IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

LAW AND VULNERABILITY IN THE ERA OF DIGITAL TRANSFORMATION: COMBATING CYBER ECONOMIC OFFENCES AGAINST WOMEN

DEEPTHI SOMAN
ASSISTANT PROFESSOR
GOVERNMENT LAW COLLEGE
THIRUVANANTHAPURAM
INDIA

Abstract
The era of digital transformation has amplified both opportunities and risks, with women increasingly becoming targets of sophisticated cyber economic offences. As digital platforms grow integral to woman's access to employment, education and entrepreneurship, so do their vulnerabilities to crimes such as phishing, identity theft, sextortion and online financial fraud. These offences often exploit traditional biases about women's roles and are further worsened by women's lack of digital knowledge and existing social inequalities. As a result, they not only undermine women's financial independence but also deepen the social and economic gaps they already face. This paper critically examines the legal and social dimensions of cybercrimes against women, highlighting the limitations of Information Technology Act,2000 in addressing gender-specific harms. It explores the psychological, emotional and financial impact of cyber economic offences on victims, particularly women and also highlights the legal and jurisdictional challenges that impede enforcement. The study suggests a comprehensive approach involving stronger legal protection, improved digital and financial awareness among women, the use of AI-based tools to detect threats, and the development of strong community support system. It emphasises the responsibility of social media platforms and digital finance service providers in fostering safer online environments. Ultimately, this paper advocates for inclusive, collaborative action across governmental, technological and civil society sectors to ensure that women can engage confidently and safely in the digital economy.

Keywords
Cyber economic crimes against women, women's digital safety, digital vulnerabilities, socio legal implications, jurisdictional complexities, Information Technology Act, AI-driven threat detection, community-based support, digital empowerment, gender disparities, cross border cybercrime, collaborative governance

Introduction

In traditional Indian culture women were highly esteemed and revered as goddesses embodying strength and divinity. They played a central role in the society, and their mistreatment was seen as demeaning to the community. However today, women often face objectification, undervaluation and systematic gender biases, creating an environment where some men feel entitled to act unjustly without accountability.

The digital age has transformed societal structures, offering connectivity and economic opportunities. The digital India initiative has revolutionised technology and integrated different digital platforms into daily life. While digital progress has strengthened India in areas like education, governance and the economy, it has also heightened vulnerabilities for marginalised groups, especially women.

The COVID-19 pandemic has accelerated our dependence on digital technologies, solidifying internet access as a vital human right. Digital platforms have often been hailed as tools for democratising self-expression and enabling equal participation across social strata. However, this promise of inclusivity has not been equally realised. In reality, the digital sphere increasingly serves as a site for exclusionary, violent and discriminatory discourse, often amplified by anonymity and lack of accountability that cyberspace affords.

Cybercrimes such as online harassment, phishing scams, identity theft and sextortion, have emerged as a new form of crime, fuelled by the anonymity of the internet. This anonymity shields perpetrators, making women frequent targets of digital abuse. Economic cybercrimes disproportionately affect women, driven by societal stereotypes, limited access to digital education and gaps in technological infrastructure. These crimes harm woman's financial independence and perpetuate gender disparities, discouraging their full participation in the digital world.

This article seeks to explore the intersection of gender, law and digital vulnerability by critically examining the legal and policy challenges in combating cyber economic offences against women in India. It argues for a more gender sensitive and technologically adaptive framework to ensure that digital empowerment does not come at the cost of digital exploitation.

Common cybercrimes against women

1. Cyber grooming

Cyber groomers use online platforms to form emotional connections with victims, often for exploitation, sexual abuse, or trafficking. They manipulate women by gaining their trust through deception. Young girls are more vulnerable to the online grooming which is a technology facilitated process of befriending a young person by an adult perpetrator for abusive purposes.[1]

2. Cyber Hacking

Hacking involves unauthorized access to personal data like financial information, addresses or private communications. Studies reveal that women are frequent targets of online harassment. According to a European study cited by UN Women, women are significantly more vulnerable to online harassment, being up to 27 times more likely than men to experience such abuse.[2] Cyber hacking compromises privacy leading to identity theft and financial losses. A study by the National Commission for Women in India found that 54.8% of women have faced cyber harassment, with 26% involving morphed images or videos.[3]

3. Online harassment

Online harassment includes abusive messages, comments or emails aimed at intimidating or demeaning women. Victims often face depression, anxiety and other mental health challenges, leading some to withdraw from public platforms which affects their career opportunities. Online threats may escalate to offline stalking or violence.

4. Revenge pornography

This crime involves sharing someone's intimate photos or videos without their permission, often to embarrass, control or take revenge on them. Women are disproportionately targeted, often by former partners, hackers or trolls. Perpetrators may demand money or compliance through threats of exposure. Victims suffer anxiety, depression, social ostracism and reputational harm.

5. **Fake Social media profiles**

Fake profiles are created using fabricated information or stolen identities to harass, deceive or defraud women. Perpetrators send abusive messages, post defamatory content or lure victims into exploitative relationships. Stolen images or personal details may be used for scams or blackmail, causing victims emotional distress, reputational damage and financial losses.

[1] Government of Gujarat,"Online grooming,"CAWACH, accessed June 8,2025 https://cawach.gujgov.edu.in/dist/documents/sop/cyberAwareness/OnlineGrooming.pdf

[2] U.N. Women, Creating Safe Digital Spaces Free of Trolls, Doxing, and Hate Speech (Nov.2023), https://www.unwomen.org/en/news-stories/explainer/203/11creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech

[3] Harish Yadav, *Unveiling the Dark Side of Cyberspace: A Study of Cyber Crimes Against Women in India*, 11 Int'l J. Food & Nutritional Sci. 3408 (2022), https://www.ijfans.org/uploads/paper/374cf990d6568e78319acc782da11df2.pdf

6. Online trolling

Trolling involves provocative, offensive comments aimed at harassing individuals. Women in public roles, such as journalists or activists, are frequent targets .Trolling can escalate to threats of violence leading victims to withdraw from online platforms due to mental and emotional harm.

7. Sexting and sextortion

Sexting involves consensual sharing of explicit messages or images, but these can later be misused. Sextortion occurs when perpetrators blackmail victims by threatening to share explicit content unless demands are met. Teenagers are particularly vulnerable, often targeted through fake profiles or malware. Victims experience shame, anxiety and financial loss.

8. **Doxxing**

Doxxing is a form of digital exposure where an individual's confidential or identifying information is deliberately shared online, typically without their knowledge or permission, to cause fear, distress or reputational harm. "Doxxing is defined as the intentional public release onto the internet the personal information about an individual by a third party, often with the intent to humiliate, threaten intimidate or punish the identified individual."[4] Attackers extract data from public posts or unauthorised account access. Victims face anxiety, reputational damage and social isolation, with stolen data sometimes used for fraud.

9. Cyber morphing

Morphing involves unauthorised editing of a person's images to create fake or explicit content, often shared on adult websites or social media.[5] Perpetrators use stolen photographs to manipulate images, causing emotional trauma, societal stigma and reputational harm.

10. Deepfakes

Deepfakes are hyper-realistic video or images generated using digital technology to falsely depict individuals engaging in actions or making statements they never actually performed. The widespread access to face-swapping tools has led to a surge in deepfake content, creating challenges in detecting and filtering them.[6] Women targeted by deepfakes face psychological, social and economic harm, including reputational damage, and ongoing abuse due to the permanent nature of digital content.

Cyber Economic crimes targeting women

Women face significant financial exploitation through cyber economic crimes, which leverage digital platforms and technology for financial gain or cause harm. These crimes not only drain victims financially but also disrupt their personal and professional lives leaving lasting emotional and psychological impacts. Some of the cyber economic crimes which specifically affects women includes:

1. Financial exploitation through cyber hacking

Gaining unauthorised access to sensitive financial data, such as bank account numbers, credit card credentials or personal records frequently results in identity theft and financial fraud. Offenders misuse the stolen information to secure illegitimate loans or carry out unauthorised purchases, often causing significant monetary harm to victims and leaving them in a financially vulnerable position.

2. Online scams through fake social media profiles

Online romance scams[7] have become a prevalent form of financial exploitation, where fraudsters create fake profiles to build emotional trust. Perpetrators use fabricated identities to manipulate women into providing money, often citing personal emergencies or travel expenses. If victims comply, scammers may demand additional funds often disappear after receiving money. Online dating platforms, combined with social pressures linking a woman's worth to her relationship status make women particularly susceptible to these scams. The anonymity of the internet allows perpetrators to target women, often from marginalised communities, increasing their financial and emotional suffering.

3. Cyber extortion through revenge pornography

Perpetrators use intimate images or videos to extort money, favours or compliance from women. Victims may face financial hardship by paying ransoms or incurring legal expenses to remove explicit content from the

[4] Douglas, D.M., *Doxing : A Conceptual Analysis*,18 Ethics & Info. Tech.199 (2016). https://doi.org/10.1007/s10676-016-9406-0
[5] Nidhi Agarwal & Neeraj Kaushik, Cyber Crimes Against Women, *Global J. of Research in Mgmt.*, Vol. 4, Issue 1 (2014)
[6] Pavel Korshunov & Sébastien Marcel, *DeepFakes: A New Threat to Face Recognition? Assessment and Detection*, *arXiv:1812.08685* (Dec. 20, 2018), https://doi.org/10.48550/arXiv.1812.08685
[7] Thumboo, Sharen & Mukherjee, Sudeshna, Digital Romance Fraud Targeting Unmarried Women, 2 DISCOV. GLOBAL SOC'Y 105 (2024), https://doi.org/10.1007/s44282-024-00132-x

internet. In conservative societies, exposure can lead to job loss, social ostracization and reputational damage, compounding the financial toll.

4. Financial impact of Sextortion on women

Sextortion involves using intimate photos or videos, often shared consensually for blackmail victims. Perpetrators threaten to distribute of explicit materials unless their demands are met, typically involving money, sex or emotional compliance. The victims are coerced into paying significant amounts to keep their images private, suffering both financial and emotional harm. Teenage girls and young women are especially vulnerable with cyber criminals exploiting social media to gain their trust before extorting them.

5. Financial and professional consequence of Online trolling

Online trolling while primarily affects mental health, also has significant financial and professional impacts on women. Female professionals particularly journalists, politicians and activists are disproportionately targeted to silence or discredit them. This often leads to women withdrawing from public platforms, hindering career opportunities, income potential, damage personal and professional networks. Legal fees to pursue justice further add financial burden on victims.

Challenges in preventing cyber economic crimes against women in India

Tackling cyber economic offences targeting women poses unique challenges, especially within the criminal justice framework due to the borderless and anonymous nature of cyberspace. Even though statutes like Information Technology Act,2000 and Bharatiya Nyaya Sanhita,2023 aim to address such crimes, gaps in enforcement persist as a critical concern. The key challenges include

1. Jurisdictional Challenges

Jurisdiction is a fundamental issue in addressing cybercrimes. The internet's transnational nature complicates the identification of where an offence occurred. Offences such as unauthorised sharing of private images or online blackmail often involve victims, perpetrators and evidence spread across different jurisdictions. India's reliance on traditional jurisdiction standards under Bharatiya Nagarik Suraksha Sanhita (BNSS) is insufficient for effectively addressing the transnational crimes. Additionally, India's non- membership in the Cybercrime Convention limits International cooperation, further complicating investigations thus delaying justice.

(2) Issues with search and seizure

Digital evidence is crucial in cyber economic offences, but collecting, storing and securing it presents challenges. The absence of specific systems or guidelines for cyber search warrants forces reliance on outdated conventional methods, which are often inadequate. Misuse of discretionary power by investigating officers during searches can violate of victim's privacy.

3. Encryption and Privacy barriers

Encryption technology, while essential for data security, poses challenges in cyber crimes investigations. For example, Cyberstalking or blackmail often involves encrypted communication, making it difficult for investigators to access critical evidence. Although Section 69 of the IT Act[8] allows data decryption, it can conflict with privacy rights, creating legal and ethical challenges.

4. Anonymity and attribution

The anonymity of cyberspace facilitates crimes against women including identity theft, financial fraud and online harassment. Attribution, which involves linking a cybercrime to specific individuals, devices or entities is often hindered by techniques used by perpetrators to avoid detection. These include VPNs, anonymous email services and remotely controlled malware-infected devices. Such devices often compromised without their owner's knowledge, can be manipulated to carry out cybercrimes. These methods make it difficult to trace offenders, frequently delaying justice for women victims.

5. Challenges in Electronic evidence and Cyber forensics

The collection and presentation of electronic evidence in courts require technical expertise, which is often lacking in India's investigative agencies. Challenges includes identifying tampered evidence, ensuring a proper chain of custody, and establishing authenticity. Inadequate cyber forensic infrastructure and the lack of trained personnels delay investigations, adversely affecting cases involving women.

6. Lack of awareness and sensitisation

Many cybercrimes targeting women go unreported due to societal stigma, lack of awareness or mistrust in law enforcement. Victims often hesitate to report incidents, fearing judgement or lack of support from authorities. Additionally, investigative officers are frequently not sensitised to handle such cases, leading to secondary victimisation.

[8] Information Technology Act ,2000

7. Deficit in International Cooperation

The transnational nature of cybercrime requires robust international collaboration. India's non signatory status to the Cybercrime convention[9] and the absence of reciprocal arrangements with other nations hinder cross-border investigations. Without mutual arrangements, accessing evidence located in foreign jurisdictions become a cumbersome and time-consuming process.

Role of judiciary in combating cybercrimes in India

Judiciary in India plays a critical role in addressing cybercrimes against women, significantly influencing legal frameworks and ensuring victim protection through its judgements and directives. By recognising the grave impact of online crimes like revenge pornography, cyber bullying and harassment, the judiciary has taken pro-active stance in safeguarding women's rights and well-being in the digital sphere

Judicial interventions and case laws

1. Safeguarding women's right in the digital space

The Supreme court has emphasised that consent and privacy are crucial in the digital world, stating that unsolicited sexual advances, offensive messages and other forms of harassment are punishable by law. The landmark judgement in Justice K.S. Puttaswamy (Retd.) V. Union of India[10] affirmed that the right to privacy is protected as a fundamental right under Article 21 of the Indian Constitution emphasising need for legal protection against nonconsensual sharing of intimate images, including revenge pornography. Similarly, in *Shafhi Muhammed Vs State of Himachal Pradesh*[11] the court ruled that the unauthorised distribution of explicit videos violates privacy rights, stressing the importance of safeguarding individuals from such violations in the digital space

2. Strengthening cybercrime response mechanisms

To ensure a comprehensive response to cybercrimes targeting women, the judiciary has mandated the establishment of specialised infrastructure for reporting and addressing such crimes. In *Prajwala Vs Union of India*[12], The Supreme Court instructed the government to create a centralised portal for reporting child sexual abuse material and establish cyber cells in all States and Union Territories. In *State Vs Jayanta Das*[13] following Supreme Court's directives the Odisha Court highlighted the importance of protecting women in cyberspace and convicted the accused for online harassment.

3. Obligations of intermediaries

The judiciary has held online intermediaries accountable for the swift removal of harmful content and the prevention of its dissemination. In *Mr X Vs Union of India and ors*[14],the Delhi High Court directed the removal of unlawful content from pornographic websites and instructed search engines to deindex it. In *Sabu Mathew George Vs Union of India*[15], the Supreme Court emphasised the accountability of online platforms in curbing advertisements that encourage gender discrimination, mandating adherence to the provisions of the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act,1994.

4. Awareness and Preventive measures

The Supreme Court has highlighted the essential role of public education and awareness in addressing cyber offences targeting women. In the case Shreya Singhal Vs Union of India[16], it struck down Sec 66 A of the IT Act[17] as unconstitutional, emphasising the necessity of safeguarding free speech while ensuring protection against online abuse and harassment.

Conclusion and suggestions

The digital era offers vast opportunities but also exposes women to increased risks, particularly in the form of cyber economic crimes. These crimes exploit societal biases, the anonymity of the internet, and technological vulnerabilities, causing significant emotional, social and financial harm. Jurisdictional challenges, inadequate cyber forensic resources, limited public awareness and weak international

[9] Council of Europe, Convention on Cybercrime (Budapest Convention), Nov.23,2001, ETS No.185, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[10] (2017) 10 S.C.C. 1

[11] 51 S.C., S.L.P. (Crl.) No. 2302 of 2017

[12] 2009 Latest Caselaw 231 SC.

[13] State of Odisha v. Jayanta Kumar Das, G.R. Case No. 1739/2012, T.R. No. 21/2013 (Orissa).

[14] 2023 DHC 2806, W.P.(CRL) 1505/2021

[15] (2018) 3 S.C.C. 229.

[16] AIR 2015 SC 1523

[17] Information Technology Act,2000

collaboration hinder effective prevention and prosecution in India. Addressing these gaps requires a coordinated and comprehensive approach.

Suggestions

1. Strengthen legal and policy frameworks

- Introduce specialised cybercrime legislation that acknowledges the faceless and borderless nature of cybercrimes while addressing the unique vulnerabilities faced by women
- Clarify the definition of cyber crimes and economic offences under BNS[18] and amend provisions in the BSA to streamline the admission of electronic evidence and digital search procedures[19]
- Enact robust data protection laws to safeguard personal information and prevent unauthorised access

2. Enhancing cyber forensic capabilities

- Establish cyber forensic labs equipped with advanced tools for decrypting and analysing data in each state.
- Provide specialised training to law enforcement personnel on forensic techniques and ensure cases involving women are handled with sensitivity and care.

3. Foster International collaboration

- India should be a part of global conventions like Budapest Convention on Cyber crimes to enhance cross-border cooperation
- Develop mutual legal assistance treaties with key countries to streamline the sharing of evidence and improve the efficiency of international investigations

4. Promote victim support and awareness

To empower women and ensure their safety online, it is essential to

- Launch nationwide awareness campaigns that educate women about online safety, recognising cybercrimes and reporting mechanisms.
- Setup secure user friendly platforms for anonymous reporting of cybercrimes, supported by dedicated helplines and counselling services to offer guidance and assistance

5. Building capacity in law enforcement

- Conduct gender sensitisation workshops for police, prosecutors and judicial members, to address the unique challenges women face online.
- Equip law enforcement agencies with advanced tools to track anonymous offenders and preserve digital evidence

6. Strengthening monitoring and reporting mechanisms

- Create a centralised crime reporting system for effectively tracking cybercrimes and improve coordination among agencies
- Employ AI powered monitoring tools to proactively detect and mitigate online threats targeting women

7. Encouraging community involvement

- Collaborate with NGOs and educational institutions to enhance digital literacy, particularly in marginalised communities
- Establish peer support networks both online and offline where women can share experiences and provide guidance on navigating digital challenges.

8. Enhancing international cooperation

- Develop transnational cooperation frameworks to support global cybercrime investigations and create a global repository of cybercriminal tactics to anticipate and address emerging threats.

Implementing these suggestions through targeted reforms and fostering a culture of accountability can significantly enhance the safety of digital environments for women in India. Ensuring a secure and inclusive cyberspace requires joint engagement by governmental bodies, industry stakeholders and community organisations.

[18] Under Sec 111, Bharatiya Nyaya Sanhita,2023, cybercrimes and economic offences are mentioned as organised crimes but there is no definition of the offences in the Section

[19] Bharatiya Sakshya Adhiniyam,2023