The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

ARTIFICIAL INTELLIGENCE AND CYBERCRIME: EMERGING LEGAL CHALLENGES IN THE DIGITAL ERA

-Saleha Haneef

ABSTRACT

The proliferation of generative artificial intelligence has transformed cybercrime from a game of scale into one of synthetic realism, enabling voice cloning, deepfake impersonation, and hyper-personalised phishing that have cost India over ₹22,495 crore in 2025 alone. This article examines India's improvisational legal response to AI-enabled fraud, tracing how the Information Technology Act 2000, Bharatiya Nyaya Sanhita 2023, and the 2025 synthetic media amendments retrofit pre-AI statutes onto novel crimes. It analyses the Delhi High Court's emergence as a de facto first responder through personality-rights litigation, alongside persistent evidentiary hurdles under the Bharatiya Sakshya Adhiniyam's certification regime. Situating India within a fragmented global mosaic spanning the EU AI Act, US state-level statutes, and the UN Convention against Cybercrime, the article identifies three unresolved fault lines — attribution, supply-chain liability, and the tension between labelling mandates and free expression and proposes decentralised forensic capacity, a dedicated AI-enabled crime aggravator, and treaty ratification as reforms.

Keywords: Artificial Intelligence, Cybercrime, Deepfake, Digital Evidence, Cyber law

INTRODUCTION

In the year 2025, it has been reported that India lost around ₹22,495 crore to internet fraudsters over 28.15 lakh fraud incidents which is an increase of 24% in case load compared to 2024, driven overwhelmingly by investment scams, 'digital arrest' extortion, and impersonation

fraud.[1] What is different in this wave of cyber crime is not just the scale of loss but also the fact that technology has improved considerably. AI has emerged as a vital tool for fraudsters making it all the more easier for them to carry out their scams. Cloning any voice from a thirty-second video clip from social media, photoshopping someone's face over a video call, or generating phishing emails in perfect English has never been this easy. The most apt example of this is a case from Hong Kong where a finance employee from Arup approved transfers worth USD 25.6 million after a video call where every single person, including the chief officer of the company was an AI deepfake.[2] This short article examines how the Indian government is struggling to formulate rules regarding AI- aided cybercrime, and identifies the structural fault lines that continue to resist easy legislative repair.

THE CHANGING ANATOMY OF CYBERCRIME IN THE AGE OF AI

Traditionally, cybercriminals operated on a large scale; they would send out phishing emails by the millions, hoping that some recipients would respond. However, the rise of generative AI has changed this playbook, allowing criminals to adopt strategies that were previously deemed impossible. With the help of large language models capable of writing perfect phishing emails, advanced voice-cloning kits as well as deepfake video generators, fraudsters can now craft messages that are highly persuasive. An example of this is the more recent 'digital arrest' scam based on the impersonation of law enforcement and court authorities using generative AI that took place in India. In this scam, victims are tricked into believing that they are discussing their arrest with a real police officer or a CBI agent via video call—this might include the usage of real-looking seals and arrest warrants, both of which are created with the help of AI. By 2025, the losses from scams based on this technology accounted for about 9% of all cybercrime activities in the country. Sextortion with the help of AI-manipulated private images and swindles through AI-operated chatbots referred to as 'pig-butchering', where clients are deceived for weeks by an imaginary partner and led to false trading productions, represent a criminal ecosystem in which AI makes it easier for the wrongdoers and harder for the victims. Crucially, each of these schemes is modular: the same underlying voice-cloning or video-

[1]Samridhi Tewari, Cybercrime Saw 24% Spike in 2025. Indians Lost Rs 22,495 Crore, Mainly in Investment Scams, The Print (Feb. 21, 2026), https://theprint.in/india/cybercrime-saw-24-spike-in-2025-indians-lost-rs-22495-crore-mainly-in-investment-scams/2859930/

[2]Heather Chen & Kathleen Magramo, British Engineering Giant Arup Revealed as Victim of $25 Million Deepfake Scam, CNN Bus. (May 17, 2024), https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk

synthesis tool can be repurposed across investment fraud, romance scams, and corporate impersonation with only minor adjustments, meaning that a single technical advance in generative AI now propagates almost instantly across the entire cybercrime economy rather than remaining confined to one niche.

INDIA'S STATUTORY TOOLKIT: RETROFITTING OLD LAW ONTO NEW CRIME

With respect to criminal legislation related to Artificial Intelligence, India does not have any such laws but is still using the provisions of general laws created for the earlier era of Internet, including the Information Technology Act 2000. Section 66 C imposes penalty for identity theft based on wrongful use of another person's identity,[3] Section 66 D prohibits cheating by impersonation with the use of computer resources including deepfake images and videos,[4] and Section 66 E is relevant in such cases where images are recorded or transmitted in violation of privacy even if it is done without the consent of the individual in the images.[5] The provisions in the Information Technology Act are general or neutral in a sense that it can cover activities related to Artificial Intelligence without having to change the laws; however, these laws do not cover the upstream issues such as the training of the model, the source of the data used for the model, or the responsibilities of developers of the AI tool used in the case.

The legal foundation for crime was completely transformed on July 1, 2024, when the Bharatiya Nyaya Sanhita, 2023 took the place of the Indian Penal Code. Cheating and dishonest persuasion, which are the most frequent applications of AI-enabled financial crime, are now defined in Section 318,[6] while the forgery of electronic documents, which is applicable when a deepfake document is used to commit fraud, is explained in Section 336.[7] The most direct legislation in response to synthetic media was enacted in October 2025 when the Ministry of Electronics and Information Technology passed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which placed the legal obligation to define "synthetically generated information" and apply labeling, watermarking

[3]The Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India) (punishing identity theft).
[4]The Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India) (punishing cheating by personation using a computer resource).
[5]The Information Technology Act, 2000, § 66E, No. 21, Acts of Parliament, 2000 (India) (punishing violation of privacy through capture, publication, or transmission of images).
[6]The Bharatiya Nyaya Sanhita, 2023, § 318, No. 45, Acts of Parliament, 2023 (India).
[7]The Bharatiya Nyaya Sanhita, 2023, § 336, No. 45, Acts of Parliament, 2023 (India).

and taking down regulations on intermediaries and go-betweens.[8] The Digital Personal Data Protection Act, 2023 consists of a parallel regulatory framework that limits processing of personal data that is used by AI systems to create sounds and faces of imitation characters, although the method of implementation of this act remains data protection oriented and not oriented toward crimes.[9]

Another layer of the framework, which plays an equally significant role, takes place upstream of prosecution against any individual incident. The Indian Computer Emergency Response Team's 2022 Directions demand that the service providers, intermediaries, data centers, and corporates report certain types of cyber incidents (identity theft, data breach, and unauthorized access) within six hours.[10] For AI-based fraud, this interval of reporting becomes significantly more critical since it is usually the financial institution's own six-hour notice rather than the victim's complaint that alerts the authorities about fraud, since victims may not even know that they have been deceived by synthetic media until a while after the money has been transacted via multiple mule accounts.

COURTS AS FIRST RESPONDERS: PERSONALITY AND PRIVACY RIGHTS LITIGATION

The Delhi High Court has become an unexpected immediate solution in the legal field due to the slow-paced lawmaking process. The Court's foundation rests on the fundamental right to privacy granted in *Justice K.S. Puttaswamy v. Union of India*[11] and the earlier legal precedent of *R. Rajagopal v. State of Tamil Nadu*[12], so it has granted Anil Kapoor, in *Anil Kapoor v. Simply Life India*[13], a broad ex-parte injunction prohibiting sixteen named respondents and everybody else from using the actor's name, voice, image or catchphrase through any means at their disposal, including generative AI. Justice Prathiba M. Singh noted that at this point 'technology tools are so advanced that even an illegal user can capture a celebrity's character

[8]Ministry of Elecs. & Info. Tech., Gov't of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025, Notification No. G.S.R. 687(E) (Oct. 22, 2025), amending the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to introduce Rule 2(1)(wa) defining 'synthetically generated information.'
[9]The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[10]Indian Computer Emergency Response Team, Ministry of Elecs. & Info. Tech., Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In (Apr. 28, 2022) (India) (mandating reporting of specified cyber incidents within six hours of notice).
[11]*Justice K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1 (India).
[12]*R. Rajagopal v. State of T.N.,* (1994) 6 SCC 632 (India).
[13]*Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914 (India).

using such technology even including Artificial Intelligence.' Following this observation, Amitabh Bachchan, Aishwarya Rai Bachchan, Abhishek Bachchan, Jaya Bachchan, Hrithik Roshan, and Ajay Devgn have jumped on the bandwagon of proceeding with similar lawsuits.[14] While these 'John Doe' orders present a judicial solution that is simple, fast, and no matter what technology is used, they are practically restricted to those capable of fighting a lawsuit; the average citizen whose voice is the basis for a bank fraud will have to rely on a longer route of criminal investigation under the IT Act and BNS.

THE EVIDENTIARY FRONTIER: PROVING WHAT AI MADE LOOK REAL

Regardless of any of the abovementioned provisions having been infringed, a conviction is still contingent on the prosecution demonstrating to the satisfaction of the court that the video/voice note/document in question was generated using artificial intelligence (AI) and is false. As of July 1, 2024, the admissibility of electronic evidence is governed by Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which mandates a certificate along with a hash value from the originator of the evidence and a forensic expert that the evidence will be treated by the court as a reliable piece of secondary evidence.[15] The practical problem is that deepfake forensics is an arms race: detection technology developed to detect a particular era of synthetic media will prove ineffective against its next iteration, and Indian cyber-forensic laboratories are few and far between, located mainly in metropolises.

THE GLOBAL REGULATORY MOSAIC

India's improvisation occurs in a disjointed global environment. The European Union's Artificial Intelligence Act outlaws a set of specific deceptive and exploitative AI applications[16] while mandating under Article 50 that the manufacturers of generative AI software label their products machine-readable and that those making use of this technology inform the public of deepfake materials, with the requirements becoming effective from August 2026.[17] As for cross-border investigations, the Council of Europe's Budapest Convention on Cybercrime which is the oldest multilateral instrument in this field has never been signed or ratified by

[14]*See* Amitabh Bachchan v. Rajat Nagi, 2022 SCC OnLine Del 4110 (India); *see* also Nandini Bhandari, India Tightens Rules on Deepfakes and AI-Generated Content, Law.asia (Feb. 10, 2026), https://law.asia/india-deepfake-regulations/ (surveying interim orders obtained by Aishwarya Rai Bachchan, Abhishek Bachchan, Jaya Bachchan, Hrithik Roshan, and Ajay Devgn).
[15]The Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47, Acts of Parliament, 2023 (India).
[16]Regulation 2024/1689, art. 5, 2024 O.J. (L 1689) (EU) [hereinafter EU AI Act].
[17]EU AI Act, *supra note* 16, art. 50.

India, the lack of participation in the drafting[18] placed Indian law-enforcement authorities in a dependent position and made them use lengthy mutual legal assistance treaty requests for effective law enforcement because many of the AI crimes are perpetrated from abroad. The United Nations Convention against Cybercrime, adopted by the General Assembly in December 2024 and opened for signature in Hanoi in October 2025, is the first genuinely global attempt to bridge this gap, and its uptake by major digital economies including India over the coming years will materially shape how quickly cross-border AI-fraud evidence can be obtained.[19]

On the contrary, the United States has yet to pass an all-encompassing federal AI-crime statute, instead relying primarily on state laws designed to combat deepfake election disinformation and non-consensual imagery. It has also begun to apply the regulatory powers of the Federal Trade Commission over unfair and misleading business practices to ban AI voice- cloning scams.[20] This fragmentation — sector-specific rules in the United States, a single horizontal statute in the European Union, and technology-neutral criminal law supplemented by ad hoc intermediary rules in India — means that an AI-enabled fraud routed through servers in three jurisdictions may be regulated quite differently in each, a mismatch that can facilitate the activities of sophisticated criminal syndicates that deliberately structure their operations to exploit those gaps.

UNRESOLVED FAULT LINES

As long-lasting as every legal remedy is a trio of structural problems. Firstly, there is attribution; generative AI tools are usually open-source, self-hosted, or run through anonymizing systems. This makes it easy to create a deepfake but extremely difficult to identify a person behind it in light of liability according to Section 66D or Section 318. Secondly, there is allocation of liabilities in the supply chain of AI technology: model developer, fine-tuner, deploying platform, and final user all play a specific role in the commission of an AI-enabled

[18]Convention on Cybercrime art. 1, Nov. 23, 2001, E.T.S. No. 185; *see* also Sunil Abraham & Elonnai Hickok, Budapest Convention and the Information Technology Act, Ctr. for Internet & Soc'y (India) (noting that India has neither signed nor ratified the Convention).

[19]United Nations Convention against Cybercrime, G.A. Res. 79/243 (Dec. 24, 2024), opened for signature Oct. 25, 2025, Hanoi, Viet Nam.

[20]*See*, e.g., Cal. Elec. Code § 20010 (criminalising the distribution of deceptive AI-generated election communications); Tex. Bus. & Com. Code § 620.001 (deepfake video disclosure requirements); Federal Trade Commission Act, 15 U.S.C. § 45 (prohibiting unfair or deceptive acts or practices, invoked by the FTC against AI-enabled voice-cloning fraud).

crime, but the Indian legislation lacks the framework able to address the matter appropriately, and the courts have to revert to intermediary liability rules under Section 79 of the IT Act that were created for any content generated by users and not for the platforms producing synthetic content in a proactive way.

The third aspect is the conflict between the regulations of obligatory labelling and the freedom of expression: Article 50 of the EU's legislation and the Indian synthetic content regulations of 2025 may be perceived as reiterated speech,[21] where satire, artistry, or honest commentary are put in one basket with fraudulent impersonation. None of these issues can be solved by prohibiting the misuse of artificial intelligence only; they require technical standards (i.e., provenance watermarking), accountability of platforms, and international cooperation together with criminal law.

WAY FORWARD

India should take three specific measures. First of all, it is imperative to create forensic cyber facilities for the identification of synthetic media in State forensic laboratories, as opposed to limiting this function to a select group of national agencies, so that compliance with Section 63 can be accomplished outside major urban areas. Secondly, Parliament ought to introduce a specific aggravation charge of 'AI-enabled crime' which is similar to hate crime aggravators employed in other jurisdictions, that would imply the imposition of a harsher penalty in case a crime falling under the BNS Act or Information Technology Act was committed through the use of synthetic impersonation, thus allowing judges and investigators to center around a specific accusation instead of a heterogeneous array of general accusations. Thirdly, India must work with the UN Convention on Cybercrime and seek the ratification of this treaty to be able to get assistance for the cross-border evidence necessary for obtaining results in every other AI fraud case.

CONCLUSION

Instead of bringing forth an entirely new form of crime, AI is rather responsible for the industrialisation of deception. This involves eliminating the time, effort, and skills once required to impersonate an individual, document, or an organisation. India has taken a creative

[21]The Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India) (intermediary safe harbour, subject to due diligence conditions).

but reactive approach to this phenomenon wherein the existing legal statutes are adapted by smart lawyers to suit the situation, a proactive High Court comes up with solutions based on its reading of personality rights, and the first synthetic media regulation has only been enacted after scandalous accidents linked to artificial media. This improvisation has helped the society to avoid problems for the time being but with no guarantees. The jurisdictions least affected by the problem of discovery of fake media will be those where it does not consider the AI-induced crimes as a new term for crimes committed in the past but instead creates new rules and procedures designed to avoid fake media implications.