INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 2 | 2026 Art. 18

Cyber Crimes Against Women & Children: A Study of Legal Protection and Challenges

Shivani Mishra
Research Scholar,
Faculty of Law, Sanskriti University, Mathura

Vijay Kumar Pandey
Research Scholar,
Agra College, Agra

Recommended Citation
Shivani Mishra and Vijay Kumar Pandey, *Cyber Crimes Against Women & Children: A Study of Legal Protection and Challenges*, 5 IJHRLR 243-254 (2026).
Available at www.humanrightlawreview.in/current-issues/.

Cyber Crimes Against Women & Children: A Study of Legal Protection and Challenges

ABSTRACT

The swift advancement of digital technologies and widespread internet access has contributed to a marked increase in cyber-crimes across the globe, with women being particularly vulnerable targets. In the Indian context, offences such as online harassment, cyber stalking, identity theft, and the unauthorized dissemination of private images have become alarmingly common. This paper explores the various forms and characteristics of cyber-crimes against women, critically examines the existing legal framework, and identifies key challenges in its implementation. It also assesses the effectiveness of legislations like the Information Technology Act, 2000, along with relevant provisions of the Indian Penal Code (BNS). The study concludes by proposing measures to strengthen legal systems, enhance awareness, and improve technological safeguards to ensure greater protection for women in the digital space.

KEYWORDS

Cyber Crime, Women, IT Act, Cyber Law, Online Harassment, India

INTRODUCTION

Cybercrime encompasses a wide range of illegal activities conducted through computers, digital devices, or internet-based platforms. With the rapid expansion of digital infrastructure and increased reliance on online communication, cybercrimes have emerged as a serious global concern, particularly affecting women. The virtual environment provides offenders with a sense of anonymity and easy access to potential victims, which significantly increases the risk of exploitation. Moreover, technological vulnerabilities and inadequate cybersecurity measures further facilitate the commission of such offences. Women, in particular, are disproportionately targeted through forms of cybercrime such as online harassment, cyberstalking, identity theft, and the unauthorized dissemination of private content. These acts not only violate individual privacy and dignity but also create barriers to women's safe and equal participation in digital spaces. Therefore, understanding the nature and

dynamics of cyber crime is essential for developing effective legal, social, and technological responses.

In India, where social structures often reinforce gender-based inequalities, the digital sphere has emerged as an additional space where women face numerous threats. These include cyberstalking, online harassment, non-consensual sharing of private images, and gender-based trolling. The incidence of cyber-crimes against women in India has risen sharply, driven by factors such as the anonymity provided by the internet, the widespread use of smartphones, and inadequate enforcement of existing laws. Data from the National Crime Records Bureau (NCRB) indicates a significant increase in offences such as online harassment, stalking, and defamation against women in recent years[1].

As the criminal is behind the screen and isn't in public, he enjoys the benefit of anonymity. So, everyone needs to be aware of the impact of cyber-crimes against women and the ways in which it differs from other forms of crimes. Law enforcement agencies and the parents should be made aware of women and children responsibilities in their use of Information and Communications Technology, and what the sanctions are for misuse. Women and Children should know that who can provide them with support if a cybercrime takes place[2].

MEANING OF CYBER CRIME

In general cyber-crime may be defined as *"Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime"*

DEFINITION OF CYBER CRIME

According to legal and academic perspectives, cyber-crime may involve crimes where the computer is used as an instrument to commit an offence, as well as crimes where the computer or network itself is the target of the offence. The increasing reliance on digital technologies has expanded the scope and complexity of cyber-crimes, making them a significant threat to individuals, organizations, and national security.

In the Indian context, cyber-crimes are primarily governed by the Information Technology Act, 2000, along with relevant provisions of criminal law, which aim to address offences committed in

[1] National Crime Records Bureau. (2021). *Crime in India 2021 - Statistics*. Available at: https://ncrb.gov.in/en/crime-india

[2] https://www.cdtighaziabad.in/pdf/CYBER%20CRIMES%20AGAINST%20WOMEN%20&%20CHILDREN.pdf

cyberspace and ensure protection against digital threats.

According to D.S. Wall*- D.S. Wall defines cyber-crime as* ***"crimes that are mediated by networked computers,"*** *emphasizing that such offences are facilitated through digital technologies and online networks[3].*

Council of Europe (Budapest Convention)*- Under the Convention on Cybercrime, cyber-crime is broadly understood as offences against the confidentiality, integrity, and availability of computer systems, networks, and data[4].*

According to Pavan Duggal*-* Cyber-crime as *"any criminal activity that uses a computer either as an instrument, target, or means for perpetuating further crimes.[5]"*

TYPES OF CYBER CRIMES AGAINST WOMEN & CHILD

1. **Harassment through e-mails:** Harassment via email, includes black mailing, threatening and constant sending of love letters in anonymous names or regular sending of embarrassing mails.

2. **Cyber stalking:** 'Stalkers are strengthened by the anonymity the internet offers. He may be on the other side of the earth, or a next door neighbour or a near relative!' It involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. In general, the stalker intends to cause emotional distress and has no legitimate purpose to his communications.

3. **Cyber defamation:** Cyber defamation also called Cyber smearing can be understood as the intentional infringement of 'another person's right to his good name. 'Cyber Defamation occurs with the help of computers and / or the Internet. It is considered more of a menace owing to its expeditious nature.

4. **Child pornography:** Child sexually abusive material (CSAM) refers to material containing sexual image in any form, of a child who is abused or sexually exploited. Section 67 (B) of IT Act states that "it is punishable for publishing or transmitting

[3] D.S. Wall, Cybercrime: The Transformation of Crime in the Information Age (Polity Press 2007).
[4] Council of Europe, Convention on Cybercrime (Budapest Convention) (2001).
[5] Pavan Duggal, Cyber Law in India (Saakshar Law Publications 2017).

of material depicting children in sexually explicit act, etc. in electronic form.

5. Cyber pornography includes pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc.). The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc. from his website and when it is for revenge, video is broadcasting on messaging app or circulating on other online platforms.

6. **Cyber bullying:** A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc.

7. Cyber bullies may also disclose victims' personal data (e.g. real name, address, or workplace/schools) on websites. Cases of piggy-backing on victim's identity are now common. This could be used to publish objectionable material in their name that defames or ridicules a subject.

8. Under the Indian law, cyber-bullying is covered by section 66 D of the Information Technology Act. This section is titled "Punishment for sending offensive messages through communication service, etc." This section provides for imprisonment up to 3 years and fine up to one lakh.

9. **Cyber grooming:** Cyber Grooming is when a person builds an online relationship with a young person and tricks or pressures him/ her into doing sexual act.

10. **Identity Theft**: Children's personal information, such as names, photographs, or school details, may be stolen and misused for fraudulent purposes or impersonation.

LAW RELATED TO CYBER CRIMES IN INDIA

India has developed a comprehensive legal framework to address cyber-crimes, including offences against women & child, through a combination of statutory provisions and institutional mechanisms. The primary legislation governing cyber-crimes is the Information Technology Act, 2000, supplemented by provisions under the Indian Penal Code, 1860 (now largely replaced by the Bharatiya Nyaya Sanhita, 2023).

Information Technology Act, 2000

The Information Technology Act, 2000 is the cornerstone of cyber law in India. It provides legal recognition to electronic transactions and penalizes cyber offences. Key provisions relevant to crimes against women include:

- **Section 66E** – Punishes violation of privacy by capturing or transmitting images of private areas without consent.[6]
- **Section 67** – Deals with publishing or transmitting obscene content in electronic form.[7]
- **Section 67A** – Addresses sexually explicit material.[8]
- **Section 67B** – Pertains to child sexual abuse material (CSAM).[9]

Indian Penal Code, 1860 / Bharatiya Nyaya Sanhita, 2023

- **Section 354D IPC/BNS SEC 78** – Criminalizes stalking, including cyber stalking.[10]
- **Section 499 IPC/BNS SEC 356** – Deals with defamation, applicable to online defamation.[11]
- **Section 509 IPC/BNS SEC 79** – Punishes acts intended to insult the modesty of a woman.[12]

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

The Protection of Children from Sexual Offences Act, 2012 addresses sexual offences against minors, including those committed online. It criminalizes the use of children for pornographic purposes and provides stringent punishments.[13]

Data Protection and Privacy Laws

The recognition of privacy as a fundamental right article 21 in *Justice K.S. Puttaswamy v. Union of India (2017[14])* has strengthened legal safeguards against cyber-crimes involving personal data.

---

[6] Information Technology Act, 2000, sec 66E.
[7] Information Technology Act, 2000, sec 67.
[8] Information Technology Act, 2000, sec 67A.
[9] Information Technology Act, 2000, sec 67B.
[10] Indian Penal Code, 1860, sec 354D/BNS SEC 78.
[11] Indian Penal Code, 1860, sec 499/ BNS SEC 356
[12] Indian Penal Code, 1860, sec 509/BNS SEC 79
[13] Protection of Children from Sexual Offences Act, 2012
[14] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

LATEST AMENDMENTS AND DEVELOPMENTS IN CYBER LAW (2023–2025)

Information Technology (Amendment) Rules, 2023[15]

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 introduced major changes:

- Regulation of online gaming platforms through verification and self-regulatory bodies
- Establishment of mechanisms to identify and address fake or misleading information
- Increased accountability of intermediaries (social media platforms)
- Strengthening due diligence obligations for digital platforms

Jan Vishwas (Amendment of Provisions) Act, 2023[16]

This amendment brought changes to the Information Technology Act, 2000 by:

- Decriminalizing certain minor offences
- Promoting ease of doing business
- Introducing a more compliance-based approach rather than punitive measures

Digital Personal Data Protection Act, 2023[17]

A major development in India's cyber legal framework is the Digital Personal Data Protection Act, 2023 (DPDP Act):

- Recognizes the importance of data privacy and consent
- Imposes obligations on companies to protect personal data
- Provides rights to individuals, including women, against misuse of their data
- Mandates reporting of data breaches

This law significantly strengthens protection against cyber-crimes like identity theft and misuse of personal information.

[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023
[16] Jan Vishwas (Amendment of Provisions) Act, 2023
[17] Digital Personal Data Protection Act, 2023

IT (Intermediary Guidelines) Amendment Rules, 2025[18]

The 2025 amendments further strengthened intermediary accountability:

- Introduced strict procedures for content removal
- Required clear and reasoned takedown orders
- Limited authority to senior officials for issuing such directions
- Ensured transparency and proportionality in content regulation

These changes aim to balance freedom of expression with cyber safety

Telecommunications (Telecom Cyber Security) Rules, 2024 & Amendment Rules, 2025[19]

New telecom-related cyber security rules were introduced to:

- Prevent misuse of telecom networks for cyber fraud
- Strengthen verification systems (KYC)
- Enhance monitoring of digital communication infrastructure

These rules expand the government's ability to tackle fraud, phishing, and digital impersonation.

Government Advisories (2023–2025)[20]

The Government of India has issued multiple advisories directing intermediaries to:

- Prevent hosting of deepfakes, impersonation, and non-consensual intimate images (NCII)
- Ensure faster removal of unlawful content
- Strengthen compliance with existing provisions of the IT Act

These advisories directly address cyber-crimes against women, such as online harassment and image-based abuse.

[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025
[19] Telecommunications (Telecom Cyber Security) Rules, 2024 and Amendment Rules, 2025
[20] https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2226335&utm

IMPACT OF CYBER CRIMES ON WOMEN

1.Psychological Impact

Victims of cyber-crimes frequently experience mental health issues such as anxiety, depression, fear, and emotional distress. Continuous harassment, cyber stalking, and threats can lead to trauma and a sense of insecurity. In extreme cases, victims may suffer from long-term psychological disorders or suicidal tendencies.[1]

2.Social Impact

Cyber-crimes often result in social stigma and victim-blaming, particularly in societies with strong cultural norms regarding women's behavior. The non-consensual sharing of private images or defamatory content can damage a woman's reputation, leading to isolation and loss of social support.[2]

3. Economic Impact:

Women affected by cyber-crimes may face financial losses due to online fraud, identity theft, or extortion. Additionally, reputational harm and psychological distress can affect their professional lives, leading to job loss, reduced productivity, or withdrawal from economic activities.[3]

4. Violation of Privacy and Dignity

Cyber-crimes such as hacking, data breaches, and the unauthorized sharing of personal content directly violate a woman's right to privacy and dignity. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) underscores the seriousness of such violations.[4]

5. Restriction on Freedom of Expression

Fear of online abuse and harassment often discourages women from expressing their opinions on digital platforms. This results in reduced participation in social, political, and professional discourse, thereby limiting their digital presence and voice.[5]

IMPORTANT CASE LAWS ON CYBER CRIMES AGAINST WOMEN

State of Tamil Nadu v. Suhas Katti (2004)

This is one of India's first cybercrime convictions. The accused

posted obscene and defamatory messages about a woman in a Yahoo message group.

- The court convicted the accused under Sections 469 and 509 of IPC and Section 67 of the IT Act.
- The case is significant for demonstrating speedy justice in cybercrime cases (judgment within 7 months).
- It established that online harassment is punishable under existing laws.

Kalandi Charan Lenka v. State of Odisha (2017)

In this case, the accused created a fake Facebook account and posted obscene content about a woman.

- The Orissa High Court held that such acts amount to cyberstalking and online harassment.
- It emphasized that morphing images and sending obscene messages violate a woman's dignity and privacy.
- The case expanded the scope of Section 354D IPC (stalking) to include online activities.

Shreya Singhal v. Union of India (2015)

A landmark judgment related to online speech and misuse of cyber laws.

- The Supreme Court of India struck down Section 66A of the IT Act as unconstitutional.
- The Court held that vague laws can be misused and violate freedom of speech.
- However, it clarified that genuine cyber harassment and threats remain punishable under other provisions.

Aveek Sarkar v. State of West Bengal (2014)

This case dealt with the issue of obscenity in digital and print media.

- The Supreme Court of India adopted the "community standards test" for determining obscenity.
- It held that not all nude or semi-nude images are obscene unless they arouse sexual interest.
- This case is relevant in cybercrime cases involving online publication of images of women.

Ritu Kohli Case (2001)

One of the earliest reported cases of cyber stalking in India.

- The accused used the victim's identity in chat rooms and shared her phone number, leading to harassment.
- The case led to the recognition of cyber stalking as a serious offense, influencing later legal reforms like Section 354D IPC (BNS SEC 78).

Aveek Sarkar v. State of West Bengal (2014)

This case dealt with the issue of obscenity in digital and print media.

- The Supreme Court of India adopted the "community standards test" for determining obscenity.
- It held that not all nude or semi-nude images are obscene unless they arouse sexual interest.
- This case is relevant in cybercrime cases involving online publication of images of women.

Ritu Kohli Case (2001)

One of the earliest reported cases of cyber stalking in India.

- The accused used the victim's identity in chat rooms and shared her phone number, leading to harassment.
- The case led to the recognition of cyber stalking as a serious offense, influencing later legal reforms like Section 354D IPC (BNS SEC 78).

CONCLUSION

Cyber-crimes against women and children have emerged as a serious and rapidly growing challenge in the digital age. While technological advancements have enhanced connectivity and opportunities, they have also created new avenues for exploitation, abuse, and victimization. Women and children, being among the most vulnerable groups, are disproportionately affected by offences such as cyber stalking, online harassment, cyber grooming, identity theft, and the non-consensual dissemination of private content. India has established a comprehensive legal framework through laws such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Protection of Children from Sexual Offences Act, 2012, along with recent developments like the Digital Personal Data Protection Act, 2023. Judicial pronouncements, including

Justice *K.S. Puttaswamy v. Union of India (2017)*, have further strengthened the protection of privacy and dignity in the digital sphere. Despite these advancements, significant challenges persist in terms of implementation, awareness, underreporting, and the evolving nature of technology. The study highlights that legal provisions alone are insufficient without effective enforcement, digital literacy, and institutional support. Societal attitudes, victim-blaming, and lack of awareness continue to hinder access to justice for victims. Additionally, jurisdictional complexities and the transnational nature of cyber-crimes pose further obstacles to effective regulation and prosecution. Therefore, a holistic and multi-dimensional approach is essential. This includes strengthening legal mechanisms, enhancing cyber policing capabilities, promoting awareness and digital education, and fostering cooperation between governments, technology companies, and civil society. Special emphasis must be placed on creating a safe and inclusive digital environment where women and children can participate without fear.

Ensuring protection against cyber-crimes is not only a matter of legal necessity but also a fundamental requirement for achieving gender justice, child safety, and inclusive digital development. A proactive, coordinated, and rights-based approach is crucial to effectively combat cyber-crimes and safeguard the dignity and security of women and children in cyberspace.