

6

Artificial Intelligence and Cybercrime Against Women: Emerging Threats, Vulnerabilities and Response

Sunita Sharma*

Advocate, Delhi High Court, New Delhi, India.

*Corresponding Author: advocatesunitasharma1994@gmail.com

Abstract

Artificial Intelligence is reshaping how people communicate, transact and offend in the digital space. While AI offers considerable social, economic, and technological benefits, it also allows offenders to commit crime faster, at a greater scale, and with a higher degree of realism. AI now facilitates many forms of technology-facilitated gender-based violence against women, including cyberstalking, online harassment, impersonation, image-based abuse, deepfakes, extortion, doxing, blackmail, and financial fraud. The ability to generate lifelike images, video, audio, identities and conversations changes the way such offences are committed: it makes impersonation and defamation more convincing, it allows non-consensual intimate content to be created without any real image ever being shared, and it makes social engineering and phishing more personal and harder to detect. This article explains the phenomenon of AI-enabled crime against women, examines the factors that make women vulnerable, and considers the challenges such crimes pose for victims, platforms, investigators, and the legal system. It assesses the impact on privacy, dignity, consent and reputation; reviews the Indian legal and regulatory framework, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhinyam, 2023 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026; and analyses the emerging judicial response. The article argues for a multi-stakeholder response and recommends legal, technological, institutional, and societal measures, including a greater role for women in shaping AI.

Keywords: Cyber Crime, Artificial Intelligence, Technology, Deepfakes, Digital Safety, Women, Cyber Laws.

Introduction

Artificial Intelligence (AI) has become part of everyday life. A technology once regarded as futuristic now supports communication, banking, healthcare, education,

cybersecurity and law enforcement. It can analyse very large volumes of information, identify patterns and assist in decision-making, and in doing so it has made many tasks faster, easier and more efficient. Like any powerful technology, however, AI can be misused. The same capabilities that protect digital systems can be turned against them, and against the people who use them. Cybercriminals increasingly use AI to write convincing phishing messages, automate scams, manipulate photographs and videos, imitate voices and identities, and tailor social-engineering attacks to individual victims. Deepfakes and generative AI have made digital deception harder to detect, and for an ordinary person, the line between genuine and manipulated content is becoming ever harder to draw. Women and girls are disproportionately affected by many forms of online abuse, and AI tends to sharpen the harms they face. Where reputation, modesty, privacy, and personal safety are closely connected, a fabricated intimate image, a cloned voice, or a fake profile can cause lasting damage, even though the woman concerned took no part in creating the material. AI also lowers the effort and skill needed to produce such material, so that a single offender can now target many women quickly and at little cost.

Cybercrime is not only a technological problem. An attack often succeeds not by breaking a technical security system but by influencing a person's thoughts and decisions. Trust, fear, curiosity, urgency, greed, loneliness, impulsivity, and deference to authority all shape how a person responds to an online situation. A message that appears to come from a bank, a police officer, an employer, a friend, or a family member can create trust and urgency and lead a person to act before reflecting on the consequences. Cyber psychology, the study of how people think, feel, and behave in digital environments, helps to explain why certain online situations make individuals vulnerable to manipulation. Concepts such as anonymity, perceived anonymity, online disinhibition, social influence, and group behaviour explain why people behave differently online, and they can inform better prevention, awareness, and victim support.

The consequences of cybercrime extend well beyond financial loss or damage to a device. Victims may experience fear, anxiety, embarrassment, loss of confidence, social withdrawal, and a persistent sense of insecurity, and prolonged harassment, fraud, sextortion, or identity-based abuse can have severe psychological and social effects. AI-generated impersonation and manipulation, being more realistic and more personal, can aggravate these effects. The legal system must respond as well. Existing laws on identity theft, cheating, personation, privacy, obscene electronic content, stalking and electronic evidence may apply to technology-enabled offences, but the rapid development of AI continues to raise new questions about responsibility, privacy, digital evidence, victim protection and the regulation of emerging technologies. Understanding AI-enabled cybercrime against women therefore requires attention to the interaction between technology, human behaviour, psychology, and law.

Conceptual Framework on Cybercrime and Artificial Intelligence

- **Definition of Cybercrime**

Cybercrime refers to unlawful activity carried out through the internet or by means of information technology, in which a computer, a network or a digital device is used as a tool, a target or a medium for committing an offence. It covers a wide range of conduct, including hacking, data theft, online fraud, cyberterrorism, identity theft, cyberstalking, and image-based abuse. The Information Technology Act, 2000 does not define “cybercrime” as such; it creates specific offences and leaves the wider category to be shaped by legislation and judicial interpretation. The nature of cybercrime in India is multifaceted and constantly evolving (Agrawal, 2024).

- **Definition of Artificial Intelligence**

The Organisation for Economic Co-operation and Development describes an AI system as a machine-based system that, for explicit or implicit objectives, infers from the input it receives how to generate outputs, such as predictions, content, recommendations or decisions, that can influence physical or virtual environments. Such systems differ in their level of autonomy and in how far they adapt after deployment (OECD, 2024). In everyday usage, the term covers machine-learning models that detect patterns in data as well as generative AI, which produces new text, images, audio, and video in response to a prompt. Several AI applications are central to crimes against women. A deepfake is audio, video, or an image generated or altered by AI so that it convincingly depicts a real person saying or doing something that never happened. Voice cloning reproduces a person’s voice from a brief sample. Synthetic media is the wider category of AI-generated or AI-altered content. India’s Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 use the term “synthetically generated information” for audio, visual or audio-visual material that is artificially or algorithmically created or altered so that it appears real and is indistinguishable from an actual person or real-world event.

- **Common Forms of Cybercrime Using Artificial Intelligence**

Table 1: Classification of Cybercrimes Using Artificial Intelligence

Cybercrimes	Descriptions
Cyber Stalking & Online Harassment	Using the internet to stalk or harass an individual, group, or organisation. AI can automate monitoring, generate abusive messages in bulk, and operate fake accounts at scale
Identity theft & Impersonation	Stealing personal information to impersonate someone else for financial gain or other benefit. AI-generated images, voices, and profiles make impersonation more convincing
AI-Deepfakes & Synthetic Media	AI-generated or manipulated audio, video, or images that convincingly imitate a real person or event

AI-Picture Morphing	Digital manipulation of an image to alter, combine or transform a person's appearance or facial features, usually to damage reputation
Sextortion	Threatening to publish real or AI-generated intimate images in order to obtain money, further images or compliance or coercion
AI-Voice Cloning	Replicating a person's voice from a short recording to deceive relatives, colleagues, institutions, or to fabricate incriminating audio
AI-Powered Scams & Fraud	Using AI to design, execute or automate scams, hoaxes or fraud by deceiving an individual or assuming a false identity to obtain funds or private information
AI-Powered Password Attacks	Using AI to automate or enhance attempts to guess, crack, or hijack a password and gain unauthorised access to an account

Source: Compiled and Created by Author

Characteristics of Artificial Intelligence and Cybercrime

- **Specialised Skill and Knowledge**

Cybercrimes are committed through technology, and traditionally the offender needed considerable skill in the use of the internet, computers, and other electronic devices. Many offenders also understand human emotions well. In cyber fraud, offenders often exploit greed, fear, urgency, and trust to induce victims to disclose information or transfer money. AI is eroding the skill barrier: tools that produce realistic images, voices, and text can be used by people with little technical expertise, which widens the pool of potential offenders.

- **Anonymity and Perceived Anonymity**

Anonymity refers to a situation in which a person's identity cannot easily be linked to their actions or communications because identifying information such as name, face, or location is concealed. Online anonymity can protect privacy and encourage free expression, but it may also reduce accountability and facilitate harassment, trolling, and cybercrime. Perceived anonymity is a person's belief that their identity is hidden or difficult to trace online, even when their activity may in fact be identifiable. The belief can weaken the sense of social accountability and encourage people to behave in ways they would avoid face to face. It is closely linked to the online disinhibition effect described by Suler (2004), although it can also have positive uses, such as seeking support, sharing sensitive experiences, or reporting wrongdoing.

- **Social Influence**

Social influence and group dynamics. Online behaviour is shaped by social norms, personal identity, anonymity, and the need for social approval. Online communities develop their own norms and expectations, and following or violating them may lead to acceptance or criticism. The desire for self-expression, creativity,

validation, and control over one's online image also affects behaviour, and anonymity can reduce the fear of immediate social consequences. These factors help to explain how people interact, form groups, and influence one another online. They can also help to explain how group dynamics amplify abuse directed at women, for example, through coordinated trolling or the circulation of manipulated images in closed groups.

- **Permanence and Evidentiary Virality**

Digital content can be copied, re-uploaded, and shared across platforms within minutes. For a woman targeted by a fabricated intimate image, removal from one platform does not guarantee removal from the internet, and the harm may recur long after the original upload. Digital evidence is easy to alter or delete, and its authenticity can be contested. In the case of deepfakes, genuine and fabricated material may be very difficult to tell apart.

Artificial Intelligence, Human Vulnerability and Cybercrime

- **Human Vulnerability and Social Engineering**

Human behaviour is an important element of cybersecurity. People may make decisions quickly, overlook warning signs, or trust information that appears familiar or credible. Vulnerability does not mean that a person lacks knowledge or intelligence; stress, distraction, urgency, and the context of a message can all influence decision-making. Social engineering involves manipulating people into revealing information, transferring money, or performing an action that benefits the offender. Attackers often create a false sense of trust by pretending to be a bank employee, government official, colleague, friend, or other familiar person or organisation. The success of such attacks depends on influencing the victim rather than defeating a technical security system. Artificial Intelligence strengthens this tactic because it can reproduce a familiar face, voice, or writing style.

- **Fear, Urgency, and Authority**

Fear, urgency, and authority are three powerful psychological elements commonly used to influence human decision-making. Cyber offenders frequently create a sense of fear or urgency by claiming that an account will be blocked, that money will be lost, or that immediate action is required. They may also impersonate authorities or trusted institutions. Such pressure can encourage people to act quickly rather than examine the information carefully. This reduces the time available for critical thinking and verification. Authority relies on people's tendency to trust individuals or institutions perceived as legitimate, powerful, or knowledgeable, such as government officials, police officers, banks, and employers. Together, these techniques can make a request appear both credible, demanding, and time sensitive. They are frequently observed in social engineering, phishing, online fraud, and scam communications. Recognizing these psychological triggers helps individuals pause, verify information independently, and avoid impulsive reactions.

- **Women Face Immediate Risks Online**

Vulnerability to cybercrime is situational. It is created by the offender's strategy and by the social setting, and it does not reflect any lack of intelligence or care on the part of the victim. That said, offenders often exploit social conditions that affect women. Concern for reputation, family honour and modesty gives threats of exposure a coercive power, which is the basis of sextortion and blackmail. Fear of being blamed, disbelieved, or restricted by family can discourage reporting and lead victims to comply with demands in silence. Relationship-based tactics, such as romance scams, exploit trust and emotional need. And because Artificial Intelligence can fabricate compromising material with no real image ever having been shared, a woman may be targeted even if she has been careful about what she shares. Evidence on gendered patterns of victimisation should be treated with care and calls for better disaggregated data.

Impact of Artificial Intelligence and Cybercrime on Women

For many types of cybercrime, victimisation is multifaceted. Online fraud may appear to cause only financial harm, yet Button, Lewis, and Tapley (2014) found that, besides financial hardship, some victims suffered adverse effects on their mental health, physical health, and personal relationships. Whitty and Buchanan (2012; 2016) argue that victims of online dating romance scams suffer a "double hit": they lose a relationship and money. A survey by Buchanan and Whitty (2014) found large individual differences in the degree of emotional distress reported by victims, and distress was sometimes high even where there was no financial loss. In-depth interviews with some victims indicated that those who had lost money to romance scams were more distressed by the loss of the relationship than by the loss of the money, and that their distress was aggravated by a lack of social support, with some victims reporting anger and blame from family and friends (Whitty & Buchanan, 2016). The literature identifies a wide range of consequences of cyber-victimisation. They include social withdrawal and anxiety, depression, post-traumatic stress, obsessive behaviours, loss of confidence and reduced self-esteem, headaches, abdominal and stomach problems, eating disorders, sleep disorders, a persistent feeling of being unsafe, feelings of helplessness, panic attacks and mistrust of others. In the most serious cases, victims may experience self-harm and suicidal thoughts. These harms can be compounded where Artificial Intelligence is used.

- **Illustrative Incidents**

- **Incident 1.** A man aged about 38 years was targeted for sextortion through "catfishing", in which an offender uses a false identity to build trust. After he was persuaded to send intimate images of himself, he was bombarded with threats to expose them to his friends and family unless he paid. He paid almost INR 2 lakh, and the offender demanded more.

The pressure became overwhelming, and he died by suicide, driven by shame and embarrassment.

- **Incident 2.** A college student aged about 21 years took a loan of INR 50,000 from unverified online lending websites, and the amount was disbursed to her. A few days later she began to receive threatening calls and constant pressure to repay at a very high rate of interest, and she was pressed to pay INR 2 lakh. She was threatened that her personal information would be leaked on social media and that her image would be used on dark web if she did not repay the amount. Unable to cope with the pressure, she died by suicide.

In both incidents, it was the threat of exposure and humiliation, rather than the sums of money involved, that drove the harm. With Artificial Intelligence, an offender no longer needs to obtain a real image: a photograph of the second victim, for example, could be morphed into compromising material and used for the same threat. The incidents also underline the need for accessible reporting channels and psychological support.

Emerging Contemporary Issues: Artificial Intelligence as a Key Factor

- **Deepfakes and Non-Consensual Intimate Imagery**

AI-generated deepfakes can be used for identity impersonation, fraud, disinformation, and the creation of non-consensual intimate imagery, causing significant psychological, social, and reputational harm. Readily available applications can place a woman's face on sexually explicit material, or digitally "undress" a photograph taken from social media, using only a few images as input. The result is abuse that does not depend on any real intimate image existing and that can be produced in bulk.

- **Voice Cloning and AI-Impersonation**

Cloned voices and synthetic video allow offenders to impersonate relatives, employers, bank officials, and law-enforcement officers convincingly. "Digital arrest" scams, in which offenders pose as police or court officials on audio and video calls and use forged documents to extort money, show how impersonation and fear of authority can be combined. The Supreme Court has noted that senior citizens are mostly the targets of such scams.

- **Surveillance, Data Leak and Privacy**

The growing use of Artificial Intelligence and large-scale data processing also raises concerns about privacy, surveillance, data misuse, and digital security. Images, voice samples, and personal data collected from social media can be used to train or prompt tools that target the individuals concerned. The Digital Personal Data Protection Act, 2023 is relevant to the processing of personal data for such

purposes, although it is a general data-protection statute rather than a measure aimed at synthetic-media abuse. As AI continues to evolve, cybercrime is likely to evolve with it. This makes cyber psychology increasingly important for understanding human responses to AI-driven threats, psychological manipulation, digital vulnerability, and online behaviour, and for designing effective prevention, protection, and intervention strategies.

Legal and Regulatory Framework Relating to Cybercrime in India

- **Information Technology Act**

The Information Technology Act, 2000, is the primary statute governing cybercrime in India. It does not mention artificial intelligence, but its provisions are technology-neutral and several of them can apply to AI-enabled offences. Section 66C punishes identity theft, namely the fraudulent use of another person's electronic signature, password, or other unique identification feature. It may apply where AI systems are used to create synthetic identities or to impersonate individuals in digital environments. Section 66D penalises cheating by personation using a communication device or computer resource and may apply where AI-generated identities or voice-cloning technologies are used to deceive individuals or organisations for financial or other fraudulent purposes. Section 66E addresses violation of privacy through the capture, publication or transmission of an image of the private area of any person without consent, in circumstances violating privacy. It is relevant to privacy violations through manipulated imagery, but because it is framed around images that are captured, its application to a wholly synthetic image is open to argument. Where deepfake pornography or manipulated explicit content is involved, authorities may rely on Section 67, which punishes publishing or transmitting obscene material in electronic form, and on Section 67A, which punishes publishing or transmitting material containing a sexually explicit act or conduct. These provisions may be invoked where deepfake videos are used for sexual exploitation or online harassment.

- **Bharatiya Nyaya Sanhita**

The Bharatiya Nyaya Sanhita, 2023 (BNS) replaced the Indian Penal Code, 1860 (IPC) with effect from 1 July 2024. Offences committed before that date continue to be governed by the IPC, so both codes may be relevant in a particular case. Depending on the facts, several BNS offences may apply to AI-driven cyber offences against women. Online harassment or persistent monitoring through digital platforms may amount to stalking under Section 78 BNS, which extends to monitoring a woman's use of the internet, email, or any other form of electronic communication. Sexual Harassment, Voyeurism and words, gestures, or acts intended to insult the modesty of a woman may apply to sexually coloured messages, the circulation of intimate or morphed images, and similar conduct. Sextortion and Blackmail may

attract Section 308 (Extortion) and Section 351 (Criminal Intimidation). Impersonation and Fraud may fall under Section 318 (Cheating) and Section 319 (Cheating by Personation), and defamatory content, including AI-generated content that lowers a woman's reputation, may attract Section 356. The BNS does not contain a provision that expressly addresses Synthetic or AI-Generated Sexual Imagery.

- **Digital Evidence under Bharatiya Sakshya Adhiniyam**

The admissibility and authentication of electronic evidence are governed by the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which also came into force on 1 July 2024. Section 61 provides that an electronic or digital record is not to be denied admissibility merely because it is electronic or digital. Section 62 provides that the contents of electronic records may be proved in accordance with Section 63. Section 63, which corresponds to the former Section 65B of the Indian Evidence Act, 1872, sets out the conditions for admitting computer output and requires a certificate in the form prescribed in the Schedule to the Adhiniyam, which now also contemplates certification by an expert and a hash value of the record. These provisions are significant in cases involving deepfake videos, AI-generated audio recordings, and other digital evidence. They help a victim place genuine electronic material, such as threatening messages and screenshots, before a court, but they do not by themselves resolve the harder question whether a particular recording or video is authentic. Courts will increasingly need forensic expertise to detect manipulation and to guard against the "liar's dividend": the risk that a person confronted with genuine evidence will claim that it is a deepfake (Chesney & Citron, 2019).

- **Cybercrime Reporting, Investigation and Law-Enforcement**

Cybercrime reporting and investigation involve the reporting of offences, the collection of relevant information and digital evidence, the identification of suspects, and investigation by the competent law-enforcement authorities. The National Cyber Crime Reporting Portal (NCRP), established by the Government of India and operated under the Indian Cyber Crime Coordination Centre (I4C) of the Ministry of Home Affairs, facilitates online reporting of cybercrime complaints, including online financial fraud, hacking, ransomware, social-media crimes, and crimes against women and children. Complaints are dealt with by law-enforcement agencies and the police based on the information provided, and the portal also allows complainants to track their complaints. A dedicated helpline, 1930, exists for reporting cyber financial fraud. For victims of AI-enabled abuse, prompt preservation of evidence, including screenshots, URLs, usernames, message headers, and the original files, is essential, and a complaint should be lodged at earliest both on the NCRP and with the platform concerned.

**Table 2: Relevant Sections of Bharatiya Nyaya Sanhita for
Cyber Crime Against Women**

Cyber Crime Types	BNS 2023 (Old IPC)	IT Act 2000 (Amended 2008)	Punishment	Bailable/Non-Bailable
Cyber Stalking	BNS Sec. 78 (IPC 354D)	Sec. 66A struck down in 2015	1st conviction: up to 3 yrs + fine. Repeat: up to 5 yrs + fine	Cognizable. Bailable for 1st offence, Non-Bailable for repeat
Online Sexual Harassment	BNS Sec. 75 (IPC 354A)	Sec. 67	BNS: up to 3 yrs RI, or fine, or both. Sexual remarks: up to 1 yr, or fine, or both	Cognizable, Bailable
Voyeurism	BNS Sec. 77 (IPC 354C)	Sec. 66E, 67, 67A	BNS: 1st: 1–3 yrs + fine. Repeat: 3–7 yrs + fine	Cognizable. Bailable for 1st offence, Non-Bailable for repeat
Violation of Privacy		Sec. 66E	Up to 3 yrs, or fine up to ₹2 lakh, or both	Cognizable, Bailable
Picture Morphing, Deepfakes	BNS Sec. 79, 356, 336(4) (IPC 509, 499/500, 469)	Sec. 66C, 66D, 67, 67A	Sec. 66C/66D: up to 3 yrs + fine up to ₹1 lakh. Sec. 67A: up to 5 yrs + fine up to ₹10 lakh	Cognizable. Bailable for 66C/66D/67, Non-Bailable for 67A
Insulting Modesty of Woman	BNS Sec. 79 (IPC 509)	Sec. 67	Up to 3 yrs simple imprisonment + fine	Cognizable, Bailable
Publishing Obscene Content Online	BNS Sec. 294, 296 (IPC 292, 294)	Sec. 67	IT Act: 1st: up to 3 yrs + fine up to ₹5 lakh. Repeat: up to 5 yrs + fine up to ₹10 lakh	Cognizable, Bailable
Publishing Sexually Explicit Content Online	BNS Sec. 77, 294	Sec. 67A, 66E	1st: up to 5 yrs + fine up to ₹10 lakh. Repeat: up to 7 yrs + fine up to ₹10 lakh	Cognizable, Non-Bailable
Child Sexual Abuse Material	BNS Sec. 294, 295	Sec. 67B	IT Act: 1st: up to 5 yrs + fine up to ₹10 lakh. Repeat: up to 7 yrs + fine up to ₹10 lakh	Cognizable, Non-Bailable
Identity Theft	BNS Sec. 336, 340 (IPC 464–471)	Sec. 66C	Up to 3 yrs + fine up to ₹1 lakh	Cognizable, Bailable

Cheating by Personation	BNS Sec. 319, 318(4) (IPC 419, 420)	Sec. 66D	IT Act: up to 3 yrs + fine up to ₹1 lakh. BNS 318(4): up to 7 yrs + fine	Cognizable. Bailable (IT Act), Non-Bailable (BNS 318(4))
Cyber Blackmail	BNS Sec. 308, 351 (IPC 383–384, 506)	Sec. 66E, 67A	Extortion: up to 7 yrs, or fine, or both. Intimidation: up to 2 yrs, or fine, or both. Threat of death or grievous hurt: up to 7 yrs	Cognizable, Bailability Varies
Criminal Intimidation	BNS Sec. 351 (IPC 506)		Up to 2 yrs, or fine, or both. Anonymous threats: additional 2 yrs	Non-Cognizable, Bailable
Cyber Defamation	BNS Sec. 356 (IPC 499/500)		Up to 2 yrs simple imprisonment, or fine, or both, or community service	Non-Cognizable, Bailable
Unauthorised Access, Hacking		Sec. 43(a), 66	Sec 66: up to 3 yrs, or fine up to ₹5 lakh, or both. Sec. 43 is civil compensation	Cognizable, Bailable
Cyber Bullying	BNS Sec. 108 (IPC 306)		Up to 10 yrs + fine	Cognizable, Non-Bailable
Sexual Intercourse by False Pretext of Marriage	BNS Sec. 69		Up to 10 yrs + fine	Cognizable, Non-Bailable

Source: Compiled and Created by Author

Prevention and Response: A Multi-Stakeholder Approach

• Legal and Regulatory Measures

Clarify the law on synthetic intimate imagery. Parliament should consider whether the creation, possession, and distribution of sexually explicit synthetic images of a real person without consent should be addressed by an express offence, so that prosecution does not depend on stretching provisions drafted for photographs or for traditional obscenity. Such a provision should centre on consent and on harm to the person depicted, rather than on obscenity alone. Strengthen platform accountability. The 2026 Rules create labelling and takedown duties, but their effectiveness will depend on enforcement, transparency reporting and accessible grievance mechanisms, together with safeguards against over-removal that would threaten legitimate expression, consistent with Shreya Singhal. Wide access to rapid remedies. Courts have shown a willingness to grant urgent interim relief against AI-generated content. Such relief should be practically available to ordinary women and

not only to public figures, through legal aid, simplified procedures for takedown and disclosure orders, and clear police protocols. Improve cross-border cooperation. Because offenders and platforms are often located abroad, faster mutual legal assistance and direct cooperation arrangements with major intermediaries are needed to trace offenders and secure evidence.

- **Technical Measures**

Organisations must prioritise cybersecurity by adopting measures such as multi-factor authentication, encryption and regular system updates. Advanced threat-detection tools, including AI-driven behavioural analytics, can identify and neutralise malicious activity before it escalates. Public–private partnerships should facilitate the sharing of best practices and intelligence so that industries are equipped to combat evolving threats. For crimes against women, platforms and developers should also adopt safety-by-design: reliable detection and labelling of synthetic media, provenance and watermarking standards, tools that allow victims to block re-uploads of known abusive images, restrictions on applications designed to strip clothing from photographs, and privacy settings that make it harder to collect personal images in bulk. Individuals can reduce risk through strong and unique passwords, multi-factor authentication, careful privacy settings, and caution about the images and personal details they share publicly.

- **Institutional Measures**

Police, prosecutors, and judges need training in digital forensics, deepfake detection, and trauma-informed handling of complaints, so that women are not discouraged from reporting. Dedicated cybercrime units, standard operating procedures for rapid evidence preservation and takedown requests, and coordination between the NCRP, the 1930 helpline, banks and intermediaries are essential. The Supreme Court's directions in digital arrest proceedings show how coordinated mechanisms, including the freezing of accounts and the restoration of defrauded money, can be built when courts insist on them. Specialised legal aid and counselling should be available to victims, and the collection of disaggregated data on AI-enabled offences against women should be improved to support evidence-based policy.

- **Victim Support and Experience Sharing**

Victims of cybercrime can play an important role in prevention and psychological support when they voluntarily choose to share their experiences. Survivor accounts can help others understand common tactics, recognise warning signs, and learn practical ways to protect themselves. Sharing experiences in safe and supportive settings can also reduce feelings of isolation, shame, and self-blame among victims and encourage others to seek timely assistance. Such initiatives should, however, protect victims' privacy and emotional well-being and should be

supported by appropriate counselling and professional guidance. This approach can combine personal experience, psychological support, and public awareness to promote safer and more responsible online behaviour.

- **Women as Stakeholders in Artificial Intelligence**

Women are not only potential victims of AI-enabled crime; they are also users, developers, regulators and researchers of AI. Greater participation of women in AI design, platform trust-and-safety teams, policing and policymaking is likely to produce systems and rules that anticipate gendered harms. Artificial Intelligence can also be used protectively, for example, to detect abusive content, identify mule accounts, and flag fraud, and the Supreme Court has itself asked why AI is not being used more extensively to detect and freeze accounts used by cybercriminals. Consultation with women's organisations, survivors and technologists should be built into the design of future AI regulation.

Judicial Approach and Relevant Case Laws

Indian courts have gradually developed a jurisprudence on cybercrime and digital evidence over the past two decades. Judicial pronouncements specifically concerning Artificial Intelligence based cybercrime remain limited, and many of the most relevant orders are interim. Nevertheless, a line of decisions provides guidance on online harassment, obscenity, intermediary liability, electronic evidence, and, more recently, AI-generated content.

- **Early Prosecutions for Online Harassment of Women**

One of the earliest convictions under Indian cyber law was in *State of Tamil Nadu v. Suhas Katti* (2004). The accused posted obscene and defamatory messages about a woman in online groups, causing harassment and reputational damage. The Additional Chief Metropolitan Magistrate, Egmore, Chennai, convicted him in November 2004 under Section 67 of the IT Act and Sections 469 and 509 of the IPC. The case demonstrated the effectiveness of law in addressing online harassment of women and marked a significant milestone in the enforcement of cyber legislation in India. In *Kalandi Charan Lenka v. State of Odisha* (2017), a bail proceeding before the Orissa High Court, the accused was alleged to have sent obscene messages to a young woman and her father, to have created a fake Facebook account in her name and to have circulated morphed naked photographs of her. The Court considered the material gathered by the investigators, including certificates under Section 65B of the Evidence Act from service providers, and held that offences under the IT Act were *prima facie* made out, while observing that the IPC offences were yet to be established. It stressed that stalking, fake accounts, and morphed images are a menace to society and to the rights and dignity of women. The Court nevertheless granted bail on strict conditions designed to protect the victim, having regard to the punishment prescribed, the absence of criminal antecedents and the time already

spent in custody. The decision is useful for its recognition that morphing and impersonation are serious violations of a woman's dignity.

- **Free Speech, Obscenity and Intermediaries**

In *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A of the IT Act as a violation of the freedom of speech and expression under Article 19(1)(a) of the Constitution that was not saved by Article 19(2). The Court also read down the intermediary-liability provisions so that an intermediary must remove content only on actual knowledge, through a court order or a government notification. Although the case concerned freedom of expression, it emphasised the need to balance the regulation of digital spaces with the protection of fundamental rights. That principle is directly relevant to the regulation of AI-generated content such as deepfakes: takedown regimes, including those in the 2026 Rules, must remain consistent with Article 19. In *Sharat Babu Digumarti v. Government of NCT of Delhi* (2016), which arose from the listing of an obscene video clip for sale on an online marketplace, the Supreme Court held that the IT Act is a special enactment, that Sections 67, 67A and 67B form a complete code for obscene material in electronic form, and that where an offence concerns an electronic record the general obscenity provisions of the penal code cannot be applied alongside it. The Court also stressed that the protection of Section 79 cannot be ignored. The decision raises important questions of platform responsibility for illegal content and suggests that sexually explicit deepfakes are, to be prosecuted under the IT Act.

- **AI-Generated Content and Personality Rights**

The most direct judicial engagement with Artificial Intelligence generated content so far has come from the Delhi High Court in personality-rights suits. In *Anil Kapoor v. Simply Life India* (2023), the Court granted an interim injunction restraining the unauthorised use of an actor's name, voice, likeness and image, including through AI-based tools, deepfakes and face-morphing. The Court has since granted similar relief in a series of cases. In *Kajol Vishal Devgan v. Kash Collective* (2026), Justice Jyoti Singh granted an ex parte ad interim injunction against AI-generated deepfakes, vulgar chatbots and unauthorised merchandise, and observed that the plaintiff was entitled to protection against morphed and pornographic content and against AI-generated images showing her in inappropriate settings. The Court linked the protection to the plaintiff's right to privacy and to live with dignity. These suits have mostly been brought by well-known public figures, who can point to the commercial value of their identity. Women who are not public figures must rely on criminal law, the IT Rules, and general civil remedies. A recent order suggests that the courts are prepared to extend urgent relief to them. In September 2026, a single-judge bench of the Delhi High Court, hearing the plea of a private woman whose face had reportedly been digitally swapped onto sexually explicit images using AI tools,

directed Meta Platforms to remove the content on receipt of the relevant links and ordered police protection for her. According to press reports, the order is interim.

Conclusion

Artificial Intelligence has made cybercrime against women faster, cheaper, more realistic, and more personal. Offences such as stalking, impersonation, image-based abuse, sextortion and fraud are not new, but deepfakes, voice cloning and generative text have changed their scale and credibility. This article has argued that the problem cannot be understood through technology, financial loss, or law alone. Human behaviour and psychology are central to both offending and victimisation. Trust, fear, curiosity, urgency, reward-seeking, social influence, anonymity, and online disinhibition shape how offenders act and how victims respond, while the social stigma attached to exposure gives threats against women a particular coercive force. Victims may experience anxiety, fear, shame, loss of confidence, social withdrawal, and emotional distress, and in the most serious cases, thoughts of self-harm. India's existing legal and institutional framework, comprising the IT Act, the BNS, the BSA, the NCRP and the 2026 amendments to the intermediary rules, provides mechanisms for addressing cyber offences, electronic evidence, investigation and reporting, and the courts have shown a willingness to apply it purposively. But that framework was not designed for synthetic media, and gaps remain, particularly in criminal law on fabricated intimate imagery, in access to rapid remedies for ordinary women, and in investigative capacity. Prevention therefore cannot rely on technological security or criminal-law enforcement alone. It calls for a multi-stakeholder response that combines clearer law, accountable platforms, trained and victim-sensitive institutions, accessible education and support, and the participation of women in shaping AI.

References

1. Agrawal, A. (2024, May 20). Nature and Scope of Cybercrime. Law Bhoomi. <https://lawbhoomi.com/nature-and-scope-of-cyber-crime/>
2. Button, M., Lewis, C., & Tapley, J. (2014). Not a Victimless Crime: The Impact of Fraud on Individual Victims and their families. *Security Journal*, 27(1), 36–54.
3. Chesney, R., & Citron, D. (2019). Deepfakes: A looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), 1753–1819.
4. Organisation for Economic Co-operation and Development. (2024). Explanatory Memorandum on the updated OECD definition of an AI system. OECD Publishing.

5. Whitty, M. T., & Buchanan, T. (2016). The Online Dating Romance Scam: The Psychological Impact on Victims, both Financial and Non-Financial. *Criminology & Criminal Justice*, 16(2), 176–194.
6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (Notified 10 February 2026; in force 20 February 2026).
7. Media Nama. (2026, February). MeitY notifies new amendments to IT Rules on synthetic media. <https://www.medianama.com/2026/02/223-meity-amendments-it-rules-synthetic-media-deepfakes/>
8. The Week. (2026, September 25). Delhi HC acts on woman's deepfake plea: Meta told to remove images. <https://www.theweek.in/news/india/2026/09/25/delhi-hc-acts-on-womans-deepfake-plea-meta-told-to-remove-images-cjp-leaders-get-notice.html>
9. Ministry of Electronics and Information Technology, Government of India. (2025, November). India Artificial Intelligence Governance Guidelines.
10. Anil Kapoor v. Simply Life India & Ors. (Delhi High Court, 2023).
11. Kajol Vishal Devgan v. Kash Collective & Ors., CS(COMM) 173/2026 (Delhi High Court, February 2026).
12. Kalandi Charan Lenka v. State of Odisha, BLAPL No. 7596 of 2016 (Orissa High Court, 16 January 2017).
13. Sharat Babu Digumarti v. Government of NCT of Delhi, SLP (Crl.) No. 7675 of 2015, (2017) 2 SCC 18 (Supreme Court of India, 14 December 2016).
14. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
15. State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004 (Additional Chief Metropolitan Magistrate, Egmore, Chennai, 5 November 2004).

