

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

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

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

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

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

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

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

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

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

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

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

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

DIGITAL SEXUAL EXPLOITATION OF WOMEN AND CHILDREN: LEGAL CHALLENGES AND THE NEED FOR EFFECTIVE REGULATION

AUTHORED BY - MANAS UNNIKRISHNAN (ASSISTANT PROFESSOR)

CO-AUTHOR - ABHIRAMI PRASAD (LLM STUDENT)

ABSTRACT

Digital technology is growing fast, leading to new ways of sexual exploitation such as non-consensual sharing of intimate images; sextortion; online grooming; cyber-stalking; and AI-generated sexual deepfakes. Women and children are especially at risk of these types of abuse, exacerbated by the anonymity of the abuser, harmful content and challenges to cross-border enforcement. The present paper will look at the regime of sexual exploitation by intermediaries in digital space with reference to the Information Technology Act, 2000 and Bharatiya Nyaya Sanhita, 2023 and the Protection of Children from Sexual Offences Act, 2012. It points out the main gaps in the current legislation, which include three fields: fragmentation, consent, synthetic sexual pictures, online grooming and the platforms' responsibility for and investigation of digital evidence. The paper will take into account constitutional principles such as equality, privacy, dignity and non-deprivation, as well as international conventions on child protection. It is supportive of the need to bring about greater clarity in definitions, coordination and action with regard to new forms of digital abuse. Finally, it proposes a uniform, rights-based regulatory approach which is more transparent, provides better remedies and strikes a balance between content regulation and freedom of expression.

Keywords: Digital Sexual Exploitation, Technology Facilitated Gender Based Violence, Online Child Sexual Abuse, Intermediary Liability and AI-Generated Sexual Deepfakes.

I. INTRODUCTION

Digital technology is developing at a swift pace, changing how communication, information sharing and social interaction are done. The digital tools have also opened up new possibilities for sexual abuse and exploitation, however. Non-consensual sharing of intimate images, sextortion, cyberstalking, online grooming, livestreamed abuse, and the generation of sexual

deepfakes by artificial intelligence illustrate how technology can be used to infringe on individual autonomy, dignity and privacy. Digital sexual exploitation is different from many other forms of offline abuse, in that the harmful content can be reproduced and disseminated over and over, perpetuating the harm long after the event.¹

While the nature of women's and children's experiences may be different, they are particularly vulnerable to technology-facilitated sexual exploitation. Sexual harassment, threats of intimate images, and the unauthorised creation or dissemination of sexually explicit content are all types of online sexual harassment that may occur to women. Children can be targeted through child sexual abuse material production or distribution, child sexual enticement and online grooming. Such abuse may be detrimental to the mental, social and reputational health of the victim. In addition, investigations and access to effective legal remedies are hindered due to the anonymity of perpetrators and the quick propagation of content and the international nature of online platforms.²

A few laws have been enacted covering this, such as the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, the Bharatiya Nyaya Sanhita, 2023 and the Rules of intermediaries in the information technology sector. These laws address various aspects of cybercrime, sexual offences and child protection, but new technologies present challenges to the effectiveness of the laws. There is a lack of clear definitions, enforcement and platform responsibility with respect to the sharing of CSAM, the use of AI to create sexual content, and the sharing of images and photographs that are not consensual. Furthermore, it can be challenging to preserve digital evidence, to investigate, and to offer prompt remedy for victims in this fragmented organisation.³

More than criminalisation is needed for effective regulation. It should also be mindful of the obligations of digital intermediaries, reporting systems and disappearance systems and the

¹ Daniel Manoj et al., Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation, 4 Child Prot. & Prac. 100088 (2025); Manu Ahlawat, Cyber Violence Against Women: Emerging Legal Challenges and the Need for Gender-Sensitive Digital Protection Laws, 4 Indian J.L. 1 (2026).

² Aritra Biswas, Cybercrimes, Women's Safety, and Child Protection: A Comprehensive Analysis of Legal Frameworks, Challenges, and Remedial Strategies, The Lawway with Lawyers J. (Aug. 15, 2025); Sumi S. Shaji, Safeguarding Digital Vulnerabilities: A Socio-Legal Examination of Cyber Violence Against Women and Children Within India's Contemporary Penal Framework, 9 Int'l J.L. Mgmt. & Human. 3764 (2026).

³ Information Technology Act, No. 21 of 2000, §§ 66E, 67, 67A, 67B, 79 (India); Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 75, 77–79, 294, 308 (India); Protection of Children from Sexual Offences Act, No. 32 of 2012, §§ 11–15 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Feb. 25, 2021).

remedies that can be provided to those affected. The regulations need to make a clear distinction between violations of sexual activity and legal discussion in the meantime, or otherwise arbitrary censorship will likely be imposed. The establishment of a framework which will enhance protection for victims, criminal accountability and effective enforcement is important.⁴ This should be done in compliance with the constitutional and international human rights principles. Equality and justice are the basis of our Indian Constitution, which is based on equality and non-discrimination, dignity, privacy and personal liberty of all individuals, as mentioned in Articles 14, 15 and 21 of the Constitution.⁵ The Convention on the Rights of the Child and the Committee on the Rights of the Child (CRCEC) General Comment No. 25 underscore the need to protect children from violence, exploitation and abuse in digital environments internationally.⁶ Therefore, the paper calls for an effective and coherent regulatory approach utilising a rights-based approach, ensuring greater accountability, improved victim support and that it is responsive to new means of digital sexual exploitation.

II. THE IMPACT AND NATURE OF DIGITAL SEXUAL EXPLOITATION

A. Defining Digital Sexual Exploitation

Digital sexual exploitation is defined herein as the use of information and communication technologies to sexually abuse or exploit a person without valid consent, or in the case of a child, without circumstances that would allow valid consent. In the literature, sexual abuse is differentiated from sexual exploitation, which implies some gain for a second party, financial or otherwise, as well as the production, circulation and sharing of child sexual abuse material. The United Nations Office on Drugs and Crime taxonomy of technological harms to children is divided into five categories: child sexual abuse material; commercial sexual exploitation; online enticement, solicitation and grooming; cyberbullying, harassment and stalking; exposure to harmful content.⁷ For adult women, the concept of scholarship begins to refer to technology-facilitated gender-based violence, including: non-consensual circulation of intimate images, sextortion, synthetic sexual imagery, stalking, doxing and coordinated sexualised trolling.⁸ The law doesn't define 'gender-based violence', and therefore the law is used to describe behaviour that was drafted for other purposes, resulting in a loss of the

⁴ Ahlawat, supra note 1; Shaji, supra note 2.

⁵ INDIA CONST. arts. 14, 15, 21

⁶ Convention on the Rights of the Child arts. 3, 19, 34, 36, Nov. 20, 1989, 1577 U.N.T.S. 3; U.N. Comm. on the Rts. of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).

⁷ Manoj et al., supra note 1, at 2

⁸ Biswas, supra note 2, § 3.1

gendered nature of the violence.

B. The Nature and Impact of Digital Sexual Abuse

Three aspects of digital sexual exploitation are different and have legal implications. What is one thing that stands out about them? Persistence is the first one. After the image has been uploaded, it can be copied to other websites, messaging systems and storage devices, making it very difficult to destroy images, and the person who is being portrayed will again be hurt each time they are viewed or sent.⁹ Solutions based on a single act or a single publication were not an adequate fit to this harm. The second is anonymity and reach. Victims may be in a different jurisdiction, as may be the offenders who operate under fake identities and use global virtual private networks, encrypted channels and platforms.¹⁰ The third is continuity of online harm. Online abuse of children is closely related to offline abuse; online grooming leads to physical abuse, and online cyberstalking can become a physical assault. Each of these features is accentuated by the social context. The stigma, the idea that the family has to be protected, and the concept of victim blame prevent reporting; when victims report, they are met with secondary victimisation by family and institutions to which they go, and they see that offenders will not be reported.

C. Constitutional and International Standards

Article 21, in light of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, ensures privacy and dignity and Articles 14 and 15 ensure equality and non-discrimination based on sex. They collectively impose a responsibility on the State which is applicable to the digital realm.¹¹ In accordance with Article 15(3), special provision is made for women and children, and Article 39(f) protects children from exploitation.¹² International law is specific. Online violence against women should be prevented and protected, investigated and remediated at the state level.¹³ The Convention on the Rights of the Child, to which India is a party, places paramount importance on the best interests of the child and requires States to take all possible measures to protect children from violence, as well as sexual exploitation and abuse and its Optional

⁹ Manoj et al., *supra* note 1, at 3; Ahlawat, *supra* note 1, at 7.

¹⁰ Shaji, *supra* note 2, at 3767, 3781; Biswas, *supra* note 2, § 5.1.

¹¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India); India Const. arts. 14, 15, 21; Ahlawat, *supra* note 1, at 4–6.

¹² India Const. arts. 15(3), 39(f).

¹³ Ahlawat, *supra* note 1, at 5 (citing U.N. Special Rapporteur on Violence Against Women, Its Causes and Consequences, Report on Online Violence Against Women and Girls from a Human Rights Perspective, U.N. Doc. A/HRC/38/47 (June 18, 2018)).

Protocol on the sale of children, child prostitution and child pornography is most directly relevant to the material in question.¹⁴ These rights have been affirmed by the Committee on the Rights of the Child and the Committee on the Elimination of Discrimination against Women, respectively, in the digital environment and in technology-mediated environments, respectively.¹⁵

The standards cut across, as will be seen, that protection is one of many rights. Children have online participation rights and provision rights (right to information, education, play and association), and blanket protections of those rights can cause harm. The Madras High Court's ban and later lifting of the TikTok application is a good example of how such decisions can be made by prohibitive measures only rather than policy-making. The Supreme Court in *Shreya Singhal v. Union of India* has stated that Section 66A of the IT Act is unconstitutional due to its being overbroad and vague.¹⁶

III. LEGAL FRAMEWORK IN INDIA

A. Offences Against Women

The offences that can be committed against the online sexual abuse of women are distributed over various parts of the IT Act and the BNS. The IT Act contains provisions that punish the capturing, publishing, or transmitting of an image of a private area of a person, in circumstances that offend the right to privacy (section 66E); the publication or transmission of obscene (section 67) and sexually explicit material (section 67A) in electronic form; and identity theft and cheating by personation (sections 66C and 66D), which lead to fake profiles.¹⁷ The BNS includes, in addition to the general provisions on obscenity and extortion, offences relating to sexual harassment, voyeurism, stalking (including monitoring a woman's use of the internet/electronic communication), and words or acts which insult a woman's modesty.¹⁸ The term “sextortion” is used interchangeably with the term “extortion”, and is prosecuted primarily under the provisions of the IT Act in addition to the provisions of the term “extortion”.¹⁹

¹⁴ Convention on the Rights of the Child arts. 3, 19, 34, 36, Nov. 20, 1989, 1577 U.N.T.S. 3; Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, 2171 U.N.T.S. 227; Shaji, *supra* note 1, at 3787.

¹⁵ U.N. Comm. on the Rts. of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021); Comm. on the Elimination of Discrimination Against Women, General Recommendation No. 35 on Gender-Based Violence Against Women, Updating General Recommendation No. 19, ¶ 20, U.N. Doc. CEDAW/C/GC/35 (July 14, 2017).

¹⁶ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

¹⁷ Information Technology Act, 2000, No. 21 of 2000, §§ 66C–66E, 67, 67A (India)

¹⁸ Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 75, 77–79, 294, 308 (India)

¹⁹ Bharatiya Nyaya Sanhita § 308; Shaji, *supra* note 2, at 3769–70.

Section 66A of the Indian Telegraph Act was struck down in the case of Shreya Singhal as it was a very wide provision covering offensive electronic communications. Since then, prosecutions for online harassment have been based on Section 67 and the stalking and modesty provisions of the penal code, with the introduction of Section 67 following the content being sexual in nature.²⁰ The ruling was constitutionally necessary because the provision had been used to shut down a social media post criticising a political leader's death, among the many instances of the provision's vague language.

The first approach is that if the content is generated through morphed images and deep fakes, then the problematic element isn't authenticity but rather any impact on privacy and dignity, which falls within the scope of sections 66E and 67. The other side of this is that there are no specific provisions on AI content in the IT Act, provisions on voyeurism and privacy were written before it was possible to manipulate content, and the fast rate of creation and distribution makes it impossible to remove AI content. The passages are very difficult to read. It is a section that is directed against images of the private parts of the body, which have been taken and/or sent in a situation that infringes on the right to privacy, and does not obviously apply to an image in which the woman's face is covered on another body. Since then, the executive has become the leader of the legislature. The new Intermediary Guidelines and Digital Media Ethics Code Rules that were notified on 10 February 2026 and will come into effect on 20 February 2026 introduce the concept of 'synthetically generated information', add to the prominence of labelling for allowed synthetic content, introduce the notion of embedded provenance for allowed synthetic content, and also shorten timelines, among others, and introduce easier requirements for takedowns of information in line with lawful takedown orders and, according to secondary news reports takedowns under complaints about nonconsensual intimate imagery to two hours instead of three hours.²¹

B. Offences Against Children

In case of an offence against children, the provisions of POCSO and section 67B of the IT Act are applicable. POCSO treats the following as sexual harassment of a child: "repeatedly and constantly following, watching or contacting a child through electronic means and encouraging the child to engage in pornography", and prescribes up to three years' imprisonment and a

²⁰ Shreya Singhal, (2015) 5 SCC 1; Shaji, *supra* note 2, at 3767, 3770.

²¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Feb. 10, 2026); see also IT Rules 2026, iPleaders (July 29, 2026), <https://blog.ipleaders.in/it-rules-2026/>

fine.²² Section 67B of the IT Act punishes the publishing or transmission of material that contains representations of a child engaging in sexually explicit conduct, and the cultivation, enticing or inducing of a child in an online relationship to engage in sexually explicit conduct. It is punishable with up to 5 years' imprisonment and a fine up to ₹10 lakh on first conviction and up to 7 years on second conviction.²³ Sections 13, 14 and 15 of POCSO deal with the exploitation of the child for pornography and the storage, sharing and commercialisation of such pornography. The amendment to section 2(1) in 2019 added a definition of child pornography that encompassed computer-generated images that appear to be a child and images that are created, adapted or modified to look like a child.²⁴

The Supreme Court's decision in *Just Rights for Children Alliance v. S. Harish* is the most significant recent development. The Court had struck down a Madras High Court decision which had held that simply storing or possessing such material does not constitute an offence and suggested that section 15 of POCSO must include constructive possession and that Parliament should consider changing the definition of child pornography to child sexual exploitation and abuse material.²⁵ There is only an indirect discussion on grooming. It is not mentioned in either POCSO or the IT Act, nor in any of the legislation of the United Kingdom, the United States, the European Union and Australia (as compared in one study). The POCSO provision gives a maximum of three years' imprisonment, while section 67B gives a maximum of five years' imprisonment. It is also a definitional issue, as it can be hard to distinguish abusive online approaches from the legitimate online connections that are part of children's participation online, which can make loose drafting dangerous on both ends.

Sharing images among adolescents highlights an internal conflict. All persons under 18 years are treated as children under POCSO and the IT Act and therefore images of their intimate parts, even if created by them, are treated as CSAM. When it comes to matters of consent, the situation is fluid, as children may do things because of peer pressure, and because they don't know or understand how to use the law to protect themselves; if the child who created or posted the image is considered an offender, then the purpose of the law is undermined.²⁶ The

²² Protection of Children from Sexual Offences Act, No. 32 of 2012, §§ 11–12 (India); Manoj et al., *supra* note 1, at 4.

²³ Information Technology Act § 67B.

²⁴ Protection of Children from Sexual Offences Act §§ 2(1), 13–15; Protection of Children from Sexual Offences (Amendment) Act, No. 25 of 2019 (India).

²⁵ *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716 (India)

²⁶ U.N. Comm. on the Rts. of the Child, General Comment No. 20 (2016) on the Implementation of the Rights of the Child During Adolescence, ¶ 40, U.N. Doc. CRC/C/GC/20 (Dec. 6, 2016); Aratrika Choudhuri, *Conceptualising Children's Rights in Digital Spaces: Emerging Issues and Challenges*, 15(2) Socio-Legal Rev. 151, 176 (2019); Shaji, *supra* note 2, at 3778.

Committee on the Rights of the Child has called on States to refrain from using the repressive criminalisation device to control consensual adolescent sexual activity, while literature from India has highlighted the need of restorative practice and counselling in differentiating a circuit of exploitation from experimentation amongst adolescents. Indian law does not have a specific offence for cyberbullying. Depending on the acts committed, the requirements of section 67 of the IT Act and the child-protection mechanism under the Juvenile Justice Act may be applicable, but the Juvenile Justice Act does not provide for aftercare of survivors of online abuse and the action of children who abuse other children through technology.

C. Intermediary Regulation

There are two principles through which intermediaries are regulated: one under section 79 of the IT Act, which states that they are not liable for the content of third parties as long as they exercise "due diligence", and the other being the Intermediary Guidelines and Digital Media Ethics Code Rules, 2021. There are various duties on the compliance side and specific nodal-officer duties for significant social media intermediaries, including the requirement to publish rules and privacy policies, and to remove specified categories of content on complaint within twenty-four hours, including content that shows private areas of a person or depicts sexual acts, or morphed impersonations.²⁷ When it came to section 79(3)(b) of the Act, in Shreya Singhal, the Court restricted the scope of imposing liability based on a private complaint by reading into it the requirement of a court order or a government notification. The power to block public access to information is provided by section 69A.²⁸

D. Investigation, Digital Evidence and Enforcement Mechanisms

The procedure has been updated. Further, a first information report and issue of process may be made on electronic medium and, as per the Bharatiya Sakshya Adhiniyam, 2023, the electronic records such as screenshots and photographs of the electronic devices and records of servers used for recording electronic records shall be stamped and signed.²⁹ POCSO has established Special Courts and child-friendly procedures. The Indian Cyber Crime Coordination Centre (ICCC) in the Ministry of Home Affairs coordinates the enforcement of

²⁷ Information Technology Act § 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Feb. 25, 2021); Ahlawat, *supra* note 1, at 6; Shaji, *supra* note 2, at 3768, 3771.

²⁸ Information Technology Act § 69A.

²⁹ Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 173 (India); Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63 (India); Shaji, *supra* note 2, at 3772–73.

cybercrime and operates the National Cyber Crime Reporting Portal, which has a specific section for women- and child-related offences and a National helpline, along with forensic labs. Examples of intelligence-led and preventive enforcement include Operation Megh Chakra by the Central Bureau of Investigation (CBI) to combat online child sexual abuse and Operation P-Hunt by the Kerala Police. There is also an e-box (children can report through) known as a POCSO e-box, but not a lot of awareness about it. Policing is state-related, and the level of policing will depend on state capacity.³⁰

IV. GAPS IN THE CURRENT LAWS

A. Legislative Fragmentation and Inconsistent Penalties

Digital abuse can involve obscenity, harassment, extortion, mental cruelty and ultimately physical abuse, so an element can be charged in one case. Also, the costs are apparent. Penalties vary depending on similar actions, as illustrated by the example of grooming. There isn't any definition under Section 67B itself, and literature suggests that the definition could be borrowed from Section 13 under POCSO.³¹

Overlap is another area of uncertainty as to what the appropriate charge is. In the case of *Sharat Babu Digumarti v. Government of NCT of Delhi*, the Supreme Court accepted that the Electronic publication of obscene material is regulated by a special law, namely, the IT Act and prosecution under general penal provisions on obscenity could not be continued.³² Later practice is reported in various ways. One says that in general, the parallel charges are allowed provided there is no double punishment, and another says that the IT Act has the superior position to general provisions against computer offences in the eyes of the court in Bombay. It is not yet a clear-cut practice whether, and to what extent, the special-law principle takes precedence over BNS provisions in cases of image-based abuse, extortion and stalking.

B. Image-Based Abuse: Obscenity and Consent

Obscenity is the route by which image-based abuse gets into the IT Act (sections 67 and 67A) and through a privacy provision which is limited to images of private parts (section 66E). Whether the material is lascivious or prurient is a question for obscenity law. It focuses on the nature of the content, rather than whether the person depicted gave consent to its creation or

³⁰ INDIA CONST. sch. VII, List II, entry 2; Biswas, *supra* note 2, § 4.2; Shaji, *supra* note 2, at 3783.

³¹ Manoj et al., *supra* note 1, at 4–5.

³² *Sharat Babu Digumarti v. Gov't of NCT of Delhi*, (2017) 2 SCC 18 (India).

circulation, and therefore focuses on the content, rather than on its impact on the victim.³³ The orientation is not based on human rights but on moral values, which has been a criticism of the Indecent Representation of Women (Prohibition) Act, 1986 for long. On their face, the 'whoever' language of the provisions could extend to a person who created or published the content, and complainants were allegedly questioned about their dress and appearance.³⁴ The consequences are very real: victims of the images are re-victimised during the reporting process, and trials are often conducted on what kind of images were produced, rather than whether or not they were the wrong images, produced without trust and consent.

C. Platform Accountability and Risk of Over-Removal

The two crucial questions being posed are: What platforms can and should be doing more than just takedown, and how can platforms monitor the wrong takedown? We have already seen variations in the level of moderation, delayed responses, problematic moderation systems which define sexualised abuse as a disagreement, women being targeted and penalised for their sexualised abuse, and 'foreign' platforms that may not see this behaviour as illegal.³⁵ From cutting down on the section 79 protections for those in the middle of gender-based violence to introducing child-safety policies and regular audits and ombuds for platforms that profit from children's data. On the second, liability-driven regimes encourage intermediaries to avoid anything that risks liability, resulting in privatised censorship of lawful expression, including of children. The same concern is evident in the knowledge standard, as presented by Shreya Singhal, and in the case of automated detection, there are risks of both surveillance and false-positive detection. Any reform must therefore make a distinction between types of content. In the context of child sexual abuse material and non-consensual intimate imagery, there is no argument that this is illegal and duties can be stringent and proactive.

V. TOWARDS A COHERENT REGULATORY FRAMEWORK

A. Harmonising Existing Laws

One study suggests a specific statute on online sexual abuse of children which would have overriding effect; another defines statutory overlap as a positive feature; and a third suggests that the statutory definition of technology-facilitated gender-based violence should include

³³ Ahlawat, *supra* note 1, at 6

³⁴ Akanksha Pathak & Prateek Tripathi, *Digital Victimization of Women in Cyberspace: An Analysis of Effectiveness of Indian Cyber Laws*, 7 NLUA L. Rev. 168 (2023)

³⁵ *Id.*

ingredients of proof.³⁶ Harmonising first is the better way. The IT Act should have a common definitions provision which would establish definitions as such to define child sexual exploitation and abuse material, grooming, intimate image, synthetic sexual content and technology-facilitated GBV. Should correlate penalties with similar conduct and make it clear which provision will take precedence when multiple provisions are involved. If the amendment is not coherent, then a consolidated statute should be considered only if it will not supplant the existing statutes.

B. Non-Consensual Intimate Images and Deepfakes

The offence should be triggered by the lack of consent of the person depicted in the case of an adult. It should include provisions for the creation, publishing, or transmission (or threatened transmission) of an intimate image, whether the image is real or fabricated or altered, without a requirement that it show obscenity; should have aggravated provisions when the image is transmitted for extortion or coercion; and should clarify that someone who creates or shares her own image is not an offender.³⁷ The provision shall include the means of remedial action such as takedown orders and images for hash-matching. For children, the statutes should take the terms proposed in Harish, keep the realistic-image requirement in the 2019 definition, and explicitly include synthetic and stylised depictions of children.³⁸

C. Grooming and Adolescent Image-Sharing

A standalone offence of online grooming should be applicable irrespective of whether a meeting is arranged, should include some harmonisation between POCSO and the IT Act and finally, should include proof of sexual intent to ensure that age-appropriate interactions online are not caught up. It is most appropriate that the law also protects adolescents, as guidance should be given to prosecutorial authorities and procedures should be established for the diversion from prosecution of consensual image sharing between similarly aged minors, with restorative and counselling responses, and coercion, blackmail and onward circulation, if not prohibited, at least fully punished. What it does not need is to lower the age of consent, what it does need is the difference between exploitation and experimentation in the exercise of

³⁶ Manoj et al., supra note 1, at 8; Shaji, supra note 2, at 3779–80; Ahlawat, supra note 1, at 10.

³⁷ Ahlawat, supra note 1, at 10; Shaji, supra note 2, at 3769, 3789.

³⁸ Just Rights for Children Alliance, 2024 INSC 716; Manoj et al., supra note 1, at 5; Shaji, supra note 2, at 3787, 3789.

discretion.³⁹

VI. CONCLUSION

There is growing evidence that digital technology has emerged as an important instrument in child and female exploitation, and the law must adapt to the nature of the technology. Online sharing of intimate photos, online grooming, sextortion, cyberstalking and A.I. generated deepfakes all constitute digital tools that can invade personal autonomy, dignity, and privacy. The potential for harmful material and anonymity of the offender and the cross-border nature of electronic communication can make these offences hard to prevent and/or prosecute and can harm the victim of an offence with ongoing stigma and psychological distress. These offences have a pivotal place in Indian laws, including the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 and the Protection of Children from Sexual Offences Act, 2012. But there are still some issues that need to be addressed concerning AI-generated sexual content, online grooming, and the sharing of intimate content without consent. Current protections are constrained by unclear definitions, the lack of consistent laws, and the lack of consistent enforcement. Moreover, too much emphasis on the nature of content can cause consent to be overlooked, and the person depicted's dignity to be violated.

Harmonised statutory definitions, clear rules on synthetic sexual content, reporting systems which are easy to access, and material removed on time are essential for effective regulation. Digital intermediaries should be held accountable for their activities in a very specific way and arbitrary censorship should be prevented and, above all, lawful expression. In addition, maintaining and collecting digital evidence and performing forensic analysis are significant, as are institutional support and assistance to victims. Where children are involved, the law must continue to protect, and be responsive but proportionate and sensitive. Finally, there must be a move away from punishment towards prevention and meaningful remediation for those who have been abused. A coherent, forward-looking, rights-based legal framework can enhance accountability while at the same time protecting fundamental freedoms. Legislation, effective enforcement with a focus on the needs of victims, can move India towards a safer digital environment for women and children.

³⁹ Choudhuri, *supra* note 26, at 157–59; U.N. Comm. on the Rts. of the Child, General Comment No. 20, *supra* note 26.