International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
An International Quarterly bi-lingual Multidisciplinary Double Blind Open Access Peer Reviewed Refereed Journal
ISSN:2581-9925, Impact Factor (Cosmos: 7.555 & I2OR: 5.105), Volume 08, No. 03(IV)(Special Issue), July-September, 2026, pp. 244-248

Legal Protection against Cybercrime for Women Entrepreneurs in India: Critical Analysis

Dr. Poonam Khanna[1*] | Dr. Neetu Khanna[2]

[1]Professor, Law Department, IME Law College, Sahibabad.
[2]Assistant Professor, Modern Law College, Ghaziabad.

[*]Corresponding Author: poonamlld@gmail.com

DOI Citation: Khanna, P. & Khanna, N. (2026). Legal Protection against Cybercrime for Women Entrepreneurs in India: Critical Analysis. International Journal of Education, Modern Management, Applied Science &Amp; Social Science, 08(03(IV)), 244–248.

ABSTRACT

The growth of the use of digital technologies and online platforms has greatly benefited businesspeople in India. Women businesspeople or entrepreneurs have particularly benefited, allowing them to build their business through online platforms. However, with the rising use of online platforms, women businesspeople have also had to face harassment in the form of cyber harassment, which includes cyber stalking, identity theft, defamation online, financial fraud, impersonation, and abuse of women in relation to their gender. Some of the issues discussed in this paper include the current legal responses that the Indian government has provided to women entrepreneurs to protect them from cyber harassment. The two primary documents that are discussed in this paper are the Bharatiya Nyaya Sanhita, the Information Technology Act of India 2000, and the Digital Personal Data Protection Act 2023. Besides, the research also evaluates how cyber crimes against women in business may be tackled, including discussing enforcement. When it comes to enforcing the laws on cyber crime, several key hurdles have been encountered, which include inadequate knowledge of the laws, underreporting of cybercrime, challenges in the technical and procedural aspects of investigating cybercrimes, and delays in police action. The authors emphasize the necessity of modifying the laws regarding cybercrime to be better in tune with the concerns of female entrepreneurs and facilitating enforcement of existing laws to the fullest. The paper goes on to highlight the reality that awareness about the legal protection against cybercrime in India is increasing with the emergence of new laws, online safety initiatives,, and stricter enforcement measures in place to protect female entrepreneurs.

***Keywords**: Cybercrime, Women Entrepreneurs, Digital Safety, Cyberstalking, Financial Fraud, Legal Protection, Information Technology Act, 2000, Cyber Laws in India, Digital Privacy, Online Defamation.*

Introduction

The advent of the digital economy in India has brought about significant transformation in business practices and opened various possibilities for female entrepreneurs to develop their businesses[1]. With the development of technology and the growing use of the internet, the global communication network, including e-commerce platforms and online payment facilities, is benefiting women entrepreneurs in running their businesses autonomously and gaining access to the big market. This shift in transformation has been additionally catalysed by governmental initiatives like Digital India

[*] *Copyright © 2026 by Author's and Licensed by Inspira. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work properly cited.*

[*] ***A Special Issue for the papers accepted for publication in the Two-Days Multidisciplinary National Seminar on Role of Entrepreneurship in Socio-Economic Upliftment of Women in India(22-23May 2026) Organized by Faculty of Commerce, The Graduate School College for Women, Jamshedpur, Jharkhand(A Constituent Unit of Kolhan University, Chaibasa, Jharkhand)in Collaboration with Jharkhand State Higher Education Council, Department of Higher and Technical Education, Govt. of Jharkhand & Punjab and Sind Bank, Sakchi, Jamshedpur.***

[1] https://www.researchgate.net/publication/373107532_DIGITAL_TRANSFORMATION_IN_BUSINESSES_OWNED_BY_WOMEN

which stimulated digital literacy, varied financial inclusion measures and technological adoption of women that push towards active technology-enabled firms.[1]

In addition, mobile technologies and inexpensive internet availability allow women from rural and semi-urban locations to enter the job market. E-commerce sites, social networks, and online banking services provide solutions to previous problems such as high expenses of becoming a businesswoman, movement restrictions, and inability to access shops; thus, women started to take an increasing part in the business context and, therefore, became major contributors to economic progress and job creation. On the other hand, being an online entrepreneur presents various risks too[2]. The same platforms that allow businesswomen to improve their operations create possibilities of taking advantage of women. The increasing number of cybercrimes against women will be examined below in terms of increasing instances of cyberbullying, identity theft, fraud, as well as other forms of cybercriminal activities. Such crimes can potentially lead to various unpleasant consequences because of which a woman might lose her reputation, safety, and financial well-being.[3]

The other problem is that online violence often targets women, which makes it even harder to combat this problem. There are many cases of people sending messages to women that are abusive in some form or the other. Many times, cases of stalking and harassment happen while women perform online activities.[4] Despite the legal measures designed to provide women with some protection against online harassment, the effectiveness of these measures is limited due to lack of awareness, low reporting rates, and enforcement problems Cso due to the absence of a legal framework that would help women continue their development in the digital world, a lot of women will not become active participants of the digital economy.[5]

Cyber Crime: An Overview of the Types of Cybercrime

Cybercrime is an illegal activity that takes place via computers, digital networks, or some other form of digital equipment. Women business owners are often targets of cybercrime, including:

- **Cyberstalking** - repeated stalking or following someone over the internet or via electronic means**.**
  - **Identity Theft** - The use of someone else's personal or business identity without their permission**.**
  - **Phishing & Financial Fraud -** Fraudulent transactions or scams that result in financial loss.
  - **Online Defamation -** Negative reviews or information that damages a person's or business's reputation.
  - **Cyberbullying/Harassment—Abusive** messages, threats, or trolling.

These crimes not only negatively impact the victims but also their mental and emotional health.[6]

Laws Relating to Cyberspace in India

The IT Act, 2000, serves as the core foundation for cyberspace's legal framework in India. The Act specifies several key elements related to the treatment of cybercrime that specifically impact women entrepreneurs:

Important Elements:

- **Section 65**-Tampering with Computer Source Documents can lead to fines and/or imprisonment for a maximum of three years. The documents above are important for business activities, and a rival or an internally placed person can tamper with the information or codes related to a woman's official site to harm her.[7]
- **Section 66** of the IT Act addresses examples of computer misuse like data theft, phishing, spreading viruses, and damaging computer systems. It is often used as a basis for prosecution in cybercrimes, with 3 years of imprisonment or 5 lakh Indian Rupees or both.[8]

[1] https://indianapublications.com/articles/IJEBM_5(6)_33-39_6929eb39a82c36.77704215.pdf
[2] https://www.defindia.org/wp-content/uploads/2024/08/An-exploratory-study-of-adoption-and-usage-of-technology-by-women-for-Entrepreneurship-and-Empowerment_2-August-2024.pdf
[3] https://acr-journal.com/article/digital-inclusion-of-women-entrepreneurs-in-the-unorganized-sector-a-systematic-review-879/
[4] https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women
[5] https://nluassam.ac.in/docs/Journals/NLUALR/Volume-7/Article%207.pdf
[6] https://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf
[7] Information Technology Act, 2000
[8] ibid

Case: Suhas Katti Vs. the State of Tamil Nadu 2004 He posted obscene and defaming messages online. This serves as one of the earliest convictions for cybercrimes in India and demonstrates that the distribution of obscene material (improper conduct) can be punished by law.[1]

- **Section 66C** – Identity Theft This section addresses fraudulent actions that use another person's digital identity to acquire gain. These fraudulent actions can include the unauthorized access or use of the following: passwords; digital signatures; and account sign-in credentials.

  Punishment: 3 year max prison term; maximum fine of ₹1 lakh[2]
- **Section 66D** – Cheating through impersonation using a computer resource This section relates to the use of computer resources to commit online fraud by impersonating another person in order to defrauding victims; for example, offenders may impersonate someone else using false email accounts, create fraudulent websites or use other means such as creating fake social media profiles.
  - **Penalty:** Imprisonment for a term not exceeding 03 YRS and a fine of not exceeding ₹1 lakh.
  - **Example:** The creation of fictitious Instagram or Whatsapp business accounts that are impersonating female entrepreneurs in order to defraud victims by collecting payments.
- **Section 66E -** Violation of Privacy This provision is a criminal offence to take, publish or transmit images of a person's private body parts without consent. The penalty is imprisonment for up to 3 years, or a fine up to ₹2

  Lakh, or both. Women entrepreneurs may be victims of the misuse of personal photographs resulting in harassment and/or extortion of money.
- **Section 67** - Publishing or Sending Obscene Materials This section addresses the electronic publication/transmission of obscene materials; the focus would be on online forms of harassment involving sexually explicit and/or offensive material.

  Punishment- First conviction = 3 years in prison with a possible monetary fine.

  Subsequent conviction = 5 years in prison with larger monetary fine.

Case: Avnish Bajaj v State (Bazee.com case) 2008 the former CEO of Bazee.com was prosecuted for selling obscene materials online. This case discussed intermediary liability and how regulation of online platforms is necessary to prevent the distribution of obscenity.[3]

The provisions found in the IT Act 2000 (India) are very important to help protect women entrepreneurs from being victimized by cyber-related crimes. The effectiveness of these laws will completely depend on creating awareness amongst the public, prompt reporting, and enforcing the law.

Relevant Case Law

- **Sexual Harassment & Online Harassment**

Vishaka v State of Rajasthan*& Ors.* (AIR 1997 SC 3011) This case did not involve cyberspace; however, it established guidelines regarding sexual harassment at work or the workplace. The Vishaka Guidelines apply equally to digital/online workspaces. Thus giving rise to the need to protect women entrepreneurs who are using digital platforms.[4]

- **Online Harassment and Cyberstalking**

In the Animesh Boxi versus State of West Bengal (2018) case, the accused was found guilty under IPC provisions as well as the IT Act for creating false identities as well as using inappropriate images of the victims.

- **Defamation Online**

Subramanian Swami v Union of India 2016 The Supreme Court ruled that criminal defamation is constitutional. Protects Women Entrepreneurs from false Internet allegations, phony reviews, and reputation damage.[5]

---

[1] https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3776961_code3922698.pdf?abstractid=3776961&mirid=1&__cf_chl_tk=JjstsVdBfpnnYRAPwLVZRxppCAtrA0d_tPPRA4v7aZs-1792684055-1.0.1.1-7iqchPhonHwz0c9.I6GRthlHYZElLPW77vHsFnqMPpw

[2] Information Technology Act, 2000

[3] https://indiankanoon.org/doc/309722/

[4] https://indiankanoon.org/doc/1031794/

[5] https://indiankanoon.org/doc/80997184/

- **Intermediary Liability – Online Content**

Shreya Singhal v Union of India 2015 Section 66A of the IT Act was declared unconstitutional.[1]

Clarified that only legitimate law enforcement officers can remove online content.

Relevance: Balances Freedom of Speech with Protection from Online Harassment.

- **Criminal Law Provisions: IPC Vs. BNS**

Cybercrimes committed against women businesses are addressed by the cybercrime and general crimes laws. While women businesses were protected from cybercrimes later covered under the IPC 1860, the current provisions of the IPC are being superseded by the 2023 Bharatiya Nyaya Sanhita (BNS), which will help to modernise and strengthen India's criminal justice system.

Comparative Table: IPC vs. BNS

Offence	IPC Section	BNS Section (2023)	Description
Sexual Harassment	Section 354A	Section 75	Covers unwelcome physical contact, sexual advances, and online harassment including explicit messages
Stalking (including cyber stalking)	Section 354D	Section 78	Monitoring a woman's online activity, repeated messages, or digital tracking
Defamation	Sections 499/500	Sections 356–357	Publishing false statements harming reputation, including online reviews or posts
Insult to Modesty of a Woman	Section 509	Section 79	Words, gestures, or online content insulting dignity or modesty

Additional Relevant Legislation

- Indecent Representation Of Women (Prohibition) Act 1986
- Sexual Harassment Of Women At Workplace (Prohibition) Act 2013
- Data Protection and Privacy Frameworks (Emerging Laws).
- Digital Personal Data Protection Act 2023.
- **Cyber Crime and Women Entrepreneurs: Critical Understanding**
- **Business Vulnerability -** Women-Owned Businesses Have Experienced: -
- Fake Reviews On The Internet Damaging Brand Value
- Unauthorized Access To Their Business Accounts
- Fraud And Scams Through Payments
- **Risks Associated with Gender**
- Sexual Harassment & Threats
- Image Morphing
- Blackmail & Extortion
- **Social & Economic Impact**
  - Depending on the nature of the crime, being a victim of cybercrime can cause many financial and non-financial issues, including:-
- Loss of income
- Loss of reputation
- Increased stress and reduced participation in the digital marketplace.

Challenges in Legal Protection

There are many limitations that arise despite the presence of strong laws.

- Women entrepreneurs continue to be unaware of legal remedies and reporting options.
- Women entrepreneurs often do not report crimes due to fear of social stigma or damage to their reputations.

[1] https://indiankanoon.org/doc/110813550/

- Weak enforcement by law enforcement and government agencies contributes to delays in investigating crimes that have been reported against women entrepreneurs; there are limited resources available to perform cyber forensics; there are not enough trained personnel to conduct necessary investigations.
- Jurisdictional issues arise with cybercrime, as often perpetrators are located outside the country in which the crime was committed, making enforcement difficult.

Government & Institutions

Initiatives taken by the Indian Government include:-

- Establishment of a national portal for reporting cybercrime
- A helpline number (1930) for cybercrime questions
- Digital Safety awareness campaigns
- Cyberspace law enforcement agencies & cyber cells are being actively strengthened, however, more initiative must be taken to help improve issues related to cybercrime.

Suggestions/Recommendations

- Legal Reforms:
- Simplification/unification of laws affecting the internet
- Gender-specific clauses in all internet laws
- Enhancing Law Enforcement
- Establishment of Specialty Cyber Courts
- Acceleration of Investigations and Trial Process
- Education & Training on Cyber Crime
- Education for Women in Business using Digital Media
- Cyber Crime Vulnerability & Awareness Training
- Detection using Artificial Intelligence (AI) / Cyber Threats
- Implementation of a Secure Data Storage / Protection System

Conclusion

Women entrepreneurs contribute substantially to India's economic development. The active participation of women entrepreneurs in the online economy needs to be supported by the establishment of a solid legal framework.

An existing legal framework regulates the activities that are carried out online. It consists of the Information Technology Act of 2000 and various criminal laws.

But the problem here arises with the enforcement and implementation of those two laws, which makes these laws ineffective.Thus, it is clear that a comprehensive approach towards the establishment of the secure environment for women entrepreneurs should be applied, which includes legal reform and improvement of institutions.

References

1. IT Act 2000
2. BNS, 2023
3. Indecent Representation of Women Act, 1986
4. Government of India Cyber Crime Reports
5. Research articles on cybersecurity and gender issues.

❑❑❑