SUPREMO AMICUS

VOLUME 38 | August, 2025 ISSN 2456-9704

CYBER CRIME IN INDIA WITH SPECIAL REFERENCE TO ARTIFICIAL INTELLIGENCE : A LEGAL STUDY

By *Rachna Bilgaiya*
Ph.D. from Bundelkhand University, Jhansi

Abstract

This paper explores the interactive dynamic between Artificial Intelligence (AI) and the Indian cyber-crime landscape. It critically analyses AI's double-edged role—as a force amplifier for cybercriminals utilizing deepfakes, AI-based phishing, and impersonation scams—and as a law enforcement force multiplier using technologies like predictive policing and deep fake detection. The research assesses the effectiveness of India's current legal framework consisting of the IT Act, Bharatiya Nyaya Sanhita, and DPDP Act in combating AI-based threats based on early landmark cases such as the Tinsukia morphed-image deepfake fraud and AI-based electoral disinformation. It further examines enforcement deadlocks like slim forensic capabilities, jurisdictional complexities, and privacy issues. Lastly, the study suggests specific reforms in legal, technology, and institutional areas—e.g., definitions of AI-specific offenses, improving digital forensic facilities, AI governance mechanisms, and protection of privacy—to guarantee that innovation and civil liberties go hand-in-hand.

Keywords: Deepfakes, Artificial Intelligence, Information Technology Act, 2000, Digital Personal Data Protection ACT, 2023, Phishing, MARVEL

1. Introduction

Over the past few years, India's digital revolution has been characterized by unprecedented growth—fueled by increasing internet penetration, mobile coverage, and digital payments. But the rise in digital activity has been paralleled by equally advanced cyber threats. The driving force behind this transformation has been Artificial Intelligence (AI), which has empowered both bad actors and law enforcement agencies.

On the one hand, AI technologies have taken cybercrime to new levels:

- **Deepfakes**, artificial images and videos created by AI—have been employed in cases of sexual extortion, defamation, and impersonation. In the case of Tinsukia in Assam, a man employed AI software to create pornographic images involving a former classmate, sharing them through subscription websites and earning ₹10 lakh in the process. The offense invoked several counts of the Bharatiya Nyaya Sanhita (BNS) law including cyber bullying and privacy invasion.
- **Digital arrest scams**, a newer phenomenon, involve perpetrators masquerading as law enforcers through video calls or messages, threatening citizens with arrest for non-existent crimes. Investigators discovered organized "scam farms" in Cambodia, hiring agents from all over India to carry out such schemes—cheating victims of more than ₹2,140 crore in 2023 alone.
- **AI-spawned disinformation spiked during elections**. Viral deepfakes—showing public personalities dancing or late political stalwarts supporting candidates—led to judicial orders and Election Commission advisories.

On the other hand, AI is becoming a force multiplier for public safety:

- The MARVEL system, implemented by Maharashtra Police in 2024 at a budget of ₹23 crore, employs AI for predictive policing and speedy criminal tracking.
- Software such as Vastav.AI, introduced in 2025, offers real time deepfake detection with about 99% accuracy—hence a key frontier in law enforcement tech.

2. Legal Framework Regulating Cyber Crimes

2.1 Information Technology Act, 2000 (IT Act) and Amendments

The IT Act, 2000 is still the bedrock of India's cybercrime legislation. Applicable provisions that can be used for AI-enabled crimes are:

- Section 66E: Capturing or transmitting private images without authorization—liable to up to three years' imprisonment or ₹2 lakh fine.
- Section 66C: Impersonation through electronic means—liable to up to three years' imprisonment and/or ₹1 lakh fine Section 66D deals with cheating through impersonation.
- Sections 67, 67A, and 67B: Focus on address distribution of obscene or explicit material, with increasing punishment for explicit or child-related material.
- IT Rules 2021: Mandate removal of impersonating or AI-altered content by intermediaries on notice; in default "safe haven" protection is forfeited.

2.2 Bharatiya Nyaya Sanhita (BNS), 2023 & Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023

BNS increases the ambit of law with crimes including:

- **Section 356**: Defamation by electronic means; Section 351: Criminal intimidation; Section 77(1): Voyeurism through electronic media Juris Centre.

Following is a neat and reader-friendly table giving a summary of material provisions of the IT Act, 2000 and chosen sections of the Bharatiya Nyaya Sanhita (BNS), 2023, particularly in relation to AI-enabled cyber-crimes in India. Every row contains the provision, description, and penalties

Act & Section	Crime / Description	Penalty
IT Act, 2000 – Section 66E	Unauthorized recording, publication, or transmission of private areas without consent	Up to 3 years' imprisonment or ₹2 lakh fine, or both
IT Act, 2000 – Section 66C	Identity theft using electronic means	Up to 3 years' imprisonment and/or ₹1 lakh fine
IT Act, 2000 – Section 66D	Impersonation cheating using electronic messages	Penalty as in Section 66C (IT Act, similar application)
IT Act, 2000 – Sections 67, 67A, 67B	Distribution of obscene or explicit material; stricter with sexual or child content	Max 3 years for 1st crime (Section 67); max 7 years and/or ₹10 lakh fine for explicit/child content (Section 67A/B)
IT Rules 2021	Impersonating or AI-morphed content must be removed by intermediaries on notice, or forfeit safe harbor protection	Removal within 36 hours to preserve immunity
BNS, 2023 – Section 356	Defamation by electronic, visual, or other representations	Simple imprisonment for up to 2 years or fine, or both, or community service

Notes & Observations

- Similar case application: Without AI-specific provisions, some sections of the IT Act are used against AI abuse—e.g., deepfake identity theft under Sections 66C/D, while non-consensual intimate materials can be brought under Section 67 or 67A/B.
- Holding the intermediaries accountable: The 2021 IT Rules place greater responsibility on the platforms to take prompt action against detrimental or impersonating AI content, or lose protection under the law.
- Contemporary criminal code: BNS Section 356 modernizes defamation law via digital channels, providing the amenity of community service—a contemporary sentencing measure.

2.3 Digital Personal Data Protection Act (DPDP Act), 2023

The Act requires lawful and consent-based processing of personal data—such as biometric data employed in AI deepfakes—providing a potential redress for abuse.

2.4 Institutional Frameworks

- CERT-In and NCIIPC: Organizations facilitating cyber security incident response and critical infrastructure security.
- I4C: Facilitates cybercrime response, including cross-border initiatives.
- MARVEL: Maharashtra's AI-powered predictive policing application; illustrates AI's dual-use potential—efficient but needing robust controls.

3. Literature Review & Challenges

3.1 AI-Powered Cybercrime Threats

- AI facilitates spear phishing, adaptive malware, impersonation, and other sophisticated tactics.
- Deepfakes, sexualized and used to harass, defame individuals, are disproportionately widespread, particularly against women.
- Researchers report unsatisfactory legal definitions of AI abuse, privacy and security concerns not being adequately addressed.

3.2 Enforcement Deficits

- Technical skills and AI-forensic capabilities are deficient in enforcement agencies.
- Transnational jurisdictional issues also add to the challenge of prosecuting AI-facilitated crimes.

3.3 Privacy and Rights Issues

- Lack of clear consent standards for likeness use incites Article 21 privacy issues.
- AI-driven enforcement, if not regulated, can foster surveillance that is not transparent or accountable.

3.4 Regulatory Gaps & Solutions Emergence

Category	Key Issue / Strategy	Details
Lack of AI-specific laws	No specific legislation exists targeting deepfakes or synthetic media	Reliance on outdated analogies under IT Act; calls for dedicated offense definitions and harm-based penalties
Advisories vs. enforceable regulation	Government issued advisories remain non-binding and often contradictory	Examples include MeitY's deepfake-related advisories lacking legislative backing, causing confusion
Platform accountability and liability	Safe harbor frameworks inadequate for modern AI risks	Proposals to strengthen intermediary liability, include proactive moderation, and hold platforms liable for deepfake dissemination
International regulatory models for comparison	Global jurisdictions leading with proactive legislation	UK's Online Safety Act, EU's AI Act with high-risk classification, and U.S. drafts like Deepfakes Accountability Bill provide contrasting examples

Proposed legislative frameworks	Suggested comprehensive measures	Hybrid regulatory framework including watermarking, consent norms, fair dealing exceptions, sector-specific laws, and independent oversight bodies
Need for National AI Authority	Legal oversight and ethical governance lacking	Recommendation to establish an AI Governance Authority (AIGA) to audit AI systems, assess risk, and certify compliance
Awareness, education & tech capacity	Gaps in public literacy and enforcement tools	Calls for public outreach, judicial training, cyber-forensic labs, and digital ombudsman portals for timely response
Awareness, education & tech capacity	Gaps in public literacy and enforcement tools	Calls for public outreach, judicial training, cyber-forensic labs, and digital ombudsman portals for timely response
Deepfake detection technology	Developing indigenous, scalable tech for defense	Introduction of tools like Vastav AI; however, concerns remain about bias, privacy, and false-positives

4. Case Studies

4.1 Tinsukia Deepfake Case (Babydoll Archi)

Mechanical engineer Pratim Bora from Assam created explicit morphed pictures of a former classmate using AI tools and earned approximately ₹10 lakh through subscriptions. He was arrested under various provisions of BNS such as cyber harassment, defamation, obscenity, and invasion of privacy.

4.2 Navsari Deepfake (Video of Prime Minister)

Mahendra Patel was detained for posting a deepfake video showing Prime Minister Modi involved in a simulated attack within a WhatsApp group. Offenses involve BNS Sections 197(1)(D) and 353(1)(B), and IT Act Section 66C.

4.3 Deepfakes for Elections

In India's 2024 general elections, AI-produced videos (such as politicians dancing, dead leaders supporting candidates) became rampant, leading court orders and Election Commission cautions to contain the misuse of deepfakes during polls.

5. Analysis and Recommendations

5.1 Strengthen Legal Provisions

- Create crime definitions specific to AI (deepfaking, voice cloning for scams, AI-driven impersonation).
- Enforce intermediary liability on platforms that don't tag or remove synthetic media in a timely manner.

5.2 Increase Enforcement Capacity

- Invest in forensic AI technologies and training for cyber forces across the country.
- Integrate platforms such as Vastav.AI to provide timely detection assistance.

5.3 Develop Regulatory Paradigms for AI

- Implement enforceable norms of AI governance with transparency, auditability of bias, and redress channels.
- Align with NITI Aayog's guidelines and global standards for ethical AI.

5.4 Protect Privacy and Civil Rights

- Make sure AI-facilitated policing upholds constitutional privacy standards and DPDP Act requirements for consent.
- Make transparency and accountability conditions a requirement for any use of AI in law enforcement.

5.5 Encourage International Cooperation & Platform Accountability

- Enhance MLAT arrangements and approach international cybercrime platforms.
- Make content labeling (e.g., watermarking deepfakes) mandatory and have rapid takedown enforced under IT Rules.

6. Conclusion

AI has significantly transformed cyber threats in India—from defamation via deepfakes to impersonation scams. Current legal provisions provide a foundation, but are ill-suited for AI's unique challenges. A multi-faceted response—comprising legislative refinement, enforcement enhancement, technological adoption, and rights-driven oversight—is urgently required to protect individuals while fostering ethical innovation.

References

- Times of India. (2025, July 14). *Tinsukia techie held for creating, circulating morphed pics using AI. The Times of India*. The Times of India
- Indiatimes. (2025, July 14). *Babydoll Archi's ex-boyfriend turns revenge into AI racket, earns money by faking influencer's identity online. Indiatimes Trending*. IndiatimesIndiatimes
- EasternEye. (2025). *Ex -Boyfriend Arrested in Archita Phukan AI Deepfake Porn Scandal. EasternEye*. EasternEye
- NDTV. (2025, July 13). *एआई इंजीनियर का प्यार ठुकराया तो बना दिया एक्स गर्लफ्रेंड का फेक पॉर्न पेज, असम पुलिस ने कैसे पकड़ा गुनहगार को* [How Assam cops cracked case of deepfake account by jilted lover]. *NDTV*. NDTV India
- The Economic Times. (2025, July 16). *Babydoll Archi's secret unveiled: She's neither a content influencer nor living in US. ET Online*. The Economic Times
- Wikipedia. (2025, last updated). *Maharashtra Advanced Research and Vigilance for Enhanced Law Enforcement*. In *Wikipedia*. Wikipedia
- PTI. (2025, April 1). Maharashtra govt to set up panel on using AI in government offices. *The Week*. The Week
- Wikipedia. (2025, last updated). *Vastav.AI*. In *Wikipedia*. Wikipedia+1
- Wikipedia entry on Santhosh Kumar (hacker). (2025, last updated). *Santhosh Kumar (hacker)*. In *Wikipedia*. Wikipedia
- **Digital Personal Data Protection Act (DPDP Act), 2023**
  Digital Personal Data Protection Act, 2023. *Wikipedia*. Retrieved August 17, 2025, from Wikipedia page on DPDP Act Wikipedia.
  India-Briefing. (n.d.). *India's Digital Personal Data Protection (DPDP) Act, 2023: Key Provisions*. Retrieved August 17, 2025, from India+Briefing India Briefing.
  Data Protection Board of India. *Wikipedia*. Retrieved August 17, 2025, from Wikipedia page on Data Protection Board of India Wikipedia.
- **Institutional Framework – I4C**
  Indian Cyber Crime Coordination Centre (I4C). *Ministry of Home Affairs, Government of India*. Retrieved August 17, 2025, from official "About I4C" page MHA India.
  Indian Cyber Crime Coordination Centre (I4C): Safeguarding India's Cyberspace. *Plutusias*.

Retrieved August 17, 2025, from Plutusias website Plutusias.

Indian Cyber Crime Coordination Centre (I4C). *Ministry of Home Affairs, Government of India*. Retrieved August 17, 2025, from the "Major Initiatives" page MHA India.

Indian Cyber Crime Coordination Centre. *Wikipedia*. Retrieved August 17, 2025, from Wikipedia page on I4C Wikipedia.

Times of India. (2025, May 28). 55 cyber fraud arrests: over 18,000 fraud cases linked; I4C analyzing evidence. *The Times of India*. Retrieved from Times of India The Times of India.

- The Economic Times. (2025, August 11). India's long wait for data protection law: DPDP Act still not enforced. *The Economic Times*. Retrieved from news article The Economic Times.

*****