

SOCIAL MEDIA FRAUDS TARGETING WOMEN IN INDIA: LEGAL ISSUES AND PREVENTIVE MEASURES

Dr. Ajay D. Patel

Assistant Professor,

V.T. Choksi Sarvajanik Law College, Surat

Veer Narmad South Gujarat University, Surat, Gujarat

Abstract

The rapid expansion of social media platforms has significantly transformed communication, networking and access to information, particularly empowering women by providing opportunities for expression, entrepreneurship and social participation. However, alongside these benefits, social media has also emerged as a major medium for fraudulent activities disproportionately targeting women in India. Women are increasingly becoming victims of social media frauds such as fake profiles, romance scams, financial frauds, identity theft, impersonation, online job scams and fraudulent matrimonial offers. These crimes not only cause financial loss but also result in psychological trauma, social stigma and erosion of digital trust, thereby undermining women's empowerment.

This paper examines the legal issues arising from social-media frauds targeting women in India and evaluates the adequacy of the present legal framework. It focuses principally on the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology Act, 2000 (IT Act), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA). The paper also considers the Digital Personal Data Protection Act, 2023 (DPDP Act), to the extent relevant to personal-data protection and subject to the staged commencement of its provisions.

The research adopts a doctrinal methodology, relying on statutory provisions, judicial decisions, reports and secondary sources to identify key legal challenges such as anonymity of offenders, jurisdictional issues, lack of digital awareness and under-reporting of cyber frauds by women. The paper further highlights gaps in implementation and enforcement mechanisms that hinder effective legal protection.

Finally, the study proposes preventive measures including legal reforms, gender-sensitive cyber policing, digital literacy programs, platform accountability and stronger awareness initiatives to combat social media frauds. The paper concludes that while social media holds immense potential for women's empowerment, robust legal safeguards and preventive strategies are essential to ensure a safe and inclusive digital environment for women in India.

Keywords:

Social Media Frauds, Women in India, Cyber Crime, Legal Framework, Preventive Measures.

Introduction

The rapid advancement of digital technology and widespread penetration of the internet have transformed social media into a powerful tool for communication, expression and social participation. In India, social media platforms such as Facebook, Instagram, WhatsApp, X (formerly Twitter) and various online networking applications have significantly contributed to women's empowerment by enabling access to information, economic opportunities, education and social connectivity. These platforms have provided women with new avenues for self-expression, entrepreneurship, professional networking and social awareness, thereby strengthening their participation in the digital public sphere.

However, alongside these empowering possibilities, social media has also emerged as a fertile ground for fraudulent activities, disproportionately affecting women. The anonymity, speed and borderless nature of social media platforms have facilitated the growth of various forms of fraud targeting women, including fake profiles, romance scams, financial frauds, identity theft, impersonation, online job scams and fraudulent matrimonial offers. Such fraudulent activities often exploit emotional vulnerability, financial dependence, digital illiteracy and societal trust, making women particularly susceptible to cyber deception.

Social media frauds against women have far-reaching consequences beyond monetary loss. Victims often suffer psychological trauma, loss of self-confidence, reputational harm and social stigma, which discourages reporting and further marginalizes them. These harms directly undermine the broader objective of women's empowerment by restricting women's safe participation in digital spaces. Despite the increasing incidence of such crimes, many cases remain unreported due to fear, lack of awareness and inadequate institutional support mechanisms.

The Indian legal system has sought to address cyber-enabled frauds through various statutory frameworks, including the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000 and allied cyber laws. The judiciary has also played a crucial role in interpreting these laws to protect victims of cyber-crimes, including women. However, the rapidly evolving nature of social media technologies poses significant challenges to the effectiveness of existing legal provisions and enforcement mechanisms.

In this context, the present paper seeks to examine the growing problem of social media frauds targeting women in India, analyze the adequacy of the existing legal framework and highlight

the key legal and practical challenges involved. The paper also emphasizes the need for preventive measures and policy interventions to ensure a safer digital environment that truly supports women's rights and empowerment in the digital age.

Literature Review

The issue of frauds against women in digital and social media spaces has attracted increasing scholarly attention in recent years, particularly with the rapid growth of internet penetration and social networking platforms in India. Existing literature broadly examines cyber frauds against women from legal, sociological, technological and gender justice perspectives, highlighting the multifaceted nature of the problem.¹

Legal scholarship on cybercrimes against women primarily focuses on the adequacy of existing statutory frameworks such as the Information Technology Act, 2000 and criminal law provisions dealing with cheating, fraud and impersonation. Several studies emphasize that while Indian cyber laws recognize offences such as identity theft, online cheating and electronic fraud, they were not originally designed with gender-specific vulnerabilities in mind.² Scholars have pointed out that social media frauds often fall within overlapping legal provisions, creating challenges in investigation, classification of offences and prosecution.³

Sociological and gender studies literature highlights that women are disproportionately targeted on social media due to factors such as social conditioning, trust-based online interactions, emotional manipulation and unequal access to digital literacy. Research in this domain underlines how frauds such as romance scams, fake matrimonial profiles and employment-related scams exploit emotional dependency and socio-economic pressures faced by women.⁴ These studies also draw attention to the psychological consequences of such frauds, including trauma, fear, loss of dignity and social withdrawal, which are often more severe than financial losses.⁵

Policy-oriented literature, including reports by government agencies and national crime data analyses, has consistently recognized cyber frauds against women as a growing threat to digital inclusion and empowerment. Official crime statistics reveal a steady rise in cyber-enabled cheating and online deception cases, with social media platforms emerging as common

¹ . United Nations Office on Drugs and Crime, Gender-related aspects of cybercrime (UNODC, 2023).

² . Information Technology Act, 2000 (India).

³ . Law Commission of India, Report No. 272 on Implementation of the Criminal Law Amendment Act, 2018 (2017–18).

⁴ . National Commission for Women, Cyber Crime against Women: Advisory and Reports (India).

⁵ . National Institute of Mental Health and Neurosciences (NIMHANS), Psychological Impact of Cyber Crimes on Women (Government of India).

mediums for such offences.⁶ These reports emphasize the need for improved reporting mechanisms, gender-sensitive cyber policing and institutional capacity building.⁷

Judicial discourse, as reflected in decisions of the Supreme Court and various High Courts, reveals an evolving recognition of the misuse of digital platforms for fraudulent activities. Courts have acknowledged the seriousness of cyber-enabled frauds and emphasized the duty of the State to ensure effective investigation, victim protection and technological preparedness of law enforcement agencies.⁸ However, legal commentaries note inconsistencies in judicial approaches due to the absence of a comprehensive legal framework specifically addressing social media frauds against women.⁹

Despite the growing body of work, existing literature largely treats social media frauds against women as a subset of cyber crime, without sufficient focus on preventive strategies tailored to platform-based risks. Limited attention has been paid to preventive legal mechanisms, platform accountability and digital awareness initiatives aimed at empowering women users.¹⁰ This gap underscores the need for focused legal research that integrates law, technology and prevention to ensure women's safety and empowerment in digital spaces.

Objectives of the Study

The present paper aims to study the problem of social media frauds affecting women in India from a legal perspective. With the increasing use of social networking platforms by women for personal, professional and economic purposes, incidents of fraud committed through these platforms have also increased. In this background, the objectives of the study are as follows:

1. To understand the concept and nature of social media frauds and the common ways in which women are targeted on digital platforms.
2. To examine the existing legal provisions in India dealing with frauds committed through social media, with reference to criminal law and cyber laws.
3. To analyze how effectively the present legal framework addresses the issue of frauds against women in the online environment.
4. To study the approach of Indian courts in cases relating to social media frauds and their role in protecting women's rights in digital spaces.

⁶ . National Crime Records Bureau, Crime in India Report (Latest available edition), Chapter on Cyber Crimes.

⁷ . Ministry of Home Affairs, Government of India, Cyber Crime Prevention against Women and Children (CCPWC) Scheme.

⁸ . Shreya Singhal v. Union of India, (2015) 5 SCC 1.

⁹ . State of Maharashtra v. Mohd. Yakub, AIR 1980 SC 1111 (principles on cheating and fraud applied in cyber context).

¹⁰ . OECD, Online Safety and Gender Equality in Digital Spaces (Policy Brief).

5. To identify the major difficulties faced by victims and law enforcement agencies in reporting, investigation and prosecution of such frauds.
6. To suggest practical and legal preventive measures to reduce social media frauds and to ensure a safer and more secure digital environment for women.

Research Methodology

The present study adopts the doctrinal research method. The research is mainly based on secondary sources of data such as law books, journals, research articles and monthly magazines. Relevant materials were also collected from online sources including ResearchGate, Google Scholar and official websites to understand the legal issues related to social media frauds targeting women in India.

Legal Framework

Social media frauds targeting women in India are addressed under a combination of criminal law and cyber law provisions. Although there is no separate legislation exclusively dealing with social media frauds, existing laws provide remedies to deal with cheating, fraud, impersonation and misuse of electronic platforms.

Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS) contains general provisions relating to fraud and cheating, which are applicable to offences committed through social media. Acts such as cheating, dishonestly inducing delivery of property, criminal breach of trust and impersonation committed through online platforms fall within the scope of these provisions. When social media is used as a medium to deceive women for financial gain or other wrongful purposes, the offence is punishable under the relevant sections of the BNS, irrespective of the digital nature of the act.

Information Technology Act, 2000

The Information Technology Act, 2000 plays a crucial role in dealing with technology-enabled frauds. The Act recognizes offences such as identity theft, cheating by personation using electronic means and unauthorized use of computer resources. Provisions of the Act are particularly relevant in cases where social media platforms are misused for creating fake profiles, impersonation, phishing links, fraudulent messages and extraction of personal or financial information from women.

Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS supplies the procedural framework for investigation, inquiry and trial. Section 202 deals with offences committed by means of electronic communications, letters, etc., and is relevant to jurisdictional questions in appropriate cases. Section 94 permits a Court or police officer to require production of documents, electronic communications, including communication devices likely to contain digital evidence. Section 105 provides for recording of search and seizure through audio-video electronic means. Section 530 permits trials, inquiries and proceedings to be conducted in electronic mode in accordance with the provision. These provisions are significant because cyber-fraud cases frequently require preservation, collection and production of digital evidence across different locations.

Bharatiya Sakshya Adhiniyam, 2023

Electronic evidence is central to social-media fraud cases. BSA section 61 recognises electronic or digital records and gives them legal effect subject to the statutory requirements. Section 62 contains special provisions relating to electronic records and section 63 provides for admissibility of electronic records subject to the conditions stated in the provision. Screenshots, emails, chats, transaction records, device data and other electronic material should therefore be collected and preserved carefully, with attention to authenticity, integrity, source and the statutory requirements for admissibility.

Digital Personal Data Protection Act, 2023

The DPDP Act provides a framework concerning the processing of digital personal data and the protection of individuals' personal data. Its provisions have been brought into force in stages through notification, so its application to a particular incident must be assessed according to the provision and date applicable at the relevant time. The Act should therefore be treated as a complementary data-protection framework rather than as a substitute for criminal provisions governing cheating, personation or identity theft.

Other Allied Laws and Mechanisms

In addition to criminal and cyber laws, banking regulations, digital payment guidelines and cyber crime reporting mechanisms support victims of online fraud. The establishment of cyber crime cells and online reporting portals has made it easier for women to report social media

frauds. Courts have also relied on procedural laws to ensure investigation and prosecution of cyber offences.

Judicial Interpretation

Indian courts have acknowledged that traditional criminal law principles apply equally to offences committed in the digital space. Judicial interpretation has helped extend the scope of existing laws to cover new forms of social media frauds. However, courts have also highlighted the need for effective enforcement and technological preparedness to deal with the growing complexity of cyber-enabled crimes.

Types of Social Media Frauds Targeting Women

Social media platforms are increasingly being misused to commit different types of frauds against women. Some of the common forms are discussed below:

Fake Profile and Impersonation Fraud:

Fraudsters create fake social media profiles by using false names, photographs or stolen identities to gain the trust of women. These profiles are often used to establish emotional connections and later exploit victims financially or psychologically.

Romance and Relationship Scams:

In such cases, offenders develop online romantic relationships with women and gradually demand money on false pretexts such as medical emergencies, travel expenses or business losses. Women are emotionally manipulated, making detection difficult.

Financial and Payment Frauds:

Women are targeted through fraudulent links, fake messages, UPI requests and online investment offers circulated via social media platforms. Clicking on malicious links often leads to unauthorized access to bank accounts or digital wallets.

Job and Work-from-Home Scams:

Fraudsters lure women with fake job offers, part-time work or online assignments. Victims are asked to pay registration fees or share personal and banking details, resulting in financial loss.

Matrimonial and Marriage-related Frauds:

Social media and online matrimonial platforms are misused to deceive women by making false promises of marriage, often leading to financial exploitation and emotional harm.

Case Laws Analysis

Indian courts have recognized the misuse of digital and social media platforms for fraudulent purposes and have applied existing legal principles to such offences. In *Shreya Singhal v. Union of India*, the Supreme Court acknowledged the importance of balancing freedom of expression with the need to prevent misuse of online platforms. Although the case did not deal directly with fraud, it highlighted the serious impact of online misuse.

In *State of Tamil Nadu v. Suhas Katti*, one of the early cyber crime cases in India, the court recognized the use of electronic platforms to commit offences and upheld the applicability of cyber laws. Courts have also consistently held that cheating, impersonation and fraud committed through online means are punishable under criminal law, irrespective of the medium used.

Judicial decisions indicate that traditional principles of criminal liability apply equally to offences committed through social media. However, courts have also emphasized the need for proper investigation and technical expertise in cyber fraud cases.

Challenges

Despite the existence of legal provisions, several challenges hinder effective control of social media frauds against women:

- **Anonymity of offenders**, making identification difficult
- **Jurisdictional issues**, especially when offenders operate from different states or countries
- **Lack of digital awareness** among women users
- **Under-reporting of offences** due to fear, stigma or lack of confidence
- **Limited technical expertise** within law enforcement agencies
- **Delay in investigation and trial** of cyber-related offences

These challenges reduce the effectiveness of legal remedies and discourage victims from seeking justice.

Preventive and Legal Measures

Early Reporting

Victims should report cyber offences promptly through the National Cyber Crime Reporting Portal. The official portal provides categories for women/children-related crime, financial fraud and other cyber crime, and also provides mechanisms for reporting suspect identifiers and social-media abuse. For financial cyber fraud, the portal currently directs victims to the 1930 helpline for immediate reporting.

Preservation of Digital Evidence

Victims should preserve screenshots, complete chat histories where possible, profile links, usernames, telephone numbers, email addresses, transaction IDs, bank statements, UPI details, URLs and relevant device information. Evidence should not be altered or unnecessarily deleted after reporting.

Gender-Sensitive Cyber Policing

Police and cybercrime personnel should receive training in digital evidence, victim-sensitive interviewing, online financial fraud and the particular social pressures that may discourage women from reporting. Institutional mechanisms should reduce repeated trauma during complaint and investigation processes.

Platform Accountability and Cooperation

Social-media platforms should provide accessible mechanisms for reporting impersonation, fraud and abusive accounts, preserve relevant information subject to law, and respond appropriately to lawful requests from investigative agencies.

Digital Literacy

Women and other users should be educated about verification of profiles, suspicious links, payment requests, investment offers, job advertisements and requests for passwords or one-time authentication credentials. Digital literacy should be treated as a continuing public-awareness measure rather than a one-time campaign.

Recommendations

- Develop specialised, adequately staffed cybercrime investigation units with gender-sensitive training.
- Improve coordination between police, banks, payment intermediaries, telecom operators and social-media platforms.
- Create standard operating procedures for preservation and collection of social-media and transaction evidence.
- Strengthen public awareness concerning impersonation, romance, investment, job and matrimonial scams.
- Encourage rapid reporting of financial cyber fraud so that lawful intervention may be attempted at the earliest stage.
- Provide accessible victim-support and legal-awareness mechanisms, particularly for victims hesitant to approach police.

- Periodically review cyber-law and platform-governance frameworks in response to emerging technologies such as generative AI, synthetic identities and automated scams.
- Undertake empirical research using verified government statistics rather than relying on general statements about increasing incidence.

Conclusion

Social media has emerged as a powerful tool for women's empowerment, providing opportunities for communication, education and economic participation. However, its misuse for fraudulent activities poses serious threats to women's safety, dignity and financial security. Social media frauds not only cause economic loss but also create psychological distress and discourage women from participating freely in digital spaces.

While Indian laws provide remedies to deal with such offences, rapid technological developments and enforcement challenges limit their effectiveness. There is an urgent need for a balanced approach that combines legal reforms, judicial support, technological safeguards and social awareness. Ensuring a safe digital environment is essential for achieving genuine women's empowerment and protecting women's rights in the digital age.

References

- The Bharatiya Nyaya Sanhita, 2023, Government of India, India Code.
- The Information Technology Act, 2000, Government of India, India Code.
- The Bharatiya Nagarik Suraksha Sanhita, 2023, Government of India, India Code.
- The Bharatiya Sakshya Adhiniyam, 2023, Government of India, India Code.
- The Digital Personal Data Protection Act, 2023, Government of India, India Code.
- National Cyber Crime Reporting Portal, Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- State of Tamil Nadu v. Suhas Katti, cyber-crime decision concerning online publication and the Information Technology Act.
- United Nations Office on Drugs and Crime, materials on gender-related aspects of cybercrime.

- National Commission for Women, materials and advisories concerning cyber crime against women.