Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

# Right to Privacy of Women and Children in Cyberspace: Legal Frameworks and Challenges for Protection Against Cybercrime and Surveillance

**Ms. Dev Kaur[1], Prof. (Dr.) Amar Nath[2]**

[1]Research Scholar, Faculty of law, Agra college, Agra, Dr. Bhim Rao Ambedkar University, Agra (UP)
[2] Professor, Faculty of Law, Agra college, Agra, Dr. Bhim Rao Ambedkar University, Agra (UP)

**Abstract**

This research paper analysis the legal frameworks and determined challenges in safeguarding the right to privacy of women and children from cybercrimes and digital monitoring in cyberspace in India. The paper examines prevailing legal provisions, which includes the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 and the recently enacted Digital Personal Data Protection Act, 2023. The study deals with the particular susceptibilities of women and children in context to online threats such as sexual harassment, cyber stalking, and without consent transmitting of private intimate images. The paper recognizes important key challenges, involving the cross-jurisdictional nature of cybercrime, absence of digital literacy, and the fast growth of technological developments that frequently overtake legal provisions.

To conclude, it recommends policy solutions and legal improvements to reinforce protecting measures and guarantees a harmless digital environment for the women's and children's. The study suggests strong recommendations to fortify Indian cyber legal framework, highlighting the requirement of vigorous legislation to protect women and children in this digital world.

**Keywords:** Right to privacy, Women and Children, Cybercrime in Cyberspace.

## 1. Introduction

In this digital world, internet and digital technologies had become an essential part of our modern life, providing various benefits regarding communication, health, education and social life. Although, these technologies had generated new and multifarious problems, specifically for vulnerable groups like women and children. These groups are unreasonably targeted by different forms of cybercrimes such as, cyberstalking, cyberbullying, sexual harassment and the distribution of child sexual abuse material (CSAM).

The landmark case of the Supreme Court named as K.S. Puttaswamy case in year 2017 legally recognized right to privacy as a fundamental right in India. This research paper explores the legal landscape intended to deal with these issues, censoriously evaluate its limitations, and recommends an exhaustive way to create a safer and secure digital environment for women and children.

### 1.1 Cyber Crime against Woman and Children

In today's digital world, cybercrimes against women and children are increasing day by day and they have been extremely persecuted in the cyberspace. Some computer hackers with malafide intention defame women and children. Hackers illegally follow women and children on social media platforms, transmitted obscene and vulgar text and images and also convert their images to create pornographic videos. They use their pictures without their consent of these women and children's. Majority of the times, the aggrieved party is not aware of such types of incidents. When the incident comes to their knowledge, the aggrieved party feel doubtful and due to lack of proper knowledge can't report against the cybercrime. In most part of the India, cybercrimes are increasing at a shocking pace. Mostly teenage girls and boys are the victims and easily falling in the trap of such criminals. These cybercriminals mostly target these vulnerable groups with a malafide intention to make wrongful gain (Minakshi Kumawat, 2023) [1].

## 2. Legal Frameworks

There are multiple legal statutes in our Indian legal framework to address the cybercrimes, which are:

### 2.1 Information Technology Act, 2000 (IT Act)

In this digital world, the most persistent issue is the speedy growth of technological expansion, which often considered prevailing legal statutes out-dated. For example, the Information Technology Act, 2000 was innovative for its time, but in this modern era the said statute was not able to combat serious threats such as Artificial Intelligence deepfakes, illegal cyber training, internet abuse, or encoded communication on social media portals (Anshul Kumar Manik, 2025) [2].

Section 66E of the IT Act, specifically provide punishment for violation of privacy, on the other hand Section 67 and 67A of the said Act provide punishments for Publication or Transmission of Obscene and Sexually explicit content in electronic form. And Section 67B deals with the Publishing or Transmitting of contents related to children's in sexually explicit act.

### 2.2 The Bhartiya Nyaya Sanhita, 2023 (BNS)

The newly enforced "Bhartiya Nyaya Sanhita, 2023 (BNS)" is a part of India's future legal reform, which substitutes the out-dated Indian Penal Code. The Sanhita includes specific measures to address current severe crimes also includes cybercrimes. We have discussed some important legal provisions regarding cybercrimes against women and children under BNS, 2023 (Himani Ahlawat, 2024) [3].

**2.3 Defamation and Cyber Harassment:** The Sanhita provides more precise definitions and severer punishments for the offence of "Cyber Harassment" and "Defamation", which unreasonably disrespect and harm women. Section 75 of the BNS defines the offence of Sexual Harassment and Section 356

defines the offence of Defamation. The Sanhita pursues to improve the legal vocabulary such as cyber bullying, cyber stalking, and derogatory and defamatory statements in social media platforms [3].

**2.4 Cyber Stalking:** Cyber stalking is considered as the most common and popular cybercrime in this digital world. Cyberstalking is an act where the offender repeatedly harasses or threats the victims through internet. Cyberstalking is committed when the offender continuously follows or monitors the victim through internet and leave an undesirable message. The ultimate objective for the offence of cyberstalking is:

- Sexual Harassment
- Unwanted sexual desires
- Revenge or hate
- Establishing a relationship

The cyber stalkers mostly target their victims through personal emails as well as public messages. Most common age group who are aggrieved in this offence is between 16 to 35 [1].

**2.5 Morphing:** Morphing is an offence where an unauthorized person uses someone's identity download's victim's images and posts or upload them after editing to annoy or threat someone [1].

**2.6 Email Spoofing:** Email spoofing is an offence consists of illegal activities through email where the sender's email address and other important credentials of the email has been altered or remove as it appears that the said email has been originated from a different unknown source [1].

**2.7 Revenge Porn and Digital Voyeurism**: Revenge porn and Digital Voyeurism is most common offence against the women committed in this digital world. The BNS makes severe provisions for the offence of Digital Voyeurism under section 77. The said offence is being committed where the offender transmitted the personal photos and images when the women are indulge in her private act without her consent. The BNS expressly defines heavy fines along with imprisonment to such persons who committed the said offence [3].

**2.8 Cyber Flirting:** Cyber flirting is an offence which generally considered as a petty offence. The said offence is being committed when the offender makes obscene messages and songs and tries to control the victim with his activities that leads to cyber sexual defamation and breach of modesty [1].

**2.9 Cyber Bullying:** Cyber bullying is an offence where the offenders with the help of internet or electronic communication harass a person, usually by sending threatening or intimidating messages. The key objective to commit such type of crime is to defame the victim out of hate, frustration or anger or when the offender makes fun of the image of the victim in front of his friends, classmates, colleagues, or unknown peoples. Facebook, Instagram, etc. are such social networking portal which is considered to be the main source of cyber bullying [1].

**2.10 Protection of Children from Sexual Offences Act, 2012 (POCSO Act)**

The POCSO Act was considered to be an essential legal statute in context to address the sexual offences towards minors, including those committed through online ways. There are some important provisions:

**Section 11:** Section 11 of the POCSO Act deals with the offence of "Sexual Harassment" committed upon a child. The said offence is being committed when the offender:

- Speaks any word or creates any sound, making any gestures or shows any object or part of his body; or
- Makes a situation where the child shows his body or any part of the body; or
- Shows any objective in a digital form to a child for pornographic purpose; or
- Continuously follow or stalk a child through any electronic or digital means; or
- Threatens a child to make a fabricated videography of any sexual act; or
- Seduces a child for pornographic purposes.

**Section 13:** The offence under this section is being committed, when the offender uses a child in any media form such as television programme, advertisement, television channel, internet or other electronic from, with an intention of sexual fulfilment, which includes:

- Showing sexual organs of the child;
- Child being engaged in real or stimulated sexual acts;
- Offensive or Indecent representation of the child.

**Section 14:** Section 14 deals with the punishment where the offender is using child for the purpose of pornography. The accused person shall be liable to an imprisonment not less than five years and also be liable to fine, in case of second conviction the imprisonment not less than seven years along with fine.

**Section 15:** Section 15 of the Act deals with the punishment,

- Where any person stores or possesses such pornographic material, but fails to delete them with an intention to share. The accused shall be liable to a maximum fine of Five Thousand Rupees and in subsequent conviction a maximum fine of Ten Thousand Rupees.
- Any person who stores or possesses such material for the purpose of transmitting, displaying or distributing such content shall be liable to imprisonment of Three years, or fine, or both.
- Any person who stores or possesses such pornographic material for the commercial purpose shall be liable to an imprisonment not less than Three years but extends to Five years, or fine, or both and in case of subsequent conviction, with an imprisonment of Five years which extends to Seven years and fine.

### 2.11 Indecent Representation of Women (Prohibition) Act, 1986

**Section 4:** Section 4 of the said Act makes prohibition on publication or sending through post of books, pamphlets, etc. which contains indecent representation of the women in any form. According to this section, no person can sell, let to hire, transmitted, circulate or send through post any paper, books, films, photograph or any material which contains indecent representation of women.

### 2.12 Digital Personal Data Protection (DPDP) Act, 2023

Under the DPDP Act, when the authority processes any personal data belongs to a child under the age of 18 years, the consent shall be obtained from the parents of such child or from the lawful guarding in such a manner as may be prescribed by the authority. Additionally, the data fiduciary is being

responsible that the processing of child's personal data doesn't harm its reputation or well-being. Moreover, surveillance or behavioural monitoring of children is severally prohibited (Anuradha Gandhi, et al., 2024) [4].

## 3. Key challenges

In spite of these legal frameworks, there are various complications which obstructs in effective privacy protection. Which are as follows:

**3.1 Technological Gap** (Dr. Sandeep Kumar, et al., 2025) [5].

In this modern digital world, technology is evolving very fast day by day, and cyber-attacks are comparatively more advanced and faster as compare to people's knowledge and awareness.

The speedy growth in the digital technology often exceeds the limits of presiding laws and a safety procedure, which leads to individuals mostly children are the aggrieved party into these evolving cybercrimes.

Dealing these factors through exhaustive education, awareness campaigns, enhanced legislation and combined efforts by the law enforcement agencies, tech organizations and communities is very essential to mitigate and combat cybercrimes against women's and children's in India.

**3.2 Cross-Jurisdictional Issues**

Because of the nature of the cybercrime, they mostly cross-national borders. According to Information Technology Act, 2000 cyber jurisdiction is limited to Indian border, which makes difficulty for the cyber authorities to monitor criminals outside the territory. Worldwide Co-operation amongst law enforcement organizations remains in trouble because of unresolved cases [3].

There are also various challenges which are related to the jurisdiction of the internet, because of the interconnectivity throughout the world. Out-dated offences are to be normally committed locally because of this the offender can be easily detained, on the other hand in cybercrimes, the offender might be belonged to a different country (Advocate Tanwar, 2024) [6].

**3.3 Lack of Digital Literacy**

In spite of growing internet access, in India many women are not aware of exhaustive digital literacy a skill, which leads to create more vulnerability in context to online threats. Many children do not have the knowledge or any awareness to recognize online risks or protect themselves from the probable threats [5].

**3.4 Limited parental supervision:** With the growing internet access and control of device ownership among children, guardians not to monitor their online activities efficiently [5].

**3.5 Anonymity and ease of access:** The internet service provides a cover of secrecy for the offenders so that they can easily access towards the victims that creates a challenge for the agencies to mitigate and combat cybercrime [5].

**3.6 Social and Cultural Barriers:** Enabling male-controlled thinking and victim accusing approach are the main reason behind the non-reporting of cybercrimes by the women, also creates a fear of social shame or family status [5].

**3.7 Socio-economic factors:** Children's which are belongs to underprivileged backgrounds have only limited access towards digital learning resources and support systems, which leads to enhance their vulnerability [5].

**3.8 Inadequate Enforcement:** Lack of proper resources, expert training, and sometimes improper help from law enforcement agencies might delay towards effective response to cybercrimes against women [5].

**3.9 Inadequate Legal Structure:** Indian legal framework included the laws like "POCSO Act" and the Information Technology Act, but the problem in its proper execution and implementation. The fast-evolving cyber offences make it problematic to safeguard women and children properly [5].

## 4. Measures to Mitigate the Victimization of Women and Children [1]

- There are some important key steps that we can take to deals with evolving cybercrimes against women and children, that are as follows:
- If any cybercrime is being committed against the women, she should not be discouraged to file a complaint against the offender. Her guardians and family members should encourage her to file a complaint.
- It is the duty of the parents or guardians to make a safe environment at their home where they will discuss everyday problems. They have to encourage their children to discuss every kind of problem. If the parent finds that a cybercrime has been committed against the child, it's the first duty of parents to immediately take their child to police station to file a complaint.
- Parents should not have to openly upload the pictures of their children on social media portals. If they upload openly, there is a very high risk that their photos will be transformed to make pornographic videos.
- Women and children have more cautious while exploring social media portals. They should not to accept every unknown person's request and more vigilant while interacting with peoples on the internet.
- In any circumstances, women should not to share their personal pictures on the internet.
- Internet Service Provider is come under the purview to rigorous laws.
- Women and children should have to frequently change their passwords to secure their accounts from the hackers.

## 5. Policy solutions

To maintain a secure digital environment, an exhaustive multi-layered strategy is necessary:

### 5.1 Digital Literacy and Education

Strict enforcement through timely implementation of the Data Protection Board, along with clear instructions towards child data issue is very important. Furthermore, digital learning must be encouraged

through school curriculums along with digital awareness programs for parents and children's. The government and NGOs should also arrange camps and awareness programs regarding digital literacy.

### 5.2 Introduce Digital Literacy in Schools

Digital safety and learning must be included into school education system from starting. Exhaustive components on privacy, digital protocols, cyberbullying, and secure social media practice should be established. Providing comprehensive education to children's is considered as a long-term protection against digital abuse. Similarly, conducting workshops and parent-teacher meeting programs should increase awareness among guardians [2].

### 5.3 Capacity Building for Law Enforcement

The Government of India, under the Nirbhaya Fund implements a project namely, "Cyber Crime prevention against Women and Children (CCPWC)". According to this program, various steps are being taken for spreading awareness in context to cybercrimes, issuing alerts / advisories, provide training to law enforcement personnel / prosecutor attorneys / judicial officers, improvising cyber forensic facilities, etc. are to be accepted.

### 5.4 Strengthen Legal Frameworks

It is very essential to conduct repetitive renovations and amendments under the pre-existing legal statutes because of the fast-evolving digital environment. There is a requirement to include new statutes in relation to new threats such as cyber bullying, online mentoring and use of Article Intelligence in cybercrime [6].

### 5.5 Strengthen Enforcement Infrastructure

Actual execution requires severe implementation mechanisms. The government must inaugurate enthusiastic cybercrime units across all the states, which are especially trained to deal cases related to children's. These cyber units should be furnished with specialized forensic tools, technical drill, and psychosomatic support resources to deal with sensitive cases like, cyberbullying, cyber harassment, etc. Additionally, fast-track courts are to be established to deal with cybercrimes against minors and mandates speedy justice system [2].

### 5.6 Promote International Co-operation

Maintain resilient international agreements with various countries to modernize the procedure of information sharing and fast track trial of cybercriminal who committed cybercrimes across the nation (Nobi Mohanta, 2025) [7].

## 6. Conclusion

India has recognized legal frameworks for the protection of women and children in the cyberspace, substantial loop holes in the enforcement, absence of child-related provisions, and insufficient adaption to technological progressions impose exhaustive modifications to guarantees safe and secure online environments for women and children's.

Internet technology has to be considered as a two-edged weapon. Internet services are being used broadly across different areas of the society. Increasing involvement of internet services in cyberspace leads to the emergence of cybercrime. Various groups of individuals are aiming to take advantages from illegal means. In Indian society, women and children are considered as the most vulnerable groups of the society. Due to this, they can easily be targeted by the perpetrators. The intention of these cybercriminals is being strong day by day to commit crime is just because the aggrieved persons are not seriously filed complaint against these criminals [1].

Government and the common peoples have to recognize the harmful consequences out of these cybercrimes. Enactment of law is one thing and its proper enforcement is another thing. The government have to guarantee that the IT Act and the other cyber related laws is properly enforced in whole of the country. Law enforcement officers have to help the victims while registering complaints against the cybercrime. And also take necessary actions to track the offender and mitigate the crime. In the end, there is a special need to expand cyber laws and its proper enforcement [1].

**References**

1. Minakshi K., "Cyber Crime and the Victimization of Marginalized Sections of Society", Madhya Pradesh Journal of Social Sciences, December 2023, 28(2(ix)), 7-15.
2. Anshul K.M., "Children's Safety in the Digital Space: Legal Safeguards and Gaps in Indian Cyber Laws", By Record of law blog, August 21, 2025. https://recordoflaw.in/childrens-safety-in-the-digital-space-legal-safeguards-and-gaps-in-indian-cyber-laws/
3. Himani A., Dr. Somlata S., "Cyber Crimes Against Women in India", ShodhKosh: Journal of Visual and Performing Arts, June 2024, 5(6), 1539-1544. https://www.scribd.com/document/844283135/CYBER-CRIMES-AGAINST-WOMEN-IN-INDIA
4. The Protection of Children from Sexual Offences Act, 2012. https://www.indiacode.nic.in/bitstream/123456789/9318/1/sexualoffencea2012-32.pdf
5. Indecent Representation of Women (Prohibition) Act, 1986. https://www.indiacode.nic.in/bitstream/123456789/1768/1/198660.pdf
6. Anuradha G., Rachita T., "Digital Footprints and Little Steps: Privacy for Children", December 23, 2024. https://ssrana.in/articles/digital-footprints-and-little-steps-why-privacy-matters-for-children/
7. Dr. Sandeep K., Kumari Mamta T., "Cyber Violence Against Women and Children in India: Accessing Prevalence, Impact and Policy Solutions", Journal of Emerging Technologies and Innovative Research (JETIR), August 2025, 12(8), 626-636. https://www.jetir.org/papers/JETIR2508074.pdf
8. Advocate T., "Crime against women laws, Cyber Laws, Protection of Child from Sexual Offences", 18 July 2024. https://advocatetanwar.com/children-and-cyber-safety-legal-framework-and-protections-in-india/
9. "Protecting Children's Data in the Digital Age: India's Legal Framework and Policy Imperatives", Blog, 5 August 2025. https://www.dpo-india.com/Blogs/protecting-child-data/

10. “Measures To Ensure Safety and Security of Women and Children on Online Platforms”, Press Information Bureau Government of India
Ministry of Women and Child Development (PIB Delhi), 23 March 2022.
https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1808686
11. Nobi M., “How India’s Data Protection Laws Aim to Protect Minors from Social Media Risks”, 3 Feb 2025. https://medium.com/@nobi.mohanta/how-indias-data-protection-laws-aim-to-protect-minors-from-social-media-risks-35affce64d27