming cyberspace into a site of structural domination rather than neutral participation.⁵⁸ Importantly, intersectional identities increased vulnerability: women belonging to ethnic, racial or religious minorities reported more severe and coordinated abuse.⁵⁹
- In India, caste-based abuse has increasingly moved online, with Dalit and Adivasi women facing targeted humiliation, threats of sexual violence framed through caste dominance, and circulation of morphed or degrading images. Research by Equality Labs on online harassment in India found that caste-oppressed communities, particularly Dalit women, experience organised digital harassment campaigns.⁶⁰
- Sexual minorities face similar digital targeting. The UN Special Rapporteur on violence against women has recognised technology-facilitated violence as disproportionately

⁵⁶Saumya Deep Singh and Shirsh Pandey, "The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws" *International Journal for Multidisciplinary Research*.

⁵⁷ Kimberlé Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color" 43 *Stanford Law Review* 1241 (1991).

⁵⁸ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, Cambridge, MA, 2014).

⁵⁹ Julie Posetti, Nabeelah Shabbir, Kalina Bontcheva, et al., *The Chilling: Global Trends in Online Violence against Women Journalists* (UNESCO, 2020), available at: <https://unesdoc.unesco.org/ark:/48223/pf0000375136> (last visited on june21, 2026).

⁶⁰ Equality Labs, *Caste in the Digital Sphere: A Study of Online Harassment in India* (2019), available at: <https://www.equalitylabs.org/casteinthetech> (last visited on june21, 2026).

affecting women and LGBTQ+ persons, particularly through outing, doxxing and image-based abuse.⁶¹

9. RIGHTS-BASED SOLUTIONS AND LEGAL REFORMS

Addressing digital abuse in India requires a multi-pronged approach involving legislative updates, institutional improvements, and increased accountability for digital platforms. The sources highlight that while current laws provide some protection, they are often inadequate for modern digital harms like AI-generated deepfakes and anonymous trolling.⁶²

9.1 Legislative Reforms

To close existing legal gaps, the following recommendations are given:

- Enacting a Specific Cyberbullying Act: India currently lacks a cohesive, inclusive law that explicitly targets cyberbullying and digital abuse. A dedicated act could provide a more clear definitions for online harassment, trolling, and the non-consensual sharing of digital content.⁶³
- Updating the Bharatiya Nyaya Sanhita (BNS) and IT Act: Reforms should integrate gender-sensitive provisions into the BNS to address harms such as doxxing, cyberstalking, and deepfakes. The National Commission for Women (NCW) suggests digital laws should explicitly penalise AI-generated content used for intimidation.⁶⁴
- Redefining Child Exploitation: The Supreme Court has called for replacing the term "child pornography" with "Child Sexual Exploitation and Abuse Material" (CSEAM) in the POCSO Act to reflect the abusive nature of the content rather than implying it is a category of entertainment.⁶⁵

⁶¹ UN Human Rights Council, *Report of the Special Rapporteur on Violence against Women, its Causes and Consequences on Online Violence against Women and Girls*, UN Doc A/HRC/38/47 (2018), available at: <https://undocs.org/A/HRC/38/47> (last visited on June 21, 2026).

⁶² Pallavi Gupta and Amrita, 'Digital Abuse and Legal Silence: Addressing Cyberbullying through Indian Law' (2025) 5(4) *International Journal of Advanced Legal Research*.

⁶³ *Supra* note 62.

⁶⁴ NCW *Cyber Law Reforms for Women Protection: Bharatiya Nyaya Sanhita, 2023* (The420, 23 January 2024) <https://the420.in/ncw-cyber-law-reforms-women-protection-bharatiya-nyaya-sanhita-2023/> (last visited on June 21, 2026)

⁶⁵ *Id.* at 50.

- The "Right to Be Forgotten": Introducing a legal right for victims to request the permanent removal of their private data or images from the internet is suggested as a powerful tool to help victims regain their dignity.⁶⁶

9.2 Institutional and Enforcement Solutions

Strengthening the practical response of law enforcement is essential for effective justice:

- Specialised Cyber Units: Establishing women-focused cyber cells in every district, staffed by trained female officers, would create a more sensitive environment for reporting. This includes appointing district-level psychologists and forensic experts to support victims.⁶⁷
- Fast-Track Courts: Similar to rape cases, creating fast-track courts for cyber offences would ensure timely justice and build public trust in the legal system.
- Victim Compensation and Support: Proposals include creating a mandatory victim compensation fund and ensuring strict confidentiality for complainants to encourage reporting and mitigate social stigma.
- Improved Stakeholder Coordination: Enhanced information sharing between police, technology companies, and child welfare organisations is necessary to track offenders across borders.

9.3 Digital Platform and Technical Reforms

We also advocate for shifting more responsibility onto social media intermediaries:

- Stricter Content Takedowns: Platforms should be legally mandated to remove objectionable content violating a person's dignity within 24 to 48 hours, with the NCW specifically recommending a 36-hour window.
- Real-Time Monitoring: Intermediaries should be required to deploy AI and machine learning tools for the real-time detection and deletion of child sexual abuse material

⁶⁶ *Id.* at 7.

⁶⁷ *Id.* at 51.

(CSAM).

- Increased Data Retention: Extending data retention requirements to 360 days would better assist law enforcement in investigating digital crimes that might otherwise leave no trace.
- Platform Accountability: Laws should extend liability to platforms that fail to act on reported abuse, including mandatory AI audits to verify manipulated imagery.⁶⁸

10. CONCLUSION

Digital spaces have transformed communication, education and participation, but they have also created new avenues for abuse, exploitation and technology-facilitated violence, particularly against women and children. Digital abuse, cyberbullying, online grooming, image-based violence and data misuse demonstrate how online harms can undermine dignity, privacy and equality. As digital interaction becomes inseparable from everyday life, ensuring online safety is no longer optional but a fundamental rights concern. Effective responses require gender-sensitive laws, child-centred safeguards, platform accountability, digital literacy and ethical AI governance. Protecting human rights in digital environments is essential to ensuring that technological advancement promotes empowerment rather than harm.

⁶⁸ *Id.* at 38.

BIBLIOGRAPHY

1. Johni Eka Putra, Dedah Ningrum and Al-Afandi, 'Transforming Public Spaces in the Digital Age: How Technology Changes the Face of Social Interaction' (2024) 2(10) *International Journal of Society Reviews* 2711–2724
2. Syed Faraz Akhtar and Moumita Datta Bhowmik, 'Digital Violence: The Rise of Online Gender-Based Violence Against Women in the Age of Social Media' *International Journal for Multidisciplinary Research (IJFMR)*.
3. Swarupa Dholam and Aditi Sawant, 'The Impact of Cybercrime on Human Rights' (2025) 3(1) *International Journal of Legal Studies and Social Sciences* 488–514.
4. Tatiana Tropina, "'This Is Not a Human Rights Convention": The Perils of Overlooking Human Rights in the UN Cybercrime Treaty' (2024) 9(2) *Journal of Cyber Policy* 200.
5. Kim-Kwang Raymond Choo, *Online Child Grooming: A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences* (Australian Institute of Criminology Research and Public Policy Series No 103, 2009).