

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Safeguarding Digital Vulnerabilities: A Socio-Legal Examination of Cyber Violence Against Women and Children within India's Contemporary Penal Framework

SUMI S. SHAJI*

ABSTRACT

India's rapid transition to online life after the COVID-19 pandemic has made communication and services easier while also creating new ways in which women and children are harmed through the internet. Official reports and academic work record a rise in cyber offences such as online stalking, non-consensual sharing of intimate images, child sexual abuse material, online grooming and bullying, with offenders using fake identities, foreign-based platforms and encryption to conceal themselves while harmful content spreads rapidly across social-media and messaging services. Adopting a doctrinal method, this article reads together the Information Technology Act 2000 (as amended), the Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita, and the Protection of Children from Sexual Offences Act. It first classifies forms of cyber violence against women, including cyberstalking, revenge pornography, morphing and deepfakes, sextortion, gendered trolling and fake profiles, and examines practical problems such as anonymity, viral circulation of intimate content and weak platform regulation. It then turns to cyber offences against children, focusing on child sexual abuse material, online grooming, cyberbullying, self-generated sexual images, gaming-related exploitation and dangerous viral challenges, and explains how section 67B of the Information Technology Act, key provisions of the Protection of Children from Sexual Offences Act and the 2020 Rules operate together. A separate section examines the roles of the Indian Cyber Crime Coordination Centre, the National Cyber Crime Reporting Portal and state-level cyber units in building a coordinated institutional response. The article finally proposes reforms including specialised cyber-Protection of Children from Sexual Offences courts, stronger digital-forensic capacity, clearer platform duties, better cross-border cooperation and sustained digital-literacy campaigns, so that technology and law together can create a more secure, zero-tolerance online environment for women and children.

Keywords: Social media, online gaming, CSAM, cybercrime, deepfake, digital forensics, intermediary liability, Information Technology Act 2000, online grooming, POCSO Act.

* Author is an LL.M. student at the School of Indian Legal Thought, Mahatma Gandhi University, Kottayam, Kerala, India.

I. INTRODUCTION

The rapid expansion of digital technology in India since 2020 has deeply affected the way in which individuals communicate, work, study and seek entertainment. It has also created new environments in which women and children are exposed to serious forms of online harm. Courts and scholars have noted that offences such as cyberstalking, circulation of intimate images, child sexual abuse material, online grooming and bullying are no longer exceptional incidents but part of the everyday landscape of criminal justice in the country. This shift has forced judges, police and policymakers to reconsider how traditional principles of criminal law, privacy and free speech should apply in the networked environment. In particular, the case of *Shreya Singhal v. Union of India*, which invalidated section 66A of the Information Technology Act for infringing upon the right to freedom of speech and expression, shows how closely questions of online safety are tied to constitutional guarantees in the digital age.¹

The statutory foundation for understanding these harms lies in the core definitions in section 2 of the Information Technology Act 2000. The Act defines a "computer" as any electronic, magnetic, optical or other high-speed data-processing device which performs logical, arithmetic and memory functions and includes related input, output, storage and communication facilities, while a "computer network" refers to the interconnection of one or more such computers or communication devices through various media.² These broad, technology-neutral definitions enable the law to reach a wide range of devices and platforms, from smartphones and laptops to social-media services and encrypted messaging applications, thereby establishing the legal basis for prosecuting cyber offences affecting women and children.³ Commentaries on cyber law indicate that these provisions were drafted in broad terms so that the statute would remain relevant amid rapid technological advancement.⁴

Against this legal background, the present article focuses on two particularly vulnerable groups in the Indian digital ecosystem: women and children. It argues that a separate, detailed analysis of cyber offences against women and cyber offences against children is necessary because, although both sets of victims face overlapping risks such as image-based abuse and online harassment, the social context, power dynamics and applicable legal frameworks differ in important ways. For example, while cases like *Avnish Bajaj v. State (NCT of Delhi)* highlight

¹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

² Information Technology Act, 2000, ss. 2(1)(i), 2(1)(j), No. 21 of 2000 (India).

³ *Id.*

⁴ Pavan Duggal, CYBERLAW: THE INDIAN PERSPECTIVE (5th edn, 2020).

the challenges of intermediary liability and obscene online content,⁵ child-centric operations, such as the Kerala Police's "Operation P-Hunt", show how law-enforcement agencies now use specialised tools to detect and dismantle networks trading in child sexual abuse material.⁶ Together, these strands of practice indicate that a generic, universal approach to cybercrime policy is no longer sufficient.

Methodologically, the article adopts a doctrinal approach based on a close reading of the Information Technology Act, the Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita, the Protection of Children from Sexual Offences Act and allied rules, and leading judicial decisions in the fields of cyber law and child protection. This legal analysis is supported by a careful use of National Crime Records Bureau data on cyber offences against women and children, used not to overload the argument with numbers but to illustrate broad trends and enforcement gaps.⁷ The introduction lays down the conceptual and legal framework; the next part maps specific categories of cyber offences against women and examines their treatment under the Information Technology Act, penal law and the intermediary-liability regime; the following part undertakes a parallel exercise for cyber offences against children under the Information Technology Act and the Protection of Children from Sexual Offences Act; a later section analyses the role of central and state cybercrime units and special operations; and the final part offers a set of reform proposals aimed at building an integrated, gender- and child-sensitive cybercrime response for the Indian digital age.

II. CYBER CRIMES AGAINST WOMEN

The move to a digital-first society has given women new spaces for work, study and expression, but it has also reproduced old patterns of gendered violence in new, technology-mediated forms.⁸ Online abuse rarely occurs in isolation: it often overlaps with domestic violence, workplace harassment and street-level abuse, so that the same woman may face threats, sexualised trolling and image-based extortion across multiple platforms.⁹ Indian law therefore relies on a combination of special and general statutes, the Information Technology Act 2000, the Indian Penal Code and now the Bharatiya Nyaya Sanhita, together with evidence and procedure rules, to frame charges in a way that captures both the digital tools used and the underlying gender-based harm.¹⁰

⁵ *Avnish Bajaj v. State (NCT of Delhi)*, 2005 SCC OnLine Del 1362.

⁶ 'Operation P-Hunt: Techies among 41 Arrested in Kerala', TIMES OF INDIA (28 December 2020).

⁷ National Crime Records Bureau, CRIME IN INDIA 2023 (Government of India 2024).

⁸ Duggal, *supra* note 4; Debarati Halder and K. Jaishankar, CYBER CRIME AND THE VICTIMISATION OF WOMEN: LAWS, RIGHTS AND REGULATIONS (2011).

⁹ Halder and Jaishankar, *supra* note 8.

¹⁰ Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India).

A. Typology of specific cyber crimes against women

B. Cyberstalking

Cyberstalking usually involves repeated, unwanted online contact or surveillance of a woman through social media, messaging apps, emails or tracking tools, often accompanied by threats or attempts to control her movements.¹¹ Academic studies on cyberstalking indicate that such behaviour can be as intrusive and terrifying as physical stalking, because the victim feels a sense of surveillance even within private digital spaces.¹² Courts in India have therefore begun to treat sustained online monitoring and harassment as a serious infringement of dignity and privacy rather than a minor inconvenience. In *Jayaprakash P.P. v. Sheeba Revi*, the Kerala High Court examined the ingredients of section 354D of the Indian Penal Code and reaffirmed that persistently contacting or attempting to contact a woman repeatedly without her consent, through electronic means, may amount to stalking when it fosters personal interaction despite a clear indication of disinterest.¹³

After *Shreya Singhal v. Union of India*, which struck down section 66A of the Information Technology Act as unconstitutional for its vague and overbroad language,¹⁴ prosecutions for cyberstalking have shifted to section 354D of the Indian Penal Code and its successor provision in section 78 of the Bharatiya Nyaya Sanhita, which specifically criminalise stalking, including monitoring a woman's use of the internet, email or other electronic communication.¹⁵ In practice, police often add general Information Technology Act provisions, such as section 66 for unauthorised access or misuse of credentials, alongside section 354D and section 78 of the Bharatiya Nyaya Sanhita, so that the charge-sheet reflects both the gendered nature of the offence and the misuse of computer resources.¹⁶ A major investigative challenge is that stalkers frequently use virtual private networks, foreign-based platforms or disposable accounts, which makes it harder to identify the real IP address and link it to the accused.¹⁷ Police cyber cells and initiatives such as the Kerala Police's Cyberdome use log analysis, platform responses and correlation of device identifiers to pierce this anonymity, which is reflected in the technical evidence annexed to the charge-sheet.¹⁸

¹¹ Duggal, *supra* note 4.

¹² Duggal, *supra* note 4.

¹³ *Jayaprakash P.P. v. Sheeba Revi*, 2017 SCC OnLine Ker 21544.

¹⁴ *Shreya Singhal*, *supra* note 1.

¹⁵ Bharatiya Nyaya Sanhita, 2023, s. 78 (India).

¹⁶ Information Technology Act, 2000, s. 66 (India).

¹⁷ National Crime Records Bureau, STANDARD OPERATING PROCEDURE FOR INVESTIGATION OF CYBER CRIMES (2024); K. Jaishankar, CYBER CRIMINOLOGY: EXPLORING INTERNET CRIMES AND CRIMINAL BEHAVIOUR (2011).

¹⁸ 'Operation P-Hunt', *supra* note 6.

C. Cyber pornography and "revenge porn"

Cyber pornography and so-called "revenge porn" cover a wide range of activities, from uploading intimate images without consent to running subscription-based sites or messaging groups where women's bodies are commodified and traded.¹⁹ Sections 67 and 67A of the Information Technology Act penalise publishing or transmitting obscene material and sexually explicit content in electronic form,²⁰ while section 292 of the Indian Penal Code and its successor section 294 of the Bharatiya Nyaya Sanhita address the sale and distribution of obscene material more generally.²¹ In serious cases, prosecutors combine these provisions so that the Information Technology Act sections capture online publication and storage, while the Indian Penal Code and Bharatiya Nyaya Sanhita provisions address broader concerns of obscenity raised by the victim's family or community.²² Older obscenity jurisprudence, such as *Sakal Papers (P) Ltd. v. Union of India*, is sometimes cited to balance free speech with decency and public order, even though it arose in a print-media context, to show that reasonable restrictions on expression have long been recognised.²³

From an enforcement perspective, the primary challenge is the speed and scale at which intimate images can spread once uploaded, often being copied into multiple chat groups and mirror sites before the survivor realises what has happened.²⁴ *State of Tamil Nadu v. Suhas Katti*, which involved a fake email account and obscene messages about a divorced woman in a Yahoo group, is often cited as the first conviction under section 67 of the Information Technology Act and illustrates how humiliation can be amplified by online circulation.²⁵ National mechanisms such as the National Cyber Crime Reporting Portal, which has a dedicated flow for complaints relating to women, and the National Commission for Women's online complaint system, are used to generate takedown requests that can be attached to the first information report and later produced in court to demonstrate prompt action.²⁶ These portals, read with the due-diligence obligations under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, help prosecutors argue that platforms must act quickly on non-consensual intimate-image complaints and preserve logs that can link the first uploader to the offence.²⁷

¹⁹ Information Technology Act, 2000, s. 67A (India).

²⁰ *Id.* s. 67.

²¹ Bharatiya Nyaya Sanhita, 2023, s. 294 (India).

²² *Id.*

²³ *Sakal Papers (P) Ltd. v. Union of India*, AIR 1962 SC 305.

²⁴ Duggal, *supra* note 4.

²⁵ *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004 (Egmore Magistrate 2004).

²⁶ Indian Cyber Crime Coordination Centre, Ministry of Home Affairs.

²⁷ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b) (India).

D. Morphing and deepfake videos

Morphing and deepfakes involve altering a woman's images or voice, often using artificial-intelligence tools, so that she appears nude, engaged in sexual activity or making statements she never actually made.²⁸ Here, section 66E of the Information Technology Act combines with section 67 on obscene material, and with general penal provisions on criminal intimidation and insult to modesty where threats or public shaming are involved.²⁹ Commentators such as Pavan Duggal argue that these provisions, though drafted before modern generative artificial intelligence, are broad enough to cover synthetic images because what matters is the effect on privacy and dignity, not whether the underlying pixels are "real".³⁰ Academic work on deepfakes similarly stresses the need to adapt existing privacy and obscenity doctrines rather than wait for entirely new offences to be created.³¹

The government has also relied on subordinate legislation and executive directions under the Information Technology Act, especially the Information Technology Rules 2021 and subsequent advisories, to require platforms to remove morphed or deepfake content within short timelines and to deploy automated tools for detecting previously flagged material.³² Recent public-interest litigation in the Delhi High Court over sexually explicit deepfakes has sought interim directions requiring social-media intermediaries to identify and take down such content once notified, while preserving logs that can help identify the first originator; such proceedings illustrate how an injunction remedy can sit alongside criminal prosecution.³³

E. Sextortion and online blackmail

Sextortion cases involve an accused threatening to publish a woman's intimate images or chats unless she pays money, provides further sexual content or agrees to meet in person.³⁴ In legal terms, such incidents are generally classified as extortion under section 384 of the Indian Penal Code or its counterpart in section 308 of the Bharatiya Nyaya Sanhita, along with relevant provisions of the Information Technology Act where computer resources have been misused, and they may also invoke provisions on insult to modesty or criminal intimidation when the threats are explicitly sexual. Courts have treated the use of screenshots and video calls to manipulate and solicit favours from women as a significant violation of trust and privacy, rather

²⁸ Duggal, *supra* note 4.

²⁹ Information Technology Act, 2000, s. 66E (India).

³⁰ Duggal, *supra* note 4.

³¹ *Id.*.

³² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

³³ *Chaitanya Rohilla v. Union of India*, W.P. (C) 15596/2023 (Delhi HC) (pending PIL seeking regulation of deepfakes).

³⁴ Bharatiya Nyaya Sanhita, 2023, s. 308 (India).

than simply a "private dispute", and have emphasised that the resulting humiliation can have enduring effects, even in the absence of any financial transaction.³⁵ High Courts have also indicated that merely labelling such incidents as "relationship issues" does not, by itself, provide sufficient grounds to quash a first information report where there is clear material showing threats to circulate intimate content.³⁶

From the investigative perspective, sextortion has evolved from simple bank-transfer demands to more complex methods involving prepaid wallets and cryptocurrency, making the money harder to trace.³⁷ The Indian Cyber Crime Coordination Centre has responded by building technical capacity for blockchain analysis and training state cyber cells to track money transfers across exchanges and wallets. This forensic trail is increasingly cited in charge-sheets to link the suspect device, chat handles and financial accounts. Parallel awareness campaigns by police and women's commissions urge victims to lodge complaints early and to avoid deleting chats or images, so that digital evidence can be preserved in a forensically sound manner.³⁸

F. Cyber harassment and gendered trolling

Cyber harassment and gendered trolling refer to sustained campaigns of abuse, threats, doxxing and sexualised comments aimed at women, often targeting journalists, activists or students, because of their gender or viewpoints.³⁹ Previously, section 66A of the Information Technology Act was used to address "offensive" messages; however, its striking down in *Shreya Singhal* has pushed law-enforcement agencies to rely on section 67 of the Information Technology Act for obscene content, section 509 of the Indian Penal Code and section 79 of the Bharatiya Nyaya Sanhita for words or gestures intended to insult a woman's modesty, alongside general provisions on criminal intimidation.⁴⁰ In practice, charge-sheets often bundle multiple abusive posts from the same handle and treat them as part of one continuing course of conduct, to show a pattern of misogyny rather than isolated bad language.⁴¹ *Pawan Kumar v. State of Himachal Pradesh*, though not a pure cyber case, is frequently cited to emphasise that persistent harassment and humiliation, especially of young women, can have grave psychological effects and must be taken seriously by courts.⁴²

³⁵ *Id.*

³⁶ 'High Court Refuses to Quash FIR in Sextortion Case', TIMES OF INDIA (2023).

³⁷ Indian Cyber Crime Coordination Centre, *supra* note 26.

³⁸ *Id.*

³⁹ Duggal, *supra* note 4; Centre for Communication Governance, GENDERED DIMENSIONS OF ONLINE HARASSMENT IN INDIA (2024).

⁴⁰ Bharatiya Nyaya Sanhita, 2023, s. 79 (India).

⁴¹ *Id.*

⁴² *Pawan Kumar v. State of Himachal Pradesh*, (2017) 7 SCC 780.

The Information Technology Rules 2021 attempt to address this problem structurally by placing due-diligence duties on intermediaries: they must publish clear terms of use, remove certain categories of non-consensual sexual content within twenty-four hours of receiving a complaint, and appoint grievance officers who can coordinate with law enforcement.⁴³ For women facing mass trolling, these rules provide an additional civil-regulatory layer: a survivor can demand that platforms take down abusive threads and disclose basic subscriber information or IP logs under due process, while the police simultaneously pursue criminal charges under the Indian Penal Code, the Bharatiya Nyaya Sanhita and the Information Technology Act.⁴⁴ Scholars argue that this layered approach, combining platform accountability, criminal law and support services, offers a more realistic route to tackling gendered online abuse than relying on criminal sanctions alone.⁴⁵

G. Online impersonation and fake profiles

Online impersonation occurs when someone creates accounts in a woman's name or using her photographs, often to post sexual content, solicit money or damage her reputation.⁴⁶ Sections 66C and 66D of the Information Technology Act address identity theft and cheating by personation using computer resources⁴⁷ and are commonly combined with provisions on cheating, forgery and insult to modesty under the Indian Penal Code and Bharatiya Nyaya Sanhita when fake profiles are used to lure third parties or circulate obscene content.⁴⁸ Courts have held that using another person's name and images to create social-media accounts can amount to cheating by personation, even where no direct financial loss is shown, because it undermines the victim's control over her identity and damages her dignity. Cases involving matrimonial disputes and workplace feuds have also shown how fake profiles can be used to send abusive messages to colleagues or relatives, thereby extending reputational harm beyond the original online space.⁴⁹

Investigations generally begin with platform responses that link the fake profile to a particular device or IP address, which are then cross-checked with subscriber records from internet service providers and telecom companies.⁵⁰ Gaps in SIM and device verification, and the availability of cheap pre-activated connections, make this process difficult, which is why many policy

⁴³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3 (India).

⁴⁴ *Id.*

⁴⁵ Duggal, *supra* note 4.

⁴⁶ Information Technology Act, 2000, s. 66C (India).

⁴⁷ *Id.* s. 66D.

⁴⁸ Bharatiya Nyaya Sanhita, 2023, s. 319 (India).

⁴⁹ *Id.*

⁵⁰ Indian Cyber Crime Coordination Centre, *supra* note 26.

proposals call for stronger know-your-customer norms and better record-keeping by intermediaries and telecom operators, especially for features such as end-to-end encrypted messaging and ephemeral content.⁵¹ At the same time, civil-society groups caution that any move towards strict identity linkage must be balanced against privacy and free-speech concerns, particularly for women who use pseudonyms to escape offline harassment.⁵²

H. Statutory framework and judicial precedents

The legal response to cyber crimes against women weaves together special law (the Information Technology Act), general penal law (the Indian Penal Code and Bharatiya Nyaya Sanhita) and procedural law (the Code of Criminal Procedure and the Bharatiya Nagarik Suraksha Sanhita), with older specialised statutes such as the Immoral Traffic (Prevention) Act 1956 stepping in where online spaces are used to facilitate traditional offences like trafficking or prostitution.⁵³ In many charge-sheets, prosecutors frame both Information Technology Act and Indian Penal Code or Bharatiya Nyaya Sanhita offences for the same course of conduct, for example section 67 of the Information Technology Act along with section 292 or 509 of the Indian Penal Code, arguing that the Information Technology Act provisions capture the use of computer resources while the penal-code provisions address the underlying obscenity, insult or threat.⁵⁴ Section 81 of the Information Technology Act gives the statute an overriding effect over inconsistent laws, but courts have generally allowed parallel charges as long as there is no double punishment, which preserves flexibility at the trial stage.⁵⁵

Procedurally, the gradual shift from the Code of Criminal Procedure to the Bharatiya Nagarik Suraksha Sanhita has sought to respond to the digital nature of these offences.⁵⁶ Provisions of the Bharatiya Nagarik Suraksha Sanhita on electronic first information reports, electronic service of summons and time-bound investigation, together with amendments on electronic records, are meant to reduce delays that previously discouraged women from reporting online abuse.⁵⁷ At the same time, the rules on admissibility of electronic evidence, including certificate requirements, hash values and chain-of-custody, remain crucial: without proper documentation of how screenshots, device images and server logs were collected, defence counsel can challenge the authenticity of key exhibits.⁵⁸ Digital-forensics experts in India have repeatedly

⁵¹ *Id.*; N.S. Nappinai, TECHNOLOGY LAWS DECODED (2017).

⁵² *Shreya Singhal*, *supra* note 1.

⁵³ Immoral Traffic (Prevention) Act, 1956, No. 104 of 1956 (India).

⁵⁴ Information Technology Act, 2000, s. 81 (India); Prashant Mali, CYBER LAW AND CYBER CRIMES (3rd edn, 2020).

⁵⁵ *Id.*.

⁵⁶ Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023 (India).

⁵⁷ *Id.* s. 173.

⁵⁸ Bharatiya Sakshya Adhiniyam, 2023, s. 63, No. 47 of 2023 (India).

emphasised that poor handling of devices at the police-station level is one of the main reasons why otherwise strong cyber cases collapse at trial.⁵⁹

Case law illustrates how these statutes interact in practice. In *Shreya Singhal v. Union of India*, the Supreme Court clarified that while vague provisions like section 66A cannot be used to criminalise "grossly offensive" speech, narrowly drafted obscenity and defamation provisions can still apply where women face serious harm.⁶⁰ In *Avnish Bajaj v. State (NCT of Delhi)*, the Delhi High Court examined the liability of an online-marketplace executive for obscene video clips uploaded by a user, interpreting sections 67 and 85 of the Information Technology Act and foreshadowing later debates on intermediary liability in the platform era.⁶¹ More recent High Court judgments involving social-media abuse in family and neighbourhood disputes have highlighted the need for sensitive, victim-centred handling of digital evidence and have warned against both over-criminalisation of everyday quarrels and under-protection of women facing genuine online threats.⁶²

The Immoral Traffic (Prevention) Act becomes relevant where online advertisements, messaging groups or classified sites are used to solicit customers for sexual exploitation.⁶³ Courts have recognised that websites or chat groups can act as virtual brothels, and prosecutors therefore sometimes combine provisions of the Immoral Traffic (Prevention) Act on procuring and soliciting with Information Technology Act sections on publication and transmission, especially when minors are involved.⁶⁴ Academic writing on cyber violence against women in India argues that this multi-statute strategy, though complex, reflects the lived reality that digital tools are simply new means for committing old forms of gendered oppression.⁶⁵

I. Challenges and evolving responses

Despite the growing body of law and practice, many women still hesitate to report cyber offences because of fear of stigma, victim-blaming and disbelief, especially where intimate images or romantic relationships are involved.⁶⁶ Helplines and online complaint systems run by the National Commission for Women, state commissions and the national cybercrime portal aim to lower this barrier by allowing women to file complaints from home, choose whether to

⁵⁹ Duggal, *supra* note 4; Vakul Sharma and Seema Sharma, INFORMATION TECHNOLOGY LAW AND PRACTICE (7th edn, 2022).

⁶⁰ *Shreya Singhal*, *supra* note 1.

⁶¹ *Avnish Bajaj*, *supra* note 5.

⁶² 'High Court Refuses to Quash FIR in Sextortion Case', *supra* note 36.

⁶³ Immoral Traffic (Prevention) Act, 1956, *supra* note 53.

⁶⁴ *Id.*.

⁶⁵ Duggal, *supra* note 4.

⁶⁶ National Crime Records Bureau, *supra* note 7.

reveal their identity, and receive basic legal information before approaching a police station.⁶⁷ These mechanisms, together with women-facilitated help desks and special units in metropolitan police forces, are slowly shifting the narrative from "why did you share those images?" to "why did the accused misuse your trust?"

Operationally, large-scale enforcement drives have shown both the potential and the limits of technology-driven policing. Periodic operations by metropolitan police forces, sometimes branded under names such as "Cyber Tandav", have involved coordinated raids, mass arrests and seizure of devices in cases of online harassment, sextortion and circulation of obscene material targeting women.⁶⁸ These operations rely heavily on technical surveillance, data analytics and cooperation with platforms, but they also highlight capacity constraints: forensic labs struggle with backlogs, specialist cyber units are overstretched, and district police often lack training in handling digital evidence and speaking to traumatised survivors.⁶⁹

At a policy level, central schemes such as the Cyber Crime Prevention against Women and Children scheme, the Indian Cyber Crime Coordination Centre architecture and the Information Technology Rules 2021 seek to create an integrated ecosystem where law enforcement, regulators, platforms and civil-society groups share responsibility for making online spaces safer.⁷⁰ Scholars emphasise that legal reforms must be matched by digital-literacy campaigns, gender-sensitive training for police and prosecutors, and accessible victim-support services if women are to experience the internet as a space of freedom rather than fear.⁷¹ In this sense, cyber law, criminology and gender justice all converge on the same point: without sustained investment in institutions and attitudes, the promise of the digital age will remain unequally shared between men and women.

III. CYBER CRIMES AGAINST CHILDREN

A. Types of cyber crimes against children

B. Child sexual abuse material

Child sexual abuse material, now increasingly described in legal and policy writing as child sexual exploitation and abuse material, denotes visual or digital content that records, depicts or circulates the sexual abuse of children.⁷² In Indian law, this form of abuse is not treated as mere

⁶⁷ Indian Cyber Crime Coordination Centre, *supra* note 26.

⁶⁸ 'Cyber Tandav: Delhi Police Crack Down on Sextortion Rackets', TIMES OF INDIA (15 March 2024).

⁶⁹ National Crime Records Bureau, *supra* note 7.

⁷⁰ Indian Cyber Crime Coordination Centre, *supra* note 26.

⁷¹ Duggal, *supra* note 4.

⁷² Protection of Children from Sexual Offences Act, 2012, s. 13, No. 32 of 2012 (India); UNICEF, CHILD SEXUAL ABUSE MATERIAL: A GUIDE FOR POLICY MAKERS (2023).

obscenity. It is treated as a distinct and aggravated wrong because the child is exploited not only at the moment of abuse but also each time the material is stored, viewed, transmitted or re-circulated online.⁷³ Section 67B of the Information Technology Act 2000 directly criminalises the publication, transmission, browsing, downloading, advertising and facilitation of sexually explicit material involving children in electronic form.⁷⁴ At the same time, section 13 of the Protection of Children from Sexual Offences Act addresses the use of children for pornographic purposes, while allied provisions punish storage, circulation and commercial use.⁷⁵ Read together, the Information Technology Act and the Protection of Children from Sexual Offences Act show that Indian law recognises digital sexual abuse as a continuing offence with both technological and bodily dimensions.

The judicial discussion in *Avnish Bajaj v. State (NCT of Delhi)*, commonly associated with the Bazeed.com case, remains important for understanding online liability in child-related obscene-publication cases.⁷⁶ The Delhi High Court examined whether executives of an internet platform could automatically be prosecuted when unlawful content was offered for circulation through the website. Although the case arose before the present intensity of platform regulation, it established a broader lesson: intermediaries cannot remain indifferent once unlawful material is brought to notice, and criminal law increasingly expects due diligence in content moderation where children are involved. The modern difficulty, however, lies in the migration of such material to encrypted channels, hidden forums and dark-web networks where ordinary detection systems are weak. This challenge has been met partly through specialised policing measures such as the Indian Cyber Crime Coordination Centre framework and targeted operations like the Kerala Police's Operation P-Hunt, which use cyber-forensic tracing, tip-line coordination and device analysis to identify perpetrators and rescue children.⁷⁷

C. Online grooming and enticement

Online grooming is a process through which an adult builds trust with a child in digital spaces for a concealed sexual purpose. The offender may appear as a friend, classmate, mentor, gamer or romantic partner and gradually moves the conversation from ordinary interaction to emotional dependence, sexualised communication, requests for images or meetings in person. This offence is especially dangerous because the abusive act often begins long before any physical contact and may remain invisible to parents, teachers and investigators. Section 11 of

⁷³ *Id.*

⁷⁴ Information Technology Act, 2000, s. 67B (India).

⁷⁵ Protection of Children from Sexual Offences Act, 2012, s. 14 (India).

⁷⁶ *Avnish Bajaj*, *supra* note 5.

⁷⁷ 'Operation P-Hunt', *supra* note 6.

the Protection of Children from Sexual Offences Act is wide enough to capture several grooming behaviours, including repeated contact through electronic means, showing pornography to a child, or making sexually coloured remarks.⁷⁸ In addition, section 95 of the Bharatiya Nyaya Sanhita, which penalises hiring, employing or using a child to commit an offence, may support prosecution where an adult uses a child in digital sexual exploitation.⁷⁹

Indian courts have increasingly recognised that so-called consent extracted through deception, manipulation, blackmail or emotional dependency cannot be treated as meaningful consent where minors are concerned. In cases discussed by High Courts, children are often lured into private chats, induced to share intimate material and then threatened with exposure if they resist further demands.⁸⁰ This pattern shows that grooming is rarely a single act; it is a staged abuse of vulnerability. A major enforcement problem is end-to-end encryption, which limits real-time monitoring of harmful conversations.⁸¹ For this reason, police responses have moved towards complaint-based intervention, metadata analysis, forensic recovery and child-sensitive interviewing rather than simplistic surveillance models.⁸² Operation P-Hunt in Kerala demonstrates this shift by combining cyber expertise, coordinated intelligence and victim-identification methods to trace offenders who believed they were hidden behind private networks.⁸³

D. Cyberbullying and online harassment

Cyberbullying includes repeated humiliation, intimidation, shaming, exclusion, impersonation and hostile communication carried out through digital platforms.⁸⁴ When directed against children, the harm is often deeper than ordinary insult because the abuse may be constant, publicly visible and permanently searchable. A child who is mocked in a classroom can leave the room; a child who is targeted online may find the abuse following them across platforms, devices and peer groups.⁸⁵ Indian statutory law does not create a single offence called cyberbullying, yet different provisions can be used depending on the nature of the conduct. Section 67 of the Information Technology Act may apply where obscene or sexually degrading material is published electronically,⁸⁶ while child-protection structures under the Juvenile

⁷⁸ Protection of Children from Sexual Offences Act, 2012, s. 11 (India).

⁷⁹ Bharatiya Nyaya Sanhita, 2023, s. 95 (India).

⁸⁰ *Independent Thought v. Union of India*, (2017) 10 SCC 800.

⁸¹ Duggal, *supra* note 4.

⁸² Indian Cyber Crime Coordination Centre, *supra* note 26.

⁸³ 'Operation P-Hunt', *supra* note 6.

⁸⁴ Protection of Children from Sexual Offences Act, 2012, *supra* note 72; UNESCO, SCHOOL VIOLENCE AND BULLYING: GLOBAL STATUS AND TRENDS (2024).

⁸⁵ *Id.*.

⁸⁶ Information Technology Act, 2000, s. 67 (India).

Justice Act become relevant when the child's safety, mental health or care needs are seriously affected.⁸⁷

The concerns raised in Blue Whale litigation before the courts revealed that online harassment is not always limited to abusive language; it may merge with psychological manipulation, self-harm inducement and peer pressure.⁸⁸ The legal significance of such cases lies in their recognition that digital harm to children can become life-threatening even without conventional physical assault. Courts and child-rights bodies have therefore moved towards a mixed response model: selective criminalisation, school-level intervention, mental-health support and platform-based reporting systems. Guidelines of the National Commission for Protection of Child Rights on bullying and cyberbullying, along with digital-safety materials issued by educational bodies, reflect this preventive orientation.⁸⁹ These mechanisms matter because many children report cyberbullying first to friends or online portals rather than to police stations, and a child-protective framework must therefore be accessible outside the formal criminal process.

E. Sexting and self-generated child sexual abuse material

Sexting among adolescents raises one of the most difficult questions in contemporary child-protection law. At a practical level, it may involve teenagers sharing intimate photographs or videos with romantic partners, friends or peer groups through messaging applications.⁹⁰ Yet once the person depicted is below eighteen years of age, the legal system does not simply view the image as a private expression; it may fall within the framework of child sexual abuse material. This creates tension between the protective purpose of the law and the lived reality that some minors participate in image-sharing without understanding the long-term consequences.⁹¹ The 2019 amendments to the Protection of Children from Sexual Offences Act strengthened the provisions concerning the pornographic use of children and clarified the seriousness of storage and transmission offences.⁹²

Courts have therefore had to negotiate a difficult line between strict legality and child-sensitive justice. In judicial discussions concerning so-called "selfie porn", the concern has not been merely whether an offence has technically occurred, but also whether a child who created or shared an intimate image should always be treated as an offender rather than as a vulnerable

⁸⁷ Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2 of 2016 (India).

⁸⁸ *The Registrar (Judicial), Madurai Bench of Madras High Court v. Secretary to Government, Union Ministry of Communications*, Suo Motu W.P. (MD) No. 16668 of 2017 (Madras HC).

⁸⁹ National Commission for Protection of Child Rights, GUIDELINES ON PREVENTION OF BULLYING AND CYBERBULLYING (2023).

⁹⁰ Protection of Children from Sexual Offences Act, 2012, s. 15 (India).

⁹¹ *Id.*.

⁹² Protection of Children from Sexual Offences (Amendment) Act, 2019, No. 25 of 2019 (India).

person requiring guidance, privacy protection and counselling.⁹³ The issue of consent is deeply unstable in these cases because children may act under peer pressure, coercive romance, emotional blackmail or ignorance about the permanence of digital circulation. For that reason, complaint systems such as the POCSO e-Box and similar online reporting channels are valuable not only for punitive action but also for rapid removal, support and referral.⁹⁴ A nuanced legal response must distinguish exploitative circulation from immature experimentation while never trivialising the possibility of blackmail, re-distribution and lifelong reputational harm.⁹⁵

F. Online gaming exploitation

Digital gaming spaces have become major sites of interaction for children, and this has altered the landscape of cyber risk.⁹⁶ Games are no longer isolated entertainment products; they are networked environments with voice chat, text chat, virtual economies, private messaging and algorithmic reward systems. These features create opportunities for grooming, fraud, sexual solicitation, data extraction and emotional manipulation. Where gaming spaces are used to invite children into sexually explicit interaction or the exchange of abusive material, section 67B of the Information Technology Act becomes relevant.⁹⁷ Where the conduct involves threats, coercion, inducement or extortion, the provisions of the Bharatiya Nyaya Sanhita on intimidation and related wrongs may also operate.⁹⁸

Public and judicial anxiety around gaming has often surfaced through litigation and policy debate concerning addiction, violence and youth vulnerability, including the restrictions imposed on PUBG in Gujarat and the litigation that followed.⁹⁹ Although blanket bans raise constitutional and practical concerns, those episodes helped move the conversation towards platform accountability and child-safety design. The deeper legal issue is not gaming as such, but exploitation within gaming ecosystems. This includes manipulative monetisation methods, covert adult-child contact and loot-box-style features that normalise compulsive spending behaviour.¹⁰⁰ A rights-based response therefore favours age-gating, reporting tools, parental controls, suspicious-chat detection and stronger obligations on companies to cooperate in investigations involving minors.¹⁰¹

⁹³ 'Bombay High Court Examines Juvenile Culpability in "Selfie" Image Case', INDIAN EXPRESS (2021).

⁹⁴ POCSO e-Box, National Commission for Protection of Child Rights.

⁹⁵ *Id.*

⁹⁶ Information Technology Act, 2000, s. 67B (India).

⁹⁷ *Id.*

⁹⁸ Bharatiya Nyaya Sanhita, 2023, *supra* note 10.

⁹⁹ 'Gujarat High Court Declines PIL Challenging PUBG Ban', MEDIANAMA (April 2019).

¹⁰⁰ *Id.*

¹⁰¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

G. Viral challenges: Blue Whale and Momo

The Blue Whale and Momo phenomena illustrate how online culture can weaponise fear, curiosity and adolescent vulnerability.¹⁰² Whether every reported instance was authentic is less important than the legal reality they exposed: harmful digital ecosystems can push children towards self-harm, isolation and panic through anonymous instructions, staged tasks and threats. Such challenges thrive on virality. They move quickly through copied links, altered usernames, private messages and sensational media attention. This creates difficulty for conventional policing because, by the time one link is blocked, several mirrors or clones may already exist.¹⁰³

Indian legal responses relied on a combination of blocking powers, advisories and judicial oversight.¹⁰⁴ In Blue Whale-related proceedings, the Madras High Court, taking suo motu cognisance, pressed authorities to identify dangerous links and coordinate preventive action, and concerns regarding the Momo challenge also triggered calls for takedown measures and platform cooperation.¹⁰⁵ Section 69A of the Information Technology Act provides the legal basis for blocking public access to harmful online material in appropriate cases.¹⁰⁶ But blocking alone cannot solve the problem. Children drawn into such spaces often require counselling, family support and school-based mental-health intervention rather than a purely punitive state response. The increasing role of the Indian Cyber Crime Coordination Centre, child helplines and awareness programmes suggests that the law is gradually learning that virality must be met not only with censorship tools but with early support systems and digital resilience.¹⁰⁷

H. Statutory framework and judicial precedents

The legal response to cyber crimes against children in India is layered rather than unitary.¹⁰⁸ It draws from general criminal law, the Information Technology Act, the Protection of Children from Sexual Offences Act, juvenile-protection mechanisms, evidentiary rules and intermediary regulation.¹⁰⁹ This structure is necessary because harm to children online does not stay within neat doctrinal categories. A single incident may involve obscenity, sexual harassment, image circulation, extortion, mental cruelty and eventual physical assault. The law therefore operates

¹⁰² The Registrar (Judicial), *supra* note 88.

¹⁰³ *Id.*

¹⁰⁴ Information Technology Act, 2000, s. 69A (India).

¹⁰⁵ The Registrar (Judicial), *supra* note 88.

¹⁰⁶ Information Technology Act, 2000, s. 69A (India).

¹⁰⁷ Protection of Children from Sexual Offences Act, 2012, *supra* note 72.

¹⁰⁸ *Id.*

¹⁰⁹ Bharatiya Nyaya Sanhita, 2023, *supra* note 10.

through overlap, and that overlap should be understood as a strength rather than a drafting defect.

A useful example is the relationship between the older Indian Penal Code framework and the Bharatiya Nyaya Sanhita.¹¹⁰ Under the old Indian Penal Code, section 375 was often criticised for doctrinal limitations and gendered framing, even though later amendments widened its reach. Section 63 of the Bharatiya Nyaya Sanhita marks a re-articulation of rape law in the new criminal code and must be read alongside the Protection of Children from Sexual Offences Act where minors are concerned.¹¹¹ In offences involving children, ostensible consent has little legal relevance because the age threshold itself disables a consent defence under the child-protection framework.¹¹² This is especially significant in cyber cases where online grooming leads to offline meetings or sexual assault after digital inducement.

The Information Technology Act complements this framework by distinguishing between general obscenity, sexually explicit material and child-specific abuse content in electronic form. Sections 67, 67A and 67B accordingly create a graded structure of liability based on the seriousness of the digital content.¹¹³ Case law such as *Avnish Bajaj* demonstrates the importance of intermediary responsibility and due diligence in the electronic environment.¹¹⁴ At the same time, the Protection of Children from Sexual Offences Act remains indispensable because it centres the child, not the platform, and recognises pornography, harassment and sexual assault as connected forms of exploitation.¹¹⁵ The Protection of Children from Sexual Offences Rules and child-friendly procedures further strengthen the protective model by insisting on confidentiality, supportive reporting and a process that avoids secondary victimisation.¹¹⁶

The Protection of Children from Sexual Offences Rules 2020 are particularly important for cyber offences because digital abuse often depends on fragile electronic evidence. Screenshots, chat logs, device extractions, metadata and online complaints must be preserved in a form that remains legally admissible and sensitive to the dignity of the child. Courts increasingly expect investigators to combine technical competence with child-sensitive procedure. The broader judicial pattern in Indian case law shows a movement away from treating online harm as morally offensive content alone and towards recognising it as abuse, coercion and structural

¹¹⁰ *Id.* s. 63.

¹¹¹ Protection of Children from Sexual Offences Act, 2012, *supra* note 72.

¹¹² Information Technology Act, 2000, s. 67B (India).

¹¹³ *Avnish Bajaj*, *supra* note 5.

¹¹⁴ Protection of Children from Sexual Offences Act, 2012, *supra* note 72.

¹¹⁵ Protection of Children from Sexual Offences Rules, 2020 (India).

¹¹⁶ *Id.*

vulnerability in digital settings. That shift is the real significance of current legal developments.¹¹⁷

I. Challenges to overcome

A major barrier in prosecuting cyber crimes against children has always been silence. Children may fear blame, humiliation, disbelief or retaliation. Families may avoid reporting because they are anxious about stigma, community reaction or the exposure of intimate images.¹¹⁸ For a long time, these social barriers meant that the law existed on paper but did not translate into accessible protection. Recent reporting mechanisms have improved this position to some extent. Childline services, online complaint portals and school-linked referral systems have made first contact easier.¹¹⁹

A second challenge has been anonymity in digital offending.¹²⁰ Offenders use fake profiles, encrypted channels and transnational platforms to hide their identities. Recent specialised responses, however, show institutional adaptation. Operation P-Hunt in Kerala and the larger Indian Cyber Crime Coordination Centre framework demonstrate how cyber policing is shifting towards database coordination and forensic imaging.¹²¹ These methods are especially useful in cases involving the circulation of child sexual abuse material.¹²²

The third challenge lies in treating children appropriately within the justice system itself. Some children appear simultaneously as victims and technical offenders. The emerging legal approach increasingly combines criminal law with counselling, school intervention and child-welfare support. This development matters because cyber crimes against children are offences against childhood, privacy, trust and future dignity.¹²³

IV. ENFORCEMENT OPERATIONS: STATE AND CENTRAL AGENCIES

A. Central agencies

The enforcement architecture for cyber offences against women and children in India has become more organised in recent years, especially after the creation of specialised central coordination structures. At the centre of this framework stands the Indian Cyber Crime Coordination Centre, functioning under the Ministry of Home Affairs as a nodal body for

¹¹⁷ National Crime Records Bureau, *supra* note 7.

¹¹⁸ *Id.*

¹¹⁹ Indian Cyber Crime Coordination Centre, *supra* note 26.

¹²⁰ *Id.*

¹²¹ 'Operation P-Hunt', *supra* note 6.

¹²² Ved Kumari, THE JUVENILE JUSTICE (CARE AND PROTECTION OF CHILDREN) ACT 2015: A CRITICAL ANALYSIS (2017); Ved Kumari, JUVENILE JUSTICE SYSTEM IN INDIA: FROM WELFARE TO RIGHTS (2010).

¹²³ Indian Cyber Crime Coordination Centre, *supra* note 26.

coordination, intelligence-sharing, capacity-building and technological support to law-enforcement agencies across the country.¹²⁴ Its role is not limited to policy guidance. It also works as an operational support system by integrating reporting platforms, forensic assistance, training modules, suspect repositories and inter-agency cooperation for cyber offences that often cut across territorial boundaries. In matters involving women and children, this centralised approach is particularly important because such offences usually move quickly across jurisdictions and may involve anonymous users, encrypted platforms, cloud storage and foreign intermediaries.¹²⁵

One of the most important institutional tools linked to the Indian Cyber Crime Coordination Centre is the National Cyber Crime Reporting Portal, accessible through cybercrime.gov.in. The portal has emerged as a major public-facing complaint mechanism for cyber offences, including a dedicated category for crimes against women and children. Its significance lies less in numerical volume and more in procedural accessibility: victims or their guardians can report abuse, upload evidence and initiate a state response without first navigating the barriers of a physical police station.¹²⁶ Official statements indicate that a large number of complaints have been registered on the portal, reflecting both greater public awareness and a shift towards digital-first reporting. Although not every complaint converts into a first information report, the portal has substantially improved early reporting, evidence preservation and triage in urgent matters such as sexual exploitation, impersonation, deepfake abuse, sextortion and circulation of child sexual abuse material.¹²⁷

The central role of agencies such as the Central Bureau of Investigation is most visible in nationally coordinated operations involving child sexual abuse material and transnational exploitation networks. In 2022, the Central Bureau of Investigation conducted Operation Megh Chakra, a country-wide crackdown against persons involved in the circulation and storage of such material through cloud-based systems, acting on international intelligence inputs routed through Interpol channels.¹²⁸ The operation illustrated a key feature of central enforcement: cyber abuse against children is rarely local in its structure, even when the victim or suspect is physically located in one State. The use of transnational tips, forensic seizure and simultaneous searches in multiple jurisdictions demonstrates why central agencies remain necessary in complex cyber-crime cases. Public reporting has also referred to theme-based enforcement

¹²⁴ *Id.*

¹²⁵ *Id.*

¹²⁶ Ministry of Home Affairs, ANNUAL REPORT 2024-25 (2025).

¹²⁷ 'CBI Launches Operation Megh Chakra against CSAM', THE HINDU (24 September 2022).

¹²⁸ *Id.*

against online grooming and organised digital sexual exploitation, underlining a strategy of thematic operations rather than ordinary case-by-case investigation.¹²⁹

Case law has gradually reinforced the importance of coordinated central intervention. In *Avnish Bajaj v. State (NCT of Delhi)*, the Delhi High Court exposed the difficulties of attributing criminal responsibility in online content-distribution cases and underscored the need for due diligence and responsive institutional mechanisms.¹³⁰ Later jurisprudence concerning online sexual offences against minors has shown that the ordinary police structure, without technical support and inter-state coordination, is often inadequate to deal with fast-moving digital evidence. Thus, the contribution of central agencies lies not only in prosecution but in creating a national enforcement grammar, one that links reporting, forensic capacity, inter-jurisdictional coordination and platform engagement in a unified response to cyber abuse against women and children.¹³¹

B. State agencies

While central coordination is essential, actual enforcement still depends heavily on the capacity, responsiveness and innovation of state agencies. State cyber cells, women and child protection units, district police teams and specialised digital-investigation wings serve as the first institutional responders in most cases.¹³² Their importance is both practical and constitutional: policing remains largely a state subject, and prompt rescue, seizure, victim protection and local intelligence-gathering cannot be effectively outsourced to central authorities.¹³³ The quality of enforcement therefore depends on how well state agencies adapt cyber policing to local realities while remaining connected to national systems of reporting and forensic support.¹³⁴

Kerala offers one of the clearest examples of a proactive state-level strategy through Operation P-Hunt, a recurring police initiative directed against paedophile networks and the circulation of child sexual abuse material.¹³⁵ Publicly available reports indicate that the operation combined cyber-surveillance inputs, device-based forensic examination and simultaneous action across districts to identify persons downloading, storing or sharing exploitative material involving children. The legal significance of P-Hunt lies in its preventive logic: it does not wait for a conventional complaint by a known victim but acts on digital intelligence and trace evidence to

¹²⁹ *Avnish Bajaj*, *supra* note 5.

¹³⁰ Indian Cyber Crime Coordination Centre, *supra* note 26.

¹³¹ *Id.*

¹³² INDIA CONST. sch. VII, list II, entry 2.

¹³³ *Id.*

¹³⁴ 'Operation P-Hunt', *supra* note 6.

¹³⁵ *Id.*

uncover hidden abuse networks. This is particularly relevant in cyber offences against children, where many victims are unidentified, unwilling to disclose or located outside the immediate investigative jurisdiction. Kerala's experience also shows the value of specialised cyber wings such as Cyberdome in assisting traditional policing structures with technical expertise and coordinated execution.¹³⁶

Tamil Nadu has likewise developed a recognisable profile in cyber enforcement, especially in relation to social-media abuse, impersonation, morphing and, more recently, deepfake-based victimisation of women and girls.¹³⁷ Public discussion of state initiatives reflects a growing awareness among law-enforcement agencies that artificial-intelligence-manipulated images and videos can produce forms of sexual humiliation that are rapid, scalable and difficult to reverse. Even where the naming of individual operations varies across official and media sources, the broader pattern is clear: state police forces have built district-based cybercrime structures and have increasingly treated gendered digital abuse as a serious law-enforcement issue rather than a private reputational dispute. This shift has doctrinal importance because it moves deepfake exploitation from the margins of obscenity law into the centre of dignity-based criminal protection.¹³⁸ Maharashtra has similarly used cyber-enforcement drives to address online abuse affecting women and minors, including blackmail, non-consensual image circulation and online intimidation.¹³⁹ These initiatives underline an emerging state practice of specialised campaigns directed at recurring modes of digital harm rather than isolated case registration.

Judicial decisions also demonstrate the importance of state enforcement. In Blue Whale-related litigation, courts have emphasised the obligation of state authorities to act preventively when harmful digital content threatens children's lives and mental health.¹⁴⁰ Such cases confirm that cyber policing is not confined to post-offence investigation; it also includes content-blocking requests, counselling referral, school coordination and rapid intervention where online conduct risks escalating into physical harm or suicide.¹⁴¹ State agencies therefore remain indispensable because they occupy the point where abstract law becomes immediate protection. When functioning effectively, they combine proximity to victims with procedural familiarity, local intelligence and increasingly sophisticated cyber-investigative methods.

¹³⁶ 'Tamil Nadu Police Launch Operation Blackout against Deepfakes', NEW INDIAN EXPRESS (12 January 2025).

¹³⁷ *Id.*

¹³⁸ 'Maharashtra Police Drive against Online Harassment', TIMES OF INDIA (10 February 2025).

¹³⁹ The Registrar (Judicial), *supra* note 88.

¹⁴⁰ *Id.*

¹⁴¹ National Crime Records Bureau, *supra* note 7.

C. Efficacy analysis

The overall efficacy of enforcement operations in cyber offences against women and children should be assessed with caution. Official data and government statements suggest improvement in reporting, detection and some aspects of prosecution, and public discussion has also indicated a rise in conviction-related outcomes in certain categories.¹⁴² Yet efficacy cannot be measured only by registered cases or arrest counts. The deeper test is whether the system can secure the timely takedown of harmful content, preserve admissible electronic evidence, protect victims from secondary trauma and convert digital intelligence into sustainable convictions. In this respect, India has clearly moved forward, but unevenly.

The principal strengths of the present enforcement model are visible in better reporting systems, specialised operations, inter-agency coordination and a stronger recognition that cyber abuse against women and children demands focused policing.¹⁴³ At the same time, serious structural gaps remain. Mutual legal-assistance procedures are often slow when evidence is stored abroad; encrypted services limit traceability; and many investigations still suffer from weak digital documentation, delayed seizure or poor understanding of platform architecture. Scholarly writing, including Ved Kumari's work on juvenile justice and child protection, supports the view that legal systems dealing with children must remain not merely punitive but also welfare-oriented, sensitive and institutionally trained.¹⁴⁴ Accordingly, the future of enforcement lies not only in more operations but in better-quality operations: faster preservation, stronger cross-border cooperation, trained prosecutors, child-sensitive procedure and platform accountability anchored in constitutional values.

V. COMPARATIVE ANALYSIS AND REFORMS

A. Old and new legal frameworks

A comparative study of offences relating to women and children in digital spaces shows that Indian law has moved from a fragmented and reactive model to a more specialised, rights-based framework.¹⁴⁵ Earlier legal responses depended heavily on the Indian Penal Code 1860 and the Information Technology Act 2000, with limited conceptual clarity on cyber-enabled sexual offences affecting women and minors. The older system could address obscenity, stalking, intimidation and certain forms of publication, but it did not always capture the full character of online exploitation, especially where the offence involved grooming, child sexual abuse

¹⁴² *Id.*

¹⁴³ Kumari, *supra* note 123.

¹⁴⁴ Protection of Children from Sexual Offences Act, 2012, *supra* note 72.

¹⁴⁵ *Id.* s. 28.

material, image-based sexual abuse or technology-facilitated coercion. The enactment of the Protection of Children from Sexual Offences Act 2012 marked a major doctrinal shift because it introduced child-centred definitions, special procedures and dedicated courts.¹⁴⁶ Even though the Act was not originally drafted as a pure cyber statute, its language has been interpreted broadly enough to include many forms of virtual sexual exploitation.

The contrast between the older criminal-law framework and the newer legislative design becomes sharper when one compares the Indian Penal Code with the Bharatiya Nyaya Sanhita.¹⁴⁷ Under the older structure, offences involving women and children online were often fitted awkwardly into general provisions on obscenity, insult, stalking, defamation or rape. By contrast, the new code must be read alongside the Protection of Children from Sexual Offences Act and the Information Technology Act in a more integrated manner, allowing digital conduct to be linked with bodily harm, coercion, sexual autonomy and child protection.¹⁴⁸ This integrated approach is doctrinally important because cyber offences do not remain confined to screens; they frequently culminate in blackmail, trafficking, sexual assault, extortion and long-term psychological harm. The newer legal landscape therefore reflects a shift from viewing such acts as merely offensive speech or immoral content to recognising them as violations of dignity, privacy, bodily integrity and constitutional personhood.

Case law has played a significant role in this transition. In *Avnish Bajaj v. State (NCT of Delhi)*, the Delhi High Court confronted the problem of criminal liability in the online distribution of obscene material through a digital marketplace.¹⁴⁹ The decision is important not only for intermediary liability but also because it exposed the limits of conventional criminal categories when applied to online environments.¹⁵⁰ Similarly, in *Independent Thought v. Union of India*, the Supreme Court harmonised rape law with child-protection principles by reading down the marital-rape exception in relation to minor wives, thereby reinforcing the norm that age-based protection cannot be diluted by formal status.¹⁵¹ Although the case did not arise from cyber facts, its reasoning is deeply relevant to online offences because it strengthens the doctrinal principle that the law must privilege the dignity and best interests of the child over

¹⁴⁶ Bharatiya Nyaya Sanhita, 2023, *supra* note 10.

¹⁴⁷ Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India); Protection of Children from Sexual Offences Act, 2012, No. 32 of 2012 (India); Information Technology Act, 2000, s. 66E, No. 21 of 2000 (India).

¹⁴⁸ *Avnish Bajaj*, *supra* note 5.

¹⁴⁹ *Id.*

¹⁵⁰ *Independent Thought*, *supra* note 80.

¹⁵¹ *Id.*

formalistic defences. Together, these cases show that reform in this field has come not only from legislation but also from constitutional interpretation and judicial sensitivity.¹⁵²

B. International comparison: UNCRC and child-rights standards

Any serious reform discussion must also place Indian law within the framework of international child-rights obligations.¹⁵³ The United Nations Convention on the Rights of the Child, to which India is a State Party, requires that in all actions concerning children the best interests of the child shall be a primary consideration.¹⁵⁴ It also obliges States to protect children from all forms of violence, sexual exploitation, abuse and other harmful exploitation.¹⁵⁵ These guarantees, found especially in Articles 3, 19, 34 and 36, create an international normative standard that extends beyond traditional physical abuse and logically includes technology-mediated exploitation.¹⁵⁶ In comparative terms, the Convention does not provide a detailed cybercrime code; instead, it offers a rights framework through which national legal systems must be evaluated.¹⁵⁷

Viewed against this benchmark, India has made substantial progress but still shows areas of doctrinal and institutional incompleteness.¹⁵⁸ On the positive side, the Protection of Children from Sexual Offences Act, the Information Technology Act, the Protection of Children from Sexual Offences Rules and the growth of specialised reporting and enforcement structures show that India has moved closer to a child-rights model of protection. The emphasis on child-friendly procedure, confidentiality, reporting obligations and specialised courts is consistent with the Convention's concern for best interests and protection from exploitation.¹⁵⁹ Yet international comparison also highlights gaps. Indian law still uses uneven terminology in some areas; platform accountability remains inconsistent; and emerging harms such as artificial-intelligence-generated abuse imagery, deepfake sexual exploitation and synthetic child sexual abuse material are not dealt with through sufficiently explicit statutory language.¹⁶⁰ Comparative scholarship and recent policy writing suggest that several jurisdictions are beginning to treat such material as a distinct child-protection threat because it normalises exploitation, facilitates

¹⁵² United Nations Convention on the Rights of the Child, GA Res 44/25 (20 November 1989).

¹⁵³ *Id.* art. 3.

¹⁵⁴ *Id.* art. 19.

¹⁵⁵ *Id.* art. 34.

¹⁵⁶ *Id.* art. 36.

¹⁵⁷ Protection of Children from Sexual Offences Act, 2012, *supra* note 72.

¹⁵⁸ *Id.*

¹⁵⁹ Duggal, *supra* note 4.

¹⁶⁰ United Nations Convention on the Rights of the Child, *supra* note 153; Just Rights for Children Alliance, DIGITAL HARMS AND THE MINOR VICTIM (2025).

grooming and intensifies reputational harm even where no original image was voluntarily supplied by the child.¹⁶¹

A rights-based comparative analysis also requires attention to procedure and not only to offences.¹⁶² The Convention framework insists that child protection should not become merely punitive; it must remain restorative, supportive and institutionally sensitive.¹⁶³ This is especially relevant in cases of sexting, peer circulation and self-generated abuse material, where a child may appear simultaneously as victim, witness and technical offender.¹⁶⁴ Ved Kumari's child-rights scholarship is particularly useful here because it argues that legal systems affecting children must move from welfare paternalism to a genuine rights-based approach.¹⁶⁵ That insight has direct relevance for cyber-law reform. A system that criminalises every digital mistake by a child without counselling, diversion or privacy safeguards may formally punish misconduct but still fail the deeper standard of child justice.

C. Reform directions

The next phase of reform should therefore focus on institutional specialisation. One significant proposal is the creation of dedicated cyber-Protection of Children from Sexual Offences courts or, at the very least, specially trained Special Courts with exclusive digital-evidence capacity.¹⁶⁶ Section 28 of the Protection of Children from Sexual Offences Act already contemplates Special Courts for offences under the Act.¹⁶⁷ However, many cyber cases involving minors still move through systems that are overburdened, unevenly trained or insufficiently equipped to handle metadata, device imaging, cloud evidence, takedown urgency and cross-platform attribution.¹⁶⁸ A cyber-Protection of Children from Sexual Offences model would not require a wholly new statute; it could begin through designated benches, judicial training, digital-evidence protocols and integrated forensic support at the district and regional levels.¹⁶⁹ Such an approach would reduce delay, improve evidentiary quality and protect children from repeated exposure during fragmented proceedings.¹⁷⁰

¹⁶¹ *Id.* art. 3.

¹⁶² *Id.* art. 19.

¹⁶³ *Id.* art. 34.

¹⁶⁴ Kumari, *supra* note 123.

¹⁶⁵ Protection of Children from Sexual Offences Act, 2012, *supra* note 72; Kumari, *supra* note 123.

¹⁶⁶ Protection of Children from Sexual Offences Act, 2012, s. 28 (India).

¹⁶⁷ *Id.*; National Crime Records Bureau, *supra* note 7.

¹⁶⁸ Bharatiya Sakshya Adhiniyam, 2023, s. 63, No. 47 of 2023 (India).

¹⁶⁹ Kumari, *supra* note 123.

¹⁷⁰ Indian Cyber Crime Coordination Centre, *supra* note 26; UNESCO, ETHICAL AI IN LAW ENFORCEMENT GUIDELINES (2024).

A second reform lies in the responsible use of artificial-intelligence-assisted forensics.¹⁷¹ Contemporary child-protection enforcement already uses tools such as hash-matching, pattern recognition, image clustering and facial-analysis systems to identify repeat circulation of child sexual abuse material and possible victim matches.¹⁷² International and comparative materials indicate that such systems can help investigators sort large volumes of abusive content, locate links between devices and prioritise high-risk cases more quickly than manual review alone.¹⁷³ In India, the debate is no longer whether technology should be used in child protection, but how it should be used lawfully and proportionately. Such forensics should therefore be introduced through a rights-sensitive framework that ensures auditability, chain of custody, judicial oversight, data minimisation and safeguards against false positives.¹⁷⁴ Used carefully, such tools can enhance rather than undermine child protection because they reduce investigative delay and limit repeated manual exposure to traumatic material.

Further reforms are also needed in legislative drafting and platform governance.¹⁷⁵ Parliament may eventually need to clarify that synthetic child sexual abuse material, sexually exploitative deepfakes involving minors and artificial-intelligence-generated abuse content fall within the penal framework, even where the abuse image is fabricated rather than directly photographed.¹⁷⁶ The same is true for sexual deepfakes affecting women, which blur the line between obscenity, harassment, defamation and sexual violence.

VI. CONCLUSION

The study of offences against women and children in digital spaces shows that cyber abuse is no longer a marginal extension of traditional crime. It has become a primary challenge for criminal law, child protection, gender justice and digital governance in India. The article demonstrates that online harms such as cyberstalking, non-consensual circulation of intimate images, grooming, child sexual abuse material, bullying, sextortion and exploitative gaming environments are different in form but similar in structure: each uses technology to deepen inequality, intensify vulnerability and multiply the reach of harm.¹⁷⁷ What once occurred in a limited physical space may now be repeated, stored, copied and revived indefinitely through

¹⁷¹ *Id.*

¹⁷² Duggal, *supra* note 4.

¹⁷³ *Id.*

¹⁷⁴ Information Technology Act, 2000, s. 79 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

¹⁷⁵ *Id.*; Duggal, *supra* note 4.

¹⁷⁶ National Crime Records Bureau, *supra* note 7.

¹⁷⁷ Duggal, *supra* note 4.

networked platforms.¹⁷⁸ In this way, the digital environment does not merely host old offences; it changes their magnitude, durability and evidentiary complexity.

A major theme running through this article is that Indian law has moved from a scattered response to a more integrated one.¹⁷⁹ Earlier, many cyber offences against women and children had to be categorised under broad provisions, including obscenity, insult, intimidation or sexual violence, under the Indian Penal Code and the Information Technology Act 2000. Over time, however, the legal framework has become more nuanced through the Protection of Children from Sexual Offences Act 2012, the Protection of Children from Sexual Offences Rules, the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam, read together with intermediary due-diligence norms and reporting mechanisms.¹⁸⁰ This shift is significant because it recognises that a digital offence may contain not only unlawful content but also coercion, privacy invasion, blackmail, emotional manipulation and ongoing reputational damage. The law is therefore gradually moving away from a narrow obscenity model towards a dignity-based and victim-centred understanding of cyber harm.¹⁸¹ Ultimately, a zero-tolerance institutional culture is essential to ensure that technological advancement and legal reform work together to protect the most vulnerable in the digital era.¹⁸²

This development in cyber law is supported by several judicial decisions. *Shreya Singhal v. Union of India* clarified that online regulation must remain consistent with constitutional freedom, while *Avnish Bajaj v. State (NCT of Delhi)* illustrated the practical difficulties of assigning responsibility in platform-based publication and distribution of unlawful content.¹⁸³ At the same time, *Independent Thought v. Union of India* reinforced the principle that the protection of the child must prevail over formalistic legal exceptions in cases involving minors.¹⁸⁴ Litigation related to Blue Whale and other High Court interventions further showed that cyber harms may threaten mental health, physical safety and even life itself, especially where vulnerable children are drawn into manipulative online spaces.¹⁸⁵ These cases collectively reveal that digital space must be regulated through an appropriate balance of liberty, accountability and victim protection.

¹⁷⁸ Protection of Children from Sexual Offences Act, 2012, *supra* note 72; Bharatiya Nyaya Sanhita, 2023, *supra* note 10.

¹⁷⁹ *Id.*; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

¹⁸⁰ National Crime Records Bureau, *supra* note 7.

¹⁸¹ Duggal, *supra* note 4.

¹⁸² *Shreya Singhal*, *supra* note 1; *Avnish Bajaj*, *supra* note 5.

¹⁸³ *Independent Thought*, *supra* note 80.

¹⁸⁴ The Registrar (Judicial), *supra* note 88.

¹⁸⁵ National Crime Records Bureau, *supra* note 7.

The article has also shown that legal rules alone are not adequate. Reporting barriers, social stigma, poor digital literacy, prolonged cross-border cooperation, evidentiary failures and uneven forensic competence still prevent effective justice in many cases.¹⁸⁶ Women often remain silent because online abuse is trivialised as a private matter or blamed on the victim herself. Children and their families may hesitate to report because of shame, fear and the anxiety of public exposure. Even where the law is strong on paper, a delayed seizure, an improperly preserved device or an incompetent investigation can irreparably weaken the prosecution. For that reason, the future of cyber justice is not only about introducing new offences but also about strengthening institutions that can respond quickly, sensitively and competently.

This is where the concept of zero tolerance must be properly understood. Zero tolerance does not mean mechanical punishment in every case or the indiscriminate expansion of criminal law.¹⁸⁷ It means a legal and institutional culture in which abuse is treated seriously from the first complaint, harmful content is removed without delay, electronic evidence is preserved with forensic integrity and survivors are given support without moral judgment. In relation to children, it also means that punishment must be accompanied by care, counselling, privacy and child-friendly procedures.¹⁸⁸ In cases relating to women, the judicial system must acknowledge online humiliation, deepfake abuse, sexual blackmail and persistent harassment as real violations of dignity rather than virtual inconveniences.¹⁸⁹

The future requires a stronger integration of technology and law. Specialised cyber units, trained prosecutors, district-level forensic support and better coordination between police, courts, schools, child-welfare bodies and platforms are now essential.¹⁹⁰ The proposal for cyber-Protection of Children from Sexual Offences courts or specially designated digital benches deserves serious consideration because cyber cases involving children require speed, confidentiality and technical competence at every stage. Artificial-intelligence-assisted forensic tools can also improve the detection of repeat abuse material, pattern recognition and victim identification, but they must operate within a framework of legality, transparency and rights protection. Platform accountability, secure reporting channels, age-sensitive design and public legal education must work together with criminal law rather than outside it.

Ultimately, the core lesson of this article is simple but significant: offences against women and children in the digital age are not separate from mainstream criminal justice; they are now one

¹⁸⁶ *Id.*

¹⁸⁷ Protection of Children from Sexual Offences Act, 2012, *supra* note 72.

¹⁸⁸ Bharatiya Nyaya Sanhita, 2023, *supra* note 10.

¹⁸⁹ Indian Cyber Crime Coordination Centre, *supra* note 26.

¹⁹⁰ *Id.*

of its defining tests. A legal system that cannot protect dignity online cannot fully protect dignity at all. If India is to build a safe digital society, it must treat cyber violence against women and children not as an accidental side-effect of technology but as a serious structural wrong demanding a coordinated response from law, institutions and society. Only then can the promise of the internet be aligned with the constitutional commitment to equality, safety and human dignity for all.

VII. BIBLIOGRAPHY

1. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023 (India).
2. Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India).
3. Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023 (India).
4. Code of Criminal Procedure, 1973 (India).
5. Constitution of India, 1950.
6. Immoral Traffic (Prevention) Act, 1956, No. 104 of 1956 (India).
7. Indian Penal Code, 1860 (India).
8. Information Technology Act, 2000, No. 21 of 2000 (India).
9. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
10. Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2 of 2016 (India).
11. Protection of Children from Sexual Offences Act, 2012, No. 32 of 2012 (amended 2019) (India).
12. Protection of Children from Sexual Offences Rules, 2020 (India).
13. United Nations Convention on the Rights of the Child, GA Res 44/25 (20 November 1989).
14. *Avnish Bajaj v. State (NCT of Delhi)*, 2005 SCC OnLine Del 1362.
15. *Independent Thought v. Union of India*, (2017) 10 SCC 800.
16. *Jayaprakash P.P. v. Sheeba Revi*, 2017 SCC OnLine Ker 21544.
17. *Pawan Kumar v. State of Himachal Pradesh*, (2017) 7 SCC 780.
18. *Sakal Papers (P) Ltd. v. Union of India*, AIR 1962 SC 305.
19. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

20. *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004 (Egmore Magistrate 2004).
21. *The Registrar (Judicial), Madurai Bench of Madras High Court v. Secretary to Government, Union Ministry of Communications*, Suo Motu W.P. (MD) No. 16668 of 2017 (Madras HC).
22. Pavan Duggal, CYBERLAW: THE INDIAN PERSPECTIVE (5th edn, 2020).
23. Debarati Halder and K. Jaishankar, CYBER CRIME AND THE VICTIMISATION OF WOMEN: LAWS, RIGHTS AND REGULATIONS (2011).
24. K. Jaishankar, CYBER CRIMINOLOGY: EXPLORING INTERNET CRIMES AND CRIMINAL BEHAVIOUR (2011).
25. Ved Kumari, JUVENILE JUSTICE SYSTEM IN INDIA: FROM WELFARE TO RIGHTS (2010).
26. Ved Kumari, THE JUVENILE JUSTICE (CARE AND PROTECTION OF CHILDREN) ACT 2015: A CRITICAL ANALYSIS (2017).
27. Prashant Mali, CYBER LAW AND CYBER CRIMES (3rd edn, 2020).
28. N.S. Nappinai, TECHNOLOGY LAWS DECODED (2017).
29. Vakul Sharma and Seema Sharma, INFORMATION TECHNOLOGY LAW AND PRACTICE (7th edn, 2022).
30. National Crime Records Bureau, CRIME IN INDIA 2023 (Government of India 2024).
31. National Commission for Protection of Child Rights, GUIDELINES ON PREVENTION OF BULLYING AND CYBERBULLYING (2023).
32. Centre for Communication Governance, GENDERED DIMENSIONS OF ONLINE HARASSMENT IN INDIA (2024).
