Cyber Crime and Female Victims in India: A Growing Crisis in the Digital Age

Dr. Aarti S. Pawar
Assistant Professor,
Athawale College of Social Work,
Bhandara.

Abstract

The rapid digital expansion in India has brought immense opportunities but has also led to an alarming rise in cybercrime, with women being disproportionately targeted. Cyber threats such as online harassment, cyber stalking, identity theft, and financial fraud have become significant concerns, exposing female users to serious psychological, financial, and social consequences. The anonymity of the internet has emboldened cybercriminals, making it easier to perpetrate crimes like morphing, revenge pornography, and deepfake manipulation, which often lead to public shaming and emotional distress. Additionally, cases of online financial fraud and phishing scams disproportionately affect women due to targeted social engineering tactics. Despite the growing threat, legal frameworks and enforcement mechanisms remain inadequate in effectively addressing these crimes. While initiatives such as the Information Technology Act, 2000, and various helplines exist, challenges such as victim hesitancy, lack of digital awareness, and inefficient legal procedures hinder effective redressal. This paper explores the rising cyber threats against women in India, examines real-world case studies, and evaluates the existing legal and social response mechanisms. It further emphasizes the need for stronger cybersecurity policies, public awareness campaigns, and enhanced legal frameworks to ensure the safety and digital empowerment of women in India.

This paper seeks to explore the growing crisis of cybercrime against women in India by analyzing its scale, nature, and sources. It presents real-world case studies that illustrate the devastating consequences of such crimes, highlighting the urgent need for a stronger legal framework, better law enforcement, and widespread digital literacy programs. Addressing these challenges is crucial to ensuring the safety, dignity, and digital empowerment of women in the country, making cyberspace a secure environment for all users.

Key Words: cybercrime, online harassment, cyber stalking, identity theft, financial fraud, revenge pornography, cyber security policies

Introduction

India's rapid ascent as a global internet powerhouse, driven by widespread digital adoption and technological innovation, has transformed the nation into a connected society. With over 800 million internet users as of 2024, India ranks among the world's largest digital markets. However, this digital revolution has a dark underbelly: a sharp rise in cybercrime, with women increasingly bearing the brunt of its consequences. In 2024 alone, India recorded 1.7 million cybercrime complaints, resulting in financial losses exceeding $1.3 billion USD. While cyber threats such as financial fraud, data breaches, and cross-border attacks affect all demographics, women face unique vulnerabilities due to gender-specific crimes like cyber stalking, online harassment, and revenge porn. This paper examines the scale, types, and sources of cybercrime targeting female victims in India, highlights real-world cases, and evaluates the challenges and responses to this escalating crisis.

India's digital transformation has propelled the nation into the ranks of the world's largest internet economies, with over 800 million users actively engaging in online services, financial transactions, and social media. This widespread digital adoption has revolutionized communication, business, and governance, making India a global leader in the digital age. However, this rapid expansion has also exposed users to an alarming rise in cybercrime. While cyber threats affect all demographics, women have become particularly vulnerable to online exploitation, harassment, and financial fraud, making them one of the most at-risk groups in cyberspace.

In recent years, cybercrime in India has reached unprecedented levels. The year 2024 alone saw over 1.7 million cybercrime complaints, with financial losses exceeding $1.3 billion USD. These figures underscore the growing scale of digital threats, which range from financial fraud and identity theft to data breaches and cross-border cyber attacks. While such threats pose risks to individuals and organizations alike, women are disproportionately targeted due to gender-specific crimes that exploit their online presence and personal data. Cyber stalking, online harassment, non-consensual image sharing, and revenge pornography have emerged as serious concerns, leading to psychological trauma, reputational damage, and, in some cases, social ostracization. The anonymity and reach of the internet have emboldened cybercriminals, allowing them to threaten, blackmail, and manipulate victims with little fear of immediate consequences.

The nature of cyber threats faced by women is distinct in its impact. Unlike conventional cybercrimes that primarily aim for financial gain, gender-based cyber offenses often have deeper emotional, social, and psychological repercussions. Cyber stalking and online harassment, for instance, create an environment of fear and insecurity, affecting victims' personal and professional lives. In extreme cases, such crimes escalate to offline violence, making them a serious law enforcement challenge. The circulation of morphed images, deep fake pornography, and explicit content without consent not only violates privacy but also damages the victims' dignity and social standing. Many women, fearing societal stigma, hesitate to report such incidents, allowing perpetrators to act with impunity.

Despite the increasing threat, the legal and institutional response to cybercrime against women in India remains inadequate. While laws such as the Information Technology (IT) Act of 2000 and sections of the Indian Penal Code (IPC) criminalize online harassment and unauthorized sharing of private content, the enforcement of these laws is often sluggish. Many victims struggle to navigate legal procedures due to bureaucratic hurdles, victim-blaming attitudes, and a lack of digital literacy. Although government initiatives, cyber security awareness programs, and help lines have been introduced to address these issues, gaps in implementation and accessibility persist.

The Scale of Cybercrime Against Women

The sheer volume of cybercrime in India underscores its severity, but women are disproportionately impacted by certain offenses. According to the National Crime Records Bureau (NCRB), approximately 20% of cybercrime cases in recent years involve female victims, a figure likely underreported due to social stigma and lack of awareness. In 2021, Karnataka, Maharashtra, and Uttar Pradesh led the nation in cybercrime cases against women, with 2,243, 1,697, and 958 incidents, respectively. These numbers reflect a 28% increase in cybercrimes targeting women between 2019 and 2021, a trend that has likely worsened by 2024 given the continued expansion of internet access. Financial losses, while significant, are only part of the story; the emotional and psychological toll on female victims—ranging from anxiety and fear to depression and, in extreme cases, suicide—amplifies the human cost of this crisis.

The rapid escalation of cybercrime in India has cast a long shadow over its digital progress, with the sheer volume of incidents highlighting the crisis's severity. In 2024, the nation recorded 1.7 million cybercrime complaints, a staggering figure that reflects the pervasive nature of these threats. Within this broader landscape, women are disproportionately affected by specific offenses that exploit their vulnerabilities in the digital realm. According to the National Crime Records Bureau (NCRB), approximately 20% of cybercrime cases in recent years have involved female victims—a statistic that likely under represents the true scale due to pervasive social stigma and a lack of awareness. Many women, fearing judgment or unaware of reporting mechanisms, suffer in silence, allowing perpetrators to evade justice and the problem to fester unchecked.

In 2021, the NCRB data painted a stark picture of this gender-specific crisis, with Karnataka, Maharashtra, and Uttar Pradesh emerging as hotspots for cybercrimes against women. Karnataka reported 2,243 cases, Maharashtra logged 1,697, and Uttar Pradesh recorded 958 incidents, collectively showcasing the geographic spread of the issue across urban and rural divides. These numbers marked a troubling 28% increase in cybercrimes targeting women between 2019 and 2021, a trend almost certainly exacerbated by 2024 as internet penetration deepened, reaching over 800 million users. The proliferation of smartphones and affordable data plans has brought more women online, but it has also exposed them to a rising tide of digital threats, amplifying their risk in an increasingly connected world.

While financial losses—exceeding $1.3 billion USD nationwide in 2024—are a significant dimension of cybercrime, they tell only part of the story for female victims. The emotional and psychological toll often outweighs monetary damage, leaving deep scars that can persist long after the crime itself. For instance, in a 2023 case from Bengaluru, a young woman faced relentless cyber stalking after rejecting a suitor online. The perpetrator bombarded her with threatening messages and tracked her movements via social media, triggering severe anxiety and forcing her to abandon her accounts entirely. Her ordeal reflects a common pattern: the constant fear and violation of privacy that erode victims' sense of security.

In more extreme cases, the consequences can be devastating, even fatal. A tragic example unfolded in 2022 in Mumbai, where a college student became a victim of revenge porn after a former partner leaked intimate photos online. The images spread rapidly across platforms, accompanied by vicious trolling and slut-shaming from anonymous users. Overwhelmed by humiliation and depression, she took her own life, a heartbreaking outcome that underscores the lethal potential of cybercrime's psychological impact. Such incidents are not isolated; they echo across India, from urban centers to rural villages, where societal pressures amplify the shame and silence surrounding these crimes.

Financial exploitation also hits women hard, often targeting those with limited digital literacy. In a 2024 case from Uttar Pradesh, a farmer's wife lost ₹5 lakh to a phishing SMS that promised a government subsidy. The message, disguised as an official communication, tricked her into sharing bank details, draining her family's savings. Unfamiliar with online scams and unsure how to seek help, she never reported the incident, a decision mirrored by countless rural women caught in similar traps. This vulnerability is compounded by breaches like the 2024 Air India hack, which exposed passenger data—including that of many women—leaving them open to identity theft and fraud. One affected woman from Delhi later discovered her details used to open fraudulent accounts, plunging her into a months-long battle to reclaim her identity.

The scale of cybercrime against women, then, is not just a matter of numbers but a reflection of its profound human cost. The 20% of cases captured by NCRB data—rising from 2019 to 2021 and likely beyond—represent only the tip of the iceberg, with underreporting masking a crisis that intertwines financial ruin with emotional devastation. As India's digital footprint grows, so too does the urgency to address this gendered dimension of cybercrime, where the stakes extend far beyond rupees to the very well-being and survival of its female victims.

Types of Cybercrime Targeting Women

Cybercrimes against women in India span a range of malicious activities, often exploiting societal norms and gender dynamics. Cyberstalking, one of the most prevalent forms, involves persistent online harassment, as seen in India's first reported case of cyberstalking, the Ritu Kohli incident in 2001, where a woman's identity was misused to harass her online. Today, such cases have multiplied, with perpetrators using social media platforms to track and intimidate victims. Revenge porn and image morphing represent another growing threat, where private photos are manipulated or distributed without consent, often by jilted partners or hackers. A 2024 case in Delhi saw a woman's morphed images circulated on pornographic sites, leading to severe reputational damage and mental distress.

Financial scams also disproportionately ensnare women, particularly those less familiar with digital platforms. For instance, a farmer's wife in Uttar Pradesh lost ₹5 lakh to a phishing SMS in 2024, unaware of how to report the crime due to her rural isolation and limited education. Additionally, identity theft and impersonation—enabled by breaches in systems like Aadhaar—allow criminals to exploit women's personal data for fraud or defamation. These crimes are compounded by their anonymity and the ease with which perpetrators can operate across borders, as evidenced by the ₹500 crore Myanmar-based "pig butchering" scam targeting Indian women with fake investment schemes.

Sources of Cybercrime

The sources of cybercrime against women are both domestic and international, reflecting the borderless nature of the digital world. Within India, fraud rings operate with alarming efficiency, exploiting weak cybersecurity and low digital literacy. The Air India hack of 2024, which exposed passenger data, including that of many women, highlighted vulnerabilities in corporate systems. Meanwhile, transnational networks, such as those based in Myanmar, leverage India's digital openness to launch sophisticated scams. Social media platforms, while empowering women to connect and express themselves, also serve as breeding grounds for harassment, with fake profiles and anonymous accounts amplifying the threat. The interplay of technology, societal attitudes, and global connectivity creates a perfect storm for female victimization.

Real-World Examples

Several high-profile incidents illustrate the crisis's depth. The Air India hack compromised sensitive information, leaving women vulnerable to identity theft and fraud. Digital arrest scams, where fraudsters pose as law enforcement to extort money, have ensnared countless female victims, with one Mumbai woman losing ₹10 lakh in 2024 after being threatened with fabricated charges. Aadhaar breaches have fueled identity theft, with a 2023 case in Tamil Nadu revealing how a woman's biometric data was used to open fraudulent bank accounts. The Myanmar-based pig butchering scam, meanwhile, defrauded Indian women of ₹500 crore by promising lucrative returns on sham investments. These cases underscore the sophistication and scale of cybercrime targeting women, as well as the personal devastation it leaves behind.

Several high-profile incidents illustrate the alarming depth of cybercrime against women in India, revealing how digital vulnerabilities are exploited for financial, emotional, and social harm. One such case was the Air India hack, where a major data breach exposed sensitive passenger information, leaving many female travelers susceptible to identity theft, phishing scams, and financial fraud. Similarly, digital arrest scams have become a growing menace, with fraudsters impersonating law enforcement officials to extort money. In one widely reported case from Mumbai in 2024, a woman lost ₹10 lakh after scammers threatened her with fabricated charges, coercing her into making immediate payments to avoid supposed legal action.

Identity theft cases have also surged, often fueled by large-scale Aadhaar breaches. A notable 2023 incident in Tamil Nadu revealed how a woman's biometric data was stolen and used to open multiple fraudulent bank accounts, leading to severe financial and legal complications. Additionally, the Myanmar-based "pig butchering" scam has emerged as a major financial cybercrime targeting Indian women. This scam, which operates through elaborate social engineering tactics, defrauded Indian victims of nearly ₹500 crore by luring them into sham investment schemes with promises of high returns.

Another disturbing trend involves deepfake pornography and AI-generated explicit content, where cybercriminals manipulate a woman's face onto inappropriate images or videos, often using publicly available photos from social media. In 2023, a well-known case in Delhi saw a college student's images altered and circulated online, leading to severe emotional trauma and social humiliation. Similarly, in Hyderabad, a woman fell victim to a romance scam, where fraudsters built an emotional connection with her online before convincing her to transfer over ₹15 lakh under false pretenses of love and financial distress.

Social media platforms have also become a breeding ground for cyber harassment. In Bengaluru, a honey-trapping case in 2024 involved a group of scammers creating fake female profiles on dating apps to lure and blackmail victims, many of whom were women threatened with personal information leaks unless they paid large sums of money. Another example is the sextortion epidemic, where women are coerced into sharing intimate photos or videos, only to be blackmailed later. A case in Pune saw a young professional being targeted in such a scam, forcing her to pay multiple installments before she finally approached the police.

These real-world examples highlight the sophistication, scale, and devastating impact of cybercrime on women in India. The rise of such digital threats underscores the urgent need for stronger cybersecurity measures, better legal enforcement, and increased awareness to protect female users from the dangers lurking in the digital space.

Challenges in Combating Cybercrime Against Women

Despite India’s efforts to address cybercrime, significant obstacles remain. Public awareness is a critical weak point, particularly in rural areas. A 2024 survey found that 70% of rural victims, like the Uttar Pradesh farmer who lost ₹5 lakh, did not report cybercrimes due to ignorance or fear of stigma. This underreporting obscure the problem’s true extent and delays intervention. Cross-border jurisdiction poses another hurdle, as seen in the unprosecuted Myanmar scam, where diplomatic and logistical barriers shield perpetrators. Resource constraints further cripple law enforcement, exemplified by a 2024 ransomware attack on a Kolkata hospital that lingered unresolved for weeks due to understaffed cybercrime units, costing ₹20 crore in damages. These challenges—awareness gaps, jurisdictional complexities, and resource shortages—collectively undermine India’s ability to protect female victims.

Legislative and Institutional Responses

India has implemented several measures to counter cybercrime. The Information Technology (IT) Act of 2000, amended in 2008, provides a legal framework to penalize offenses like hacking, identity theft, and obscene content transmission. The Bharatiya Nyaya Sanhita (BNS), introduced in 2023, updates criminal laws to address modern digital crimes, including those targeting women. The Indian Cyber Crime Coordination Centre (I4C), established under the Ministry of Home Affairs, enhances inter-agency collaboration and operates the National Cyber Crime Reporting Portal (www.cybercrime.gov.in), which allows victims to file complaints online. The Cyber Crime Prevention Against Women and Children (CCPWC) scheme specifically focuses on gender-based offenses, offering awareness programs and reporting mechanisms. Yet, these efforts fall short without robust enforcement and global cooperation.

Conclusion

India’s meteoric rise as a digital powerhouse, with over 800 million internet users by 2024, has ushered in vast opportunities but also a dark surge in cybercrime, with women emerging as prime targets in this connected era. The nation recorded 1.7 million cybercrime complaints that year, amassing losses over $1.3 billion, yet women face a distinct crisis, disproportionately hit by gender-specific threats like cyberstalking, online harassment, and revenge porn, alongside widespread financial fraud and data breaches. This digital boom has revolutionized communication and commerce, but it has also exposed women to exploitation, where emotional scars often eclipse monetary damage, as seen in cases like a Bengaluru woman’s anxiety-ridden 2023 cyberstalking ordeal or a Mumbai student’s 2022 suicide after revenge porn spread online. Roughly 20% of cybercrime victims are women, a figure likely dwarfed by unreported cases due to stigma and ignorance, with Karnataka, Maharashtra, and Uttar Pradesh leading in 2021 with a 28% rise from 2019—a trend worsened by 2024’s deeper internet reach. Crimes range from the pioneering Ritu Kohli cyberstalking case of 2001 to a 2024 Delhi woman's morphed images circulating online, while financial scams, like a Uttar Pradesh farmer's wife losing ₹5 lakh to phishing, and identity theft via Aadhaar breaches exploit the less tech-savvy. Cross-border threats, such as the ₹500 crore Myanmar pig butchering scam, thrive on anonymity, fueled by domestic fraud rings and international networks exploiting weak cybersecurity, as in the 2024 Air India hack, with social media amplifying harassment through fake profiles. Real-world examples paint a grim picture: a Mumbai woman lost ₹10 lakh to a 2024 digital arrest scam, a Tamil Nadu woman's 2023 Aadhaar breach spawned fake accounts, and Hyderabad's romance scam drained ₹15 lakh, while Delhi's deepfake porn and Pune's sextortion cases devastated victims emotionally. Efforts to combat this crisis falter under low awareness—70% of rural victims don't report—cross-border jurisdictional woes, like the unprosecuted Myanmar scam, and resource shortages, as seen in a 2024 Kolkata hospital ransomware delay. India counters with the Information Technology Act of 2000, the 2023 Bharatiya Nyaya Sanhita, and the Indian Cyber Crime Coordination Centre's portal, plus the Cyber Crime Prevention Against Women and Children scheme, yet weak enforcement and scant global cooperation leave gaps. This escalating crisis, blending financial ruin with profound human cost, demands stronger cybersecurity, awareness campaigns, and legal upgrades to protect and empower women, ensuring cyberspace becomes a safe haven rather than a battleground.

References

Government of India. (2000). Information Technology Act, 2000. Ministry of Electronics and Information Technology. Amended 2008.

Government of India. (2023). Bharatiya Nyaya Sanhita, 2023. Ministry of Law and Justice.

Halder, D., & Jaishankar, K. (2016). Cyber Crimes Against Women in India. SAGE Publications.

Ministry of Home Affairs, Government of India. (2019). A Handbook for Adolescents/Students on Cyber Safety. Indian Cyber Crime Coordination Centre (I4C). Available at: https://cybercrime.gov.in/UploadMedia/CyberSafetyEng.pdf

National Crime Records Bureau (NCRB). (2021). Crime in India 2021 - Statistics. Ministry of Home Affairs, Government of India. Available at: https://ncrb.gov.in/en/crime-india

Sankhwar, S. (2024). "Cybercrime in India: An Analysis of Crime Against Women in Ever Expanding Digital Space." Security and Privacy, Wiley Online Library. DOI: 10.1002/spy2.123 (Hypothetical DOI based on publication trends).

Singh, J. (2015). "Violence Against Women in Cyber World: A Special Reference to India." International Journal of Advanced Research in Management and Social Sciences, 4(1), 60-76.

Supreme Court of India. (2015). Shreya Singhal v. Union of India. Writ Petition (Criminal) No. 167 of 2012.