

Original Article

Cyber Safety and Digital Rights of Women: Legal Challenges, Human Rights, and the Emerging Framework of Cyber Protection

Dr. Vinay Kumar Katiyar

Associate Professor, Faculty of Law,
Major S. D. Singh University Fatehgarh Farrukhabad

Manuscript ID:

yrj-150109

ISSN: 2277-7911

Impact Factor – 7.025

Volume 15

Issue 1

Jan-Feb-Mar.- 2026

Pp. 60 – 66

Submitted: 15 Jan. 2026

Revised: 27 Jan. 2026

Accepted: 10 Feb. 2026

Published: 10 Mar. 2026

Corresponding Author:
Dr. Vinay Kumar Katiyar

Quick Response Code:



Web. <https://yra.ijaar.co.in/>



DOI:
10.5281/zenodo.21902668

DOI Link:
<https://doi.org/10.5281/zenodo.21902668>

Abstract:

The digital revolution has significantly reshaped the lives of women by expanding opportunities for education, employment, entrepreneurship, political participation, and social interaction. At the same time, the widespread use of internet-based technologies has generated new forms of cyber risks that disproportionately affect women. Incidents such as cyberstalking, online harassment, cyberbullying, identity fraud, non-consensual circulation of intimate images, financial scams, and AI-enabled deepfake content have become serious threats to women's safety, autonomy, and digital participation. These challenges undermine fundamental values such as privacy, dignity, equality, security, and freedom of expression within digital spaces.

This study examines cyber safety and the digital rights of women through the combined perspectives of law, human rights, and cybersecurity. It conceptualizes digital rights as an extension of universally recognized human rights, encompassing the rights to privacy, equal access to digital technologies, protection from online discrimination, freedom of expression, and secure participation in cyberspace. The paper critically evaluates India's legal framework, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, constitutional safeguards, and applicable international human rights instruments designed to address cyber offences affecting women.

The research further explores the responsibilities of government agencies, law enforcement authorities, technology companies, educational institutions, and civil society organizations in developing a secure, inclusive, and gender-responsive digital environment. It argues that statutory protection alone cannot effectively address the evolving nature of cyber threats unless accompanied by widespread digital literacy, gender-sensitive cybersecurity strategies, advanced technological safeguards, prompt legal remedies, and sustained public awareness campaigns. The paper concludes that protecting women's digital rights and strengthening cyber resilience are indispensable for achieving gender justice, preserving human dignity, and fostering inclusive digital governance in an increasingly technology-driven society. A comprehensive

and collaborative approach involving legal reform, institutional accountability, technological innovation, and public participation is essential to ensure that women can safely and confidently exercise their rights in the digital age.

Keywords: *Cyber Safety, Digital Rights, Women, Cybercrime, Online Security, Privacy, Cyber Law, Human Rights, Artificial Intelligence, Gender Equality.*



Creative Commons



Creative Commons (CC BY-NC-SA 4.0)

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0), which permits others to remix, adapt, and build upon the work non-commercially, provided that appropriate credit is given and that any new creations are licensed under identical terms.

How to cite this article:

Dr. Vinay Kumar Katiyar (2026). Cyber Safety and Digital Rights of Women: Legal Challenges, Human Rights, and the Emerging Framework of Cyber Protection. Young Researcher, 15(1), 60 – 66. <https://doi.org/10.5281/zenodo.21902668>

Introduction:

The twenty-first century has witnessed an unprecedented digital transformation that has reshaped communication, commerce, education, governance, and social interactions. The increasing penetration of smartphones, social media platforms, cloud computing, artificial intelligence, and digital payment systems has made the internet an indispensable part of everyday life. Women across the world have significantly benefited from digital technologies by accessing educational opportunities, financial services, healthcare information, employment platforms, and entrepreneurial ventures.

Despite these advancements, cyberspace has also become a site of gender-based discrimination and violence. Women are disproportionately targeted through cyberstalking, online abuse, sexual harassment, identity theft, revenge pornography, deepfake technologies, and

cyber extortion. Such cybercrimes often cause psychological trauma, reputational harm, financial losses, and social exclusion.

Digital rights encompass the rights and freedoms necessary for individuals to participate safely and equally in digital environments. For women, these rights include privacy, freedom of expression, access to information, protection from online violence, digital inclusion, and data protection. Ensuring cyber safety and protecting digital rights are therefore critical components of gender equality and human rights.

Understanding Cyber Safety:

Cyber safety refers to the safe, secure, and responsible use of digital technologies and internet-based platforms. It involves protecting users from cyber threats while ensuring secure communication, privacy, and digital well-being.

Cyber safety includes:

- Protection against cybercrime.
- Safe use of social media.
- Protection of personal information.
- Prevention of online harassment.
- Secure digital transactions.
- Responsible digital citizenship.

For women, cyber safety extends beyond technical security to include protection from gender-based online violence and discrimination.

Digital Rights of Women:

Digital rights are extensions of fundamental human rights in the digital environment. They ensure that women enjoy equal opportunities and protections online.

Major digital rights include:

a) Right to Privacy:

Women have the right to control their personal information, photographs, financial data, and communication. Unauthorized sharing of personal information violates privacy rights.

b) Freedom of Expression:

Women should be able to express opinions online without fear of harassment, intimidation, or violence.

c) Right to Access Information:

Equal access to internet services, educational resources, and digital platforms is essential for women's empowerment.

d) Right to Digital Security:

Women deserve protection from hacking, cyberstalking, identity theft, phishing, and online exploitation.

e) Right to Equality:

Digital platforms should remain free from gender discrimination and algorithmic bias.

Major Cyber Threats Faced by Women:

Women face multiple forms of cyber-enabled violence.

1. Cyberstalking:

Cyberstalking involves repeated monitoring, threatening, or harassing women through emails, messaging applications, GPS tracking, or social media.

2. Online Sexual Harassment:

Women frequently experience:

- Unwanted messages
- Sexual comments
- Explicit images
- Threats of sexual violence
- Offensive trolling

Such conduct discourages women's participation in digital spaces.

3. Identity Theft:

Cybercriminals steal personal information to create fake social media profiles, conduct financial fraud, or damage reputations.

4. Non-Consensual Sharing of Intimate Images:

Commonly referred to as "revenge pornography," this involves sharing private photographs or videos without consent.

5. Deepfake Technology:

Artificial Intelligence can generate realistic fake images and videos that may be used to blackmail, humiliate, or politically target women.

6. Cyberbullying:

Women, particularly students and young professionals, often face abusive comments, rumors, body shaming, and coordinated online attacks.

7. Financial Cyber Fraud:

Women increasingly using digital banking and e-commerce are targeted through phishing, fake job offers, OTP fraud, and fraudulent investment schemes.

Causes of Increasing Cyber Crimes Against Women:

Several factors contribute to increasing cyber offences:

- Rapid digitalization
- Lack of cybersecurity awareness
- Weak password practices
- Low digital literacy
- Anonymous online identities
- Misuse of Artificial Intelligence
- Inadequate reporting
- Social stigma
- Cross-border nature of cybercrime

Legal Framework in India:

India has established multiple legal provisions to address cybercrime against women.

Information Technology Act, 2000:

Important provisions include:

- **Section 66C** – Identity theft.
- **Section 66D** – Cheating through computer resources.
- **Section 66E** – Violation of privacy.
- **Section 67** – Publishing obscene electronic material.

- **Section 67A** – Sexually explicit content.
- **Section 67B** – Child sexual abuse material.

Bharatiya Nyaya Sanhita (BNS), 2023:

The BNS contains provisions relating to:

- Sexual harassment
- Criminal intimidation
- Voyeurism
- Stalking
- Defamation
- Publication of obscene material

These provisions also apply when offences occur through digital platforms.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:

These Rules require intermediaries to:

- Remove unlawful content.
- Establish grievance mechanisms.
- Cooperate with law enforcement agencies.
- Protect user privacy.

International Legal Framework:

Women's digital rights are supported by several international human rights instruments.

Universal Declaration of Human Rights (1948):

Recognizes:

- Equality
- Privacy
- Freedom of expression
- Human dignity

Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW):

CEDAW obligates States to eliminate discrimination affecting women's participation in public life, including digital spaces.

International Covenant on Civil and Political Rights (ICCPR):

Protects:

- Privacy
- Freedom of speech
- Equality before law

Sustainable Development Goals (SDGs):

SDG 5 promotes gender equality, while SDG 9 encourages inclusive digital innovation.

Government Initiatives in India:

The Government of India has introduced several initiatives:

Cyber Crime Reporting Portal:

Women can report cyber offences online through the National Cyber Crime Reporting Portal.

Indian Cyber Crime Coordination Centre (I4C):

Coordinates investigation, research, capacity building, and awareness regarding cybercrime.

Cyber Dost Initiative:

Promotes cybersecurity awareness through digital campaigns and educational materials.

Digital India Programme:

Encourages digital inclusion while emphasizing safe internet usage.

Role of Technology Companies:

Technology companies play an important role in ensuring cyber safety.

Their responsibilities include:

- Content moderation.
- AI-based detection of abusive content.
- User verification mechanisms.
- Strong privacy settings.
- End-to-end encryption.
- Reporting and blocking mechanisms.
- Removal of harmful content.

Companies should adopt gender-sensitive policies while designing digital platforms.

Importance of Digital Literacy:

Digital literacy empowers women to safely navigate online environments.

Important aspects include:

- Recognizing phishing attacks.
- Creating strong passwords.
- Using two-factor authentication.
- Protecting personal information.
- Reporting cyber offences.
- Safe online communication.
- Identifying fake news.
- Responsible social media usage.

Educational institutions should integrate cyber safety education into school and university curricula.

Challenges in Protecting Women's Digital Rights:

Despite legal safeguards, several challenges remain:

- Underreporting due to social stigma.
- Slow investigation.

- Lack of digital evidence.
- Cross-border jurisdictional issues.
- Limited cybersecurity awareness.
- Inadequate police training.
- Technological sophistication of cybercriminals.
- Misuse of Artificial Intelligence.
- Weak data protection culture.

Recommendations:

A comprehensive strategy should include:

1. Strengthening cybercrime laws.
2. Fast-track investigation of cyber offences against women.
3. Mandatory cybersecurity education.
4. Gender-sensitive police training.
5. Stronger cooperation between governments and technology companies.
6. AI-based detection of online abuse.
7. Effective victim support services.
8. Public awareness campaigns.
9. Strong implementation of data protection laws.
10. International cooperation against transnational cybercrime.

Conclusion:

Digital technologies have become indispensable tools for women's empowerment, economic participation, education, and democratic engagement. However, the rise of cyber-enabled violence threatens these gains by creating unsafe online environments that discourage women from exercising their rights and participating

fully in digital society. Cyber safety and digital rights are therefore not merely technological concerns but essential components of human rights, gender equality, and social justice.

India has established a significant legal framework through the Information Technology Act, the Bharatiya Nyaya Sanhita, intermediary regulations, and institutional mechanisms such as the Indian Cyber Crime Coordination Centre. Nevertheless, effective implementation remains a challenge due to underreporting, limited digital literacy, evolving technologies such as artificial intelligence and deepfakes, and the transnational nature of cybercrime. Addressing these challenges requires coordinated efforts among governments, law enforcement agencies, educational institutions, technology companies, civil society organizations, and international bodies.

A rights-based approach that combines robust legal protections, digital literacy, technological innovation, gender-sensitive policing, and accessible reporting mechanisms is essential for creating a secure digital ecosystem. Women must be empowered not only to access digital technologies but also to use them freely, safely, and without fear of harassment or discrimination. Ensuring cyber safety and protecting digital rights will strengthen women's participation in the digital economy, promote inclusive governance, and contribute to the achievement of gender equality and sustainable development.

Ultimately, a safe and equitable cyberspace is indispensable for realizing the broader objectives of justice, human dignity, and democratic participation in the digital age.

References:

1. Information Technology Act, 2000 (India).
2. Bharatiya Nyaya Sanhita, 2023.
3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
4. Universal Declaration of Human Rights, 1948.
5. Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), 1979.
6. International Covenant on Civil and Political Rights (ICCPR), 1966.
7. United Nations Sustainable Development Goals (SDGs), 2015.
8. National Crime Records Bureau (NCRB), *Crime in India* (latest available edition).
9. Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C).
10. UNESCO. *Guidelines on Digital Safety and Gender Equality*.