



**AI – enabled phishing and deepfake scams in India:
Current legal landscape and existing response systems**

Authors: Krishna CV Grandhi, Kartikey Raja, Chandra Lekha

This paper can be downloaded without charge at:

www.csail.org



EXECUTIVE SUMMARY

India is facing an alarming increase in AI-driven cyber frauds like phishing and impersonation, thereby outpacing existing legal tools. Key gaps include attribution, evidence handling, and absence of AI-specific laws. Authorities such as, MeitY, MHA's I4C, are actively introducing frameworks and enhancing inter-agency coordination for effective response to cybercrimes.

INTRODUCTION

A sharp increase in AI-driven phishing and deepfake scams in India pose alarming risks to privacy and security. While existing laws like the BNS, 2023, IT Act, 2000, and the IT Rules, 2021 offer partial protections, there are no specific provisions addressing deepfakes or AI-enabled fraud. Enforcement relies on general cybercrime laws and practices which fail to keep pace with the increasingly sophisticated nature of cybercrimes.

UNDERSTANDING PHISHING AND DEEFAKE SCAMS IN INDIA

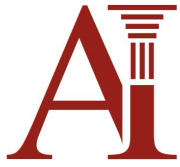
Deepfakes are a form of synthetic media created using deep learning algorithms which are highly realistic fake media created using deep learning, often used to manipulate audio, video, or images.

Phishing is a cybercrime involving deceptive communication, often impersonating legitimate sources, to trick victims into revealing sensitive data. It can lead to financial fraud, identity theft, or unauthorized access to secure systems.

In India, cybercriminals use AI tools such as, Large Language Models (LLMs) to craft highly personalized, grammatically perfect messages, and deepfakes to execute phishing scams. These attacks have caused losses exceeding ₹22,845 crore, a 206% increase from the preceding few years, averaging ₹60 crore.

PRESENT LEGAL SCENARIO: INDIAN CONTEXT

India currently lacks specific laws on deepfakes and phishing, but related offences are covered under the Information Technology (IT) Act 2000, the Bhartiya Nyaya Sanhita (BNS)2023, and the Digital Personal Data Protection (DPDP) Act 2023, among other laws.



The Constitution protects freedom of expression under Art. 19(1)(a), subject to reasonable restrictions. The Hon'ble Supreme Court, in ***K.S. Puttaswamy v. Union of India***, affirmed the right to privacy under Article 21.

Digital Personal Data Protection Act 2023

The ***Digital Personal Data Protection Act, 2023*** (“***DPDP Act***”), governs the processing of digital personal data, balancing individuals’ rights with lawful data use.

Deepfake Prevention and Criminalisation Bill, 2023

Bill No. LXX of 2023 (not in force), introduced as a private member’s bill, aiming to prevent and criminalize the creation and dissemination of deepfake content without consent or digital watermark.

Information Technology (IT) Act 2000

Chapter XI of the IT Act 2000 covers computer-related offences, with Section 66C penalizing identity theft and Section 66D penalizing cheating by personation using computer resources or communication devices.

Bharatiya Nyaya Samhita 2023

Malicious deepfake use causing reputational harm may attract defamation charges under *Section 356* of the Bharatiya Nyaya Sanhita, 2023. Additionally, threatening a person to cause alarm or compel action is punishable under *Section 351* of the same Code.

INTERNATIONAL CONTEXT

USA

The U.S. Congress introduced key Bills addressing deepfakes and cyber fraud, including the ***Take It Down Act, 2025*** which prohibits non-consensual online publication of intimate visual depictions both real and AI-generated.



European Union's General Data Protection Regulation and Artificial Intelligence Act (GDPR)

The EU's GDPR seeks to regulate personal data processing related to deepfakes, requiring victims to prove non-compliance with its provisions to seek remedy.

CHALLENGES IN IMPLEMENTATION IN INDIA

1. Lack Of Specificity

Unauthorized creation of deepfakes violates the right to privacy. However, due to the absence of specific laws, such offences must be addressed through judicial interpretation.

2. Enforcement Issues

Detection and proof of deepfake-related crimes rely on complex digital evidence requiring advanced technical expertise which India currently lacks.

3. Jurisdictional Challenges

Deepfake-related cybercrimes are often transnational thereby, complicating prosecution due to jurisdictional issues.

4. Privacy And Consent Issues

The DPDP Act 2023 requires consent to be unconditional and specific, but this may expose users to misuse of their data if consent is not fully understood by users.

LEGAL REFORMS

To address the growing threat of deepfakes, specific legislation is needed to regulate their creation and dissemination. Such reforms may include:

- Mandatory informed consent
- Mandatory disclosure requirements
- Criminal liability for unauthorized use



- Amendments to the existing laws to expressly include deepfake offences & penalties.

TECHNOLOGICAL REFORMS

The government should invest in AI-based deepfake detection systems to combat frauds such as deepfakes and phishing. The MeitY under the **IndiaAI mission**, has already invited projects, including deepfake detection, under its “**Safe & Trusted AI**” initiative. Such reforms, specific to the needs of the users are a precursor to ensure user safety and privacy.

CAPACITY BUILDING

Capacity building through training and awareness for law enforcement agencies is vital to combat deepfake-related cybercrimes.

WAY AHEAD

Addressing deepfake-enabled cybercrimes necessitates an integrated legal, technological, and awareness-driven approach. A coordinated effort involving the government, legal authorities, technical experts, and civil society is essential. Only through collective action and a robust regulatory framework can the growing threats of deepfake misuse be effectively mitigated.

www.csail.org