International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Artificial Intelligence and Cyber Crime: Legal Issues in India Treading Through the Delicate Legal System in the Age of Intelligent Technologies

Suchitra Narayan Machha

https://doi.org/10.55041/ijsmt.v2i5.373
Cite this Article: Machha, S. N. (2026). Artificial Intelligence and Cyber Crime: Legal Issues in India Treading Through the Delicate Legal System in the Age of Intelligent Technologies. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.373

ABSTRACT

The advent of Artificial Intelligence in digital transactions on a day-to-day basis has brought about tremendous change in how cybercrimes are committed. In India, which ranks among the topmost countries for the most number of internet users around the world, there is an urgent concern because the existing legal system – especially the Information Technology Act, 2000 – was formulated before the advent of Artificial Intelligence, making it impossible to deal with AI-based cybercrimes.

Keywords: *Artificial Intelligence, Cybercrime, IT Act 2000, Deepfakes, Digital India Act, Legal Framework, AI Liability, Ransomware, Phishing*

Introduction

The current century has seen a novel combination of technology and crime. Artificial Intelligence (AI), which was once confined to academia, has facilitated the creation of technologies that can create fake media content, imitate human behavior, conduct automated phishing attacks, and break the most complicated types of encryptions. This has become a grave existential threat to law enforcement agencies worldwide.

India is not different either. With over 900 million internet users, rising digital transactions through UPI, and a populace that increasingly relies on mobile phones for communication, the country provides criminals using AI a massive attack surface area. According to the National Crime Records Bureau (NCRB), India has seen a considerable increase in cases of cybercrimes registered yearly; however, the conviction rate has been extremely low because the laws could not keep pace with technology.

↑ **24%**	< **3%**
Annual rise in cybercrime cases (NCRB)	Cybercrime conviction rate in India

2. AI as a Tool for Cybercrime

The employment of artificial intelligence technologies by cybercriminals helps them improve their abilities in various respects. It is important to know how cybercrimes can be conducted using artificial intelligence to draft proper legislation.

2.1 Deepfakes and Artificial Intelligence Generated Media

Deepfakes are defined as the capacity of AI models to produce video and audio content impersonating real people. In India, deepfakes have been used to generate non-consensual intimate videos of women, speeches of political leaders that

do not belong to them, and conduct financial scams. The 2023 case involving an Indian actress whose video was published on social networks initiated a debate about deepfake legislation. The existing law does not solve the problem effectively.

2.2 Phishing and Social Engineering via AI

Language models help cybercriminals perform personalized phishing through emails and voice cloning attacks (vishing). It is possible to clone the voice of a bank officer, government official, or even a relative with surprising ease. Such scams are more affordable and scalable than regular ones.

2.3 Autonomous Malware and Ransomware

AI-driven malware can easily adapt its behavior in order to bypass any detection techniques, exploit vulnerabilities, and even negotiate with the victims of ransomware attacks. The critical infrastructure of India, which includes the electrical grid, healthcare facilities, and banking sector, is becoming more susceptible to such attacks, as evident from the AIIMS Delhi ransomware attack in 2022.

2.4 Financial Fraud Using AI

Automated bots powered by machine learning algorithms can be used to manipulate the stock market, defraud insurance companies, commit identity fraud, and abuse the UPI system. In most cases, it is quite challenging to detect AI-powered financial fraud, mainly because this complicates the process of gathering the necessary evidence.

3. The Existing Legal Framework in India

Some of the important laws in India that deal with cybercrimes include the Information Technology Act, 2000 (amended in 2008), and some provisions of the Bharatiya Nyaya Sanhita, 2023. They form the basis of cyber law in India.

Section 66C – Identity Theft: Criminalizes the fraudulent use of electronic signatures, passwords, or any other unique identification feature. It is inadequate in cases of AI-enabled synthetic identity theft.

Section 66E – Privacy Violation: Guarantees privacy from unauthorized publication of personal photos, but predated deepfake technology and does not address issues related to synthetic media.

Section 43 & 66 – Hacking/Alteration of Data: The important sections of hacking are inadequate in covering instances where an AI tool commits such actions without human interaction.

Section 67A/B – Pornography: Addresses sexual content but does not address any aspect of AI-generated and distributed content through algorithms.

BNS Section 318 – Cheating: Sections addressing fraud but inadequate in terms of technological aspects of AI-enabled financial crimes.

4. Critical Legal Challenges

A combination of AI-enabled cybercrimes and India's legal apparatus presents several inherent weaknesses that urgently require fixing.

4.1 Attribution Problem

For the prosecution to pursue a criminal case under Indian law, it must demonstrate the presence of mens rea – the intention to commit the crime. Where the perpetrator is not a human being but an autonomous AI system, it becomes quite hard to pin down who committed the crime: the programmer, the deployer, or the user of the AI? There is no precedent in Indian law regarding the vicarious liability of AI.

4.2 Lack of Legislation for Deepfakes

Even though the international community recognizes the negative impact of synthetic media on society, India does not have a special law that regulates the use of deepfakes. The MeitY released a guideline in 2023 advising internet platforms

against uploading misleading information generated using AI technology. However, guidelines do not carry any legal sanction.

4.3 Complexity of Jurisdiction

Many times, cybercrime cases have server locations outside the jurisdiction of the country in which the crime was committed. AI-based cybercrime can use multi-hop routing to mask their identity. Extradition laws of India are very narrow, and the process of exchanging evidences using MLAT is very complex.

4.4 Problem with Evidences

According to the Indian Evidence Act of 2023, electronic documents can be used as evidences, but there is no standard way to deal with evidences generated through AI. For example, a deepfake video or voice created through AI can be used as evidence, but authentication will be difficult.

4.5 Insufficient Capacity

AI-based cybercrime investigation needs exceptional knowledge of machine learning, computer forensics, and reverse engineering. This capacity does not exist in the police force and prosecution system in India. As a result, there is a huge gap between reported cybercrimes and convictions.

5. International Comparisons

Comparatively speaking, it is clear that India is much behind other similarly placed jurisdictions when it comes to the formulation of laws dealing with AI-related cybercrime. While the European Union's AI Act of 2024 provides a risk-based hierarchical approach to regulation that includes a provision relating to high-risk uses of AI, including criminal use cases, the United States has enacted some state-level laws on deepfakes and is working on national legislation for accountability in relation to applications of AI. In the case of the United Kingdom, its 2023 Online Safety Act makes it a crime to publish deepfake intimate images without consent.

These examples have lessons for us – though not all of them can be applied to our particular situation.

6. Recommendations

1. Pass the Digital India Act Immediately: The new act should include a chapter devoted to crimes enabled by AI with definitions of synthetic media, autonomous cyber agents, and AI-enabled fraud.

2. Create Deepfake-Specific Legal Framework: Criminalize the creation and dissemination of non-consensual synthetic intimate images; mandate detection and labeling of AI-generated content at the platform level.

3. Create an AI Liability Model: Establish liability of developers, deployers, and users of AI technologies with a graduated liability system based on foreseeability of damage.

4. Enhance Digital Forensic Capability: Set up AI forensics units within state CID and CBI; launch a national certification program for AI crime investigators.

5. Revise Evidentiary Standards: Amend the Bharatiya Sakshya Adhiniyam to cover AI-generated evidence standards; grant the court authority to appoint independent experts on technology issues.

6. Bilateral and Multilateral Efforts: Sign updated MLAT agreements with jurisdictions hosting prominent AI hubs; participate actively in INTERPOL's working groups on AI crime and UN cybercrime treaty talks.

7. Conclusion

It would be incorrect to term Artificial Intelligence as a tool in the commission of cybercrimes; it has completely transformed the character of crime in cyberspace. India stands at a crucial juncture where continuation with an outdated legal system would not only fail to offer any solution to the victims but will cast a shadow on the credibility of technology essential for India's growth.

An innovative legal system is not just a matter of national security but also of social justice. The law needs to evolve along with the evolving technology and not remain decades behind the latter. It is now the time when legislators, technocrats, jurists, and civil society should come together to design a legal framework suitable for the changing times.