

Protection of Women and Children in Digital Age

¹Prof.(Dr.)Param Jeet Singh, ²Mr.Arun Kumar

¹Professor, ²LL.M student

¹²University School of Law,SGGSWU, Fatehgarh Sahib, Punjab

Abstract—The rapid expansion of digital technologies has transformed human life by enabling seamless communication, e-governance, online education, and digital commerce. However, this transformation has also exposed women and children to unprecedented risks in cyberspace. Crimes such as cyberstalking, online harassment, identity theft, grooming, child sexual exploitation material (CSEM), revenge pornography, deepfake manipulation, and cyberbullying have become increasingly common. These offences are often anonymous, transnational, and difficult to trace, making enforcement of law highly complex.

This research paper examines the nature and scope of digital threats faced by women and children, evaluates the existing legal frameworks in India and internationally, analyses landmark judicial decisions, and identifies gaps in enforcement mechanisms. It also explores the role of technology platforms, artificial intelligence, and digital governance in addressing these challenges. Finally, it offers policy recommendations aimed at strengthening cyber safety and ensuring a secure digital ecosystem.

I. Introduction

The digital revolution has fundamentally altered the way human beings interact, learn, and conduct business. With over half of the global population connected to the internet, cyberspace has become an essential part of daily life. In India alone, internet penetration has increased significantly over the past decade, especially through smartphones and affordable data services.

While this digital transformation has created opportunities for empowerment, it has simultaneously created new vulnerabilities. Women and children are among the most affected groups due to their relative lack of digital literacy, social vulnerability, and increased exposure to online interactions.

Women are often targeted through gender-based cyber violence such as trolling, harassment, stalking, and non-consensual sharing of intimate images. Children face threats such as grooming, exploitation, exposure to harmful content, and cyberbullying. These crimes not only affect mental health but also lead to long-term psychological trauma and social consequences.

The anonymity of the internet, combined with weak enforcement mechanisms and cross-border jurisdictional issues, makes cybercrime particularly difficult to regulate.

II. OBJECTIVES OF THE STUDY

This research aims to:

- Identify major cyber threats faced by women and children
- Study national legal frameworks dealing with cybercrime
- Examine international conventions and agreements
- Analyse landmark judicial decisions
- Evaluate the role of digital platforms and intermediaries
- Suggest effective legal and policy reforms

III. RESEARCH METHODOLOGY

This study is doctrinal and analytical in nature. It relies on secondary sources such as:

- Statutes and legislation
- Judicial decisions of the Supreme Court and High Courts
- Reports from UNICEF, NCRB, and IT Ministry
- International conventions
- Research papers, journals, and books on cyber law

IV. DIGITAL THREATS FACED BY WOMEN AND CHILDREN

4.1 Cyber Threats Faced by Women

Women face a wide spectrum of gender-based online violence, including:

(a) Cyberstalking

Repeated monitoring, messaging, or tracking of a woman online, often leading to fear and psychological distress.

(b) Online Harassment and Trolling

Abusive comments, hate speech, and coordinated harassment campaigns targeting women, especially public figures.

(c) Revenge Pornography

Non-consensual sharing of intimate images or videos, often used for blackmail or humiliation.

(d) Deepfake Abuse

AI-generated manipulated images or videos that falsely depict women in explicit content.

(e) Doxxing

Publishing private personal information such as address, phone number, or workplace.

(f) Sextortion

Blackmail using sexual content or threats of sharing private material.

These crimes are often underreported due to social stigma and fear of reputational damage.

4.2 Cyber Threats Faced by Children

Children are particularly vulnerable due to lack of maturity and awareness.

(a) Cyberbullying

Harassment through social media, messaging apps, or online gaming platforms.

(b) Online Grooming

Predators building trust with minors to exploit them sexually.

(c) Exposure to Inappropriate Content

Unfiltered access to pornography, violence, or harmful ideologies.

(d) Gaming Exploitation

Manipulation through online gaming chats and platforms.

(e) Identity Theft

Misuse of children's data for fraudulent purposes.

According to global child safety reports, a significant percentage of minors experience online harm before adulthood.¹

¹ UNICEF, *Child Online Protection Report*, 2023

4.3 Emerging Cyber Threats

Technological advancement has created new risks:

- Artificial intelligence-generated deepfakes
- Algorithmic manipulation of user behavior
- Metaverse harassment
- Data harvesting and surveillance capitalism
- Encrypted communication misuse

V. LEGAL FRAMEWORK IN INDIA

5.1 Information Technology Act, 2000

The IT Act is the primary legislation governing cybercrime in India.

Key provisions include:

- [1] **Section 66C** – Identity theft
- [2] **Section 66D** – Cheating by impersonation
- [3] **Section 66E** – Violation of privacy
- [4] **Section 67** – Publishing obscene material
- [5] **Section 67A** – Sexually explicit content
- [6] **Section 67B** – Child sexual abuse material

However, the Act was enacted before the rise of social media and AI technologies, making it partially outdated.

5.2 Bharatiya Nyaya Sanhita (BNS), 2023

The new criminal law framework includes provisions for:

- TABLE I. Stalking (including digital stalking)
- TABLE II. Sexual harassment
- TABLE III. Criminal intimidation
- TABLE IV. Voyeurism

It modernizes several provisions of the Indian Penal Code to include digital offences.

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

The POCSO Act is a strong child protection law in India.

Key features include:

- Fig. 1. Protection against online and offline sexual abuse
- Fig. 2. Mandatory reporting of offences
- Fig. 3. Child-friendly investigation procedures
- Fig. 4. Protection of victim identity

Despite this, enforcement remains challenging in cyberspace due to jurisdictional issues.²

5.4 Digital Personal Data Protection Act, 2023

This Act introduces a modern framework for data protection:

- [1] Consent-based data processing
- [2] Special protection for children's data
- [3] Duties of data fiduciaries
- [4] Penalties for misuse of personal data

It strengthens privacy rights in the digital ecosystem.³

VI. INTERNATIONAL LEGAL FRAMEWORK

6.1 United Nations Convention on the Rights of the Child (CRC)

The CRC ensures:

- Protection from exploitation and abuse
- Right to privacy
- Protection from harmful content

6.2 Budapest Convention on Cybercrime

² Protection of Children from Sexual Offences Act, 2012

³ Digital Personal Data Protection Act, 2023

This is the first international treaty on cybercrime, focusing on:

- Harmonization of cyber laws
- International cooperation
- Evidence sharing between countries

However, not all countries have ratified it, limiting its effectiveness.⁴

6.3 General Data Protection Regulation (GDPR)

The GDPR (EU) provides:

- Strong consent requirements
- Right to be forgotten
- Special protection for minors
- Heavy penalties for violations

VII. ROLE OF TECHNOLOGY AND SOCIAL MEDIA PLATFORMS

Technology companies play a dual role — enabling communication while also enabling abuse.

7.1 Content Moderation Systems

Platforms use:

- Artificial intelligence for detecting harmful content
- Human moderation teams
- User reporting mechanisms

However, moderation is inconsistent and often delayed.

7.2 Encryption Debate

End-to-end encryption protects privacy but can also hinder investigation of child exploitation cases.

7.3 Algorithmic Risks

⁴ Council of Europe, *Budapest Convention on Cybercrime*, 2001

Algorithms may:

- Promote harmful or sensational content
- Increase exposure to unsafe material
- Reinforce addictive behavior patterns

VIII. JUDICIAL INTERPRETATION AND CASE LAWS

8.1 Justice K.S. Puttaswamy v. Union of India (2017)

- Recognized Right to Privacy as a fundamental right
- Established strong foundation for digital privacy rights

8.2 Shreya Singhal v. Union of India (2015)

- Struck down Section 66A of IT Act
- Protected freedom of speech online
- Clarified limits of intermediary liability

8.3 Judicial Trends

Courts have increasingly:

- Recognized cyber harassment as violation of dignity
- Ordered removal of obscene online content
- Emphasized accountability of digital platforms

IX. MAJOR CHALLENGES

- Cross-border nature of cybercrime
- Anonymity of offenders
- Lack of cyber awareness among users
- Inadequate cyber forensic infrastructure
- Slow legal processes
- Underreporting due to stigma

X. FINDINGS

- Legal framework exists but enforcement is weak
- Women face targeted gender-based cyber violence

- Children are highly vulnerable to online exploitation
- Technology platforms lack full accountability
- Awareness is still limited in rural and semi-urban areas

XI. SUGGESTIONS AND POLICY RECOMMENDATIONS

- Strengthen cyber laws for AI and deepfake crimes
- Mandatory cyber safety education in schools
- Fast-track cybercrime courts
- Stronger regulation of social media platforms
- Improved cyber forensic infrastructure
- International cooperation for cross-border crimes

XII. CONCLUSION

The digital age has created a complex environment where opportunities and risks coexist. Women and children, being the most vulnerable groups, face disproportionate harm in cyberspace. Although India and other countries have introduced several legal protections, enforcement remains a major challenge.

A holistic approach involving legal reform, technological innovation, institutional strengthening, and public awareness is essential to ensure a safe and inclusive digital environment. Protection of women and children in cyberspace is not only a legal necessity but also a moral and social responsibility.

XIII. BIBLIOGRAPHY

Primary Sources

- Information Technology Act, 2000
- POCSO Act, 2012
- Bharatiya Nyaya Sanhita, 2023
- Digital Personal Data Protection Act, 2023

Secondary Sources

- NCRB Cybercrime Reports
- UNICEF Publications
- Cyber Law Journals and Articles

International Sources

- UNCRC
- Budapest Convention
- GDPR (EU)