

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ARTIFICIAL INTELLIGENCE AS A NEW DIMENSION OF CYBERCRIME IN INDIA: LEGAL ISSUES AND CONCERNS

AUTHORED BY - RATNESH KUMAR

Research Scholar, Central University of South Bihar, Gaya, Bihar – 824236, India

CO-AUTHOR - DR PALLAVI SINGH

Assistant Professor, Central University of South Bihar, Gaya, Bihar – 824236, India

Abstract

In India, cybercrime has evolved from an activity requiring people with special skills into one that is far more scalable, automated and persuasive, powered by Artificial Intelligence (AI). Generative tools can now create realistic deepfake videos, cloned voices, error-free phishing messages and responsive malware at almost negligible cost, propelling the "digital arrest" frauds, investment scams and synthetic sexual images that make up much of India's complaint data. This paper analyses whether the existing Indian legal framework, comprising the Information Technology Act, 2000; the Bharatiya Nyaya Sanhita, 2023; the Bharatiya Nagarik Suraksha Sanhita, 2023; the Bharatiya Sakshya Adhiniyam, 2023; the Digital Personal Data Protection Act, 2023 (DPDP Act); and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules) as amended to include synthetically generated information, is adequate to prevent, investigate and punish AI-enabled offences. Following a doctrinal and analytical approach, supported by official crime data, judicial decisions and a comparative analysis of the European Union, the United States, the United Kingdom, China and the United Nations Convention against Cybercrime, the paper identifies six structural challenges: the absence of a statutory definition of AI or AI-generated content; problems of attribution when autonomous systems act; uncertain liability of developers, deployers and intermediaries; evidentiary barriers in verifying and disputing synthetic media; cross-border jurisdiction; and limited investigative capacity. It contends that most AI-assisted conduct falls within India's technology-neutral provisions, but that significant gaps remain in harm-specific, risk-based and procedural regulation. The paper ends with recommendations for a tailored AI-specific offence and liability framework, mandatory provenance and labelling

requirements, enhanced forensic capability, victim-centric remedies and international cooperation.

Keywords: Artificial Intelligence; Cyber Crime; Deepfake; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Intermediary Liability; Digital Evidence; Data Protection.

I. Introduction

Artificial Intelligence is the biggest force-multiplier in the history of cybercrime. Earlier generations of cyber offending required technical skill, time and a level of human effort that naturally limited their scale.

Generative AI removes these limits. A scammer with no knowledge of coding can now replicate the voice of a relative from a few seconds of audio, generate a hyper-realistic video of a police officer or a judge, write convincing phishing messages in any Indian language and carry on thousands of conversations at the same time. The underlying crime is most often an old one, such as cheating, extortion, forgery, defamation or sexual exploitation, but the instrument is new, and the new instrument transforms the scale, speed, credibility and cross-border reach of the harm.¹

India feels this shift acutely. According to the National Crime Records Bureau (NCRB), cybercrime in India rose by 31.2 per cent between 2022 and 2023, from 65,893 cases to 86,420 cases, of which fraud alone accounted for 68.9 per cent (59,526 cases).² The real problem is much larger than the number of registered FIRs suggests. Complaint data of the Indian Cyber Crime Coordination Centre (I4C) show that citizens reported losses of about ₹22,845 crore to cyber fraud in 2024,³ and about ₹22,495 crore in 2025, with investment scams constituting roughly three-quarters of that figure.⁴ Enforcement has failed to keep pace. Of 64,907 cyber

¹ Amaresh Patel et al., "Artificial Intelligence Regulation and Governance: A Comparative Doctrinal Analysis of Emerging Legal Frameworks" (2026).

² National Crime Records Bureau, *Crime in India 2023: Statistics*, vol. II (Ministry of Home Affairs, Government of India, New Delhi, 2025); see also "Crime in India 2023 – NCRB Report Highlights Surge in Cybercrime in India", *Vajiram & Ravi*, September 30, 2025, available at: <https://vajiramandravi.com/current-affairs/crime-in-india-2023-ncrb-report-highlights-surge-in-cybercrime-in-india/> (last visited on October 4, 2026).

³ Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 344, answered on July 22, 2025; "Cyber Frauds Cost India ₹22,845 Crore in 2024 as Digital Threats Escalate", *Quick Heal*, July 2025, available at: <https://www.quickheal.co.in/documents/media/2025/cyber-frauds-cost-india-digital-terminal-july2025.pdf> (last visited on October 4, 2026).

⁴ "Cybercrime saw 24% spike in 2025, Indians lost Rs 22,495 crore mainly in investment scams", *ThePrint*, February 21, 2026, available at: <https://theprint.in/india/cybercrime-saw-24-spike-in-2025-indians-lost-rs-22495-crore-mainly-in-investment-scams/2859930/> (last visited on October 4, 2026).

crime cases registered across the States in 2022, only about 1.7 per cent ended in the conviction of persons.⁵

These offences are increasingly permeated by AI. Law-enforcement agencies have observed that large language models enable wrongdoers with little skill to generate realistic fraudulent material, harmful code and misinformation at scale.⁶ Scholars describe this as the birth of "AI-Crime", a category in which AI acts as the tool of a crime, becomes the object of a crime, or behaves with a degree of autonomy that makes it difficult to attribute criminal responsibility.⁷ The "digital arrest" phenomenon, in which offenders pretend to be investigating agencies and courts through video calls and forged orders, is a severe Indian example. The Supreme Court took suo motu notice of it in October 2025, entrusted a nationwide probe to the Central Bureau of Investigation (CBI) in December 2025, and in July 2026 suggested that "digital arrest" be made an offence in its own right.⁸

Regulators have responded gradually. India has no AI-specific statute. In November 2025, the Ministry of Electronics and Information Technology (MeitY) published the India AI Governance Guidelines, which advocate a "light-touch", principle-based and sectoral approach in preference to new legislation.⁹ By a notification dated February 10, 2026, MeitY amended the IT Rules to bring "synthetically generated information", including deepfakes, within their purview with effect from February 20, 2026.¹⁰ Meanwhile, India re-enacted its core criminal laws in 2023 through the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS) and the Bharatiya Sakshya Adhiniyam (BSA), none of which refers to AI expressly.

⁵"Only 1.6% conviction rate in 2 yrs amid surge in cybercrime cases", *The Tribune*, available at: <https://www.tribuneindia.com/news/india/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrime-cases-2/amp> (last visited on October 4, 2026).

⁶Europol, *ChatGPT: The Impact of Large Language Models on Law Enforcement* (Tech Watch Flash Report, Europol Innovation Lab, The Hague, 2023).

⁷Thomas C. King, Nikita Aggarwal, Mariarosaria Taddeo and Luciano Floridi, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions" 26 *Science and Engineering Ethics* 89 (2020).

⁸*In Re: Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025 (Supreme Court of India); "Supreme Court calls for separate offence on digital arrests, harsher punishment against accused", *Bar & Bench*, July 28, 2026, available at: <https://www.barandbench.com/news/supreme-court-calls-for-separate-offence-on-digital-arrests-harsher-punishment-against-accused> (last visited on October 4, 2026).

⁹Ministry of Electronics and Information Technology, *India AI Governance Guidelines* (IndiaAI Mission, Government of India, New Delhi, November 5, 2025).

¹⁰The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), dated February 10, 2026, available at: <https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf> (last visited on October 4, 2026).

Research questions

1. What new types of cybercrime has AI created in India, and which existing ones has it exacerbated?
2. How effectively do the IT Act, 2000, the new criminal laws, the DPDP Act, 2023 and the amended IT Rules respond to AI-enabled offending?
3. What doctrinal, evidentiary, jurisdictional and institutional problems arise when existing law is employed against AI-enabled crime?
4. What can India learn from comparative and international regulatory models?

Methodology and scope

This paper uses a doctrinal and analytical approach. The primary sources are Central legislation, subordinate legislation, government notifications and the judgments of the Supreme Court and High Courts. The secondary sources include official crime statistics, parliamentary answers, reports of international organisations and academic literature. The paper compares the European Union, the United States, the United Kingdom and China, together with the Budapest Convention and the United Nations Convention against Cybercrime. The study is limited to the criminal and regulatory aspects of AI misuse; questions of intellectual property, competition and employment are considered only so far as they bear on criminal liability. The law is stated as on October 4, 2026.

Part II constructs a conceptual framework and typology. Part III outlines the forms of AI-powered cybercrime in India. Part IV examines the existing legal framework and Part V the judicial response. Part VI focuses on the key legal problems and tensions. Part VII provides a comparative context, Part VIII presents recommendations and Part IX concludes.

II. Conceptual Framework: Locating AI in Cybercrime

A. Defining the terms

Indian law does not define "artificial intelligence" or "cybercrime". The European Union's Artificial Intelligence Act defines an AI system as a machine-based system designed to operate with varying levels of autonomy, which may exhibit adaptiveness after deployment and which infers from its inputs how to generate outputs, such as predictions, content, recommendations or decisions, that can influence physical or virtual environments.¹¹ The features crucial for

¹¹Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *Official Journal of the European Union*, L series, July 12, 2024, art. 3(1).

criminal law are autonomy and inference: the system generates outputs that its developer or user did not pre-define.

In India, the term "cybercrime" is likewise descriptive rather than statutory. The IT Act, 2000 creates specific offences relating to computer resources, whereas the NCRB records as "cyber crimes" all offences in which a communication device is the medium or the target, whether they are registered under the IT Act, the penal code or special laws.¹² Accordingly, AI-enabled cybercrime may be understood as any crime in which an AI system is the instrument, is the target of attack, or autonomously helps to bring about the illegal outcome.

B. A four-fold typology

Table 1 adapts the literature on AI-Crime to the Indian context.¹³

Table 1: Typology of AI-enabled cybercrime

Category	Use of AI	Typical behaviour	Primary legal challenge
AI as a tool	Used by a human offender	Deepfake fraud, voice cloning, AI-written phishing, synthetic sexual imagery of real persons, forged orders in "digital arrest" scams	Existing offences apply, but proving authorship and authenticity is harder
AI as a force-multiplier	Automates scale and personalisation with minimal human intervention	Bot-driven investment scams, mass sextortion, automated vulnerability scanning, "crime-as-a-service" tools such as WormGPT	Penalties and enforcement were designed for individual, not industrial, offending

¹²*Supra* note 1; see also Government of India, Press Information Bureau, "Cyber Crime Cases and Forensic Capabilities", December 3, 2025, available at: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198253> (last visited on October 4, 2026).

¹³*Supra* note 6.

Category	Use of AI	Typical behaviour	Primary legal challenge
AI as a target	Attacks on the model, its data or its outputs	Data poisoning, model theft through APIs, prompt-injection attacks, adversarial attacks on biometric or fraud-detection systems	Difficult to fit within "unauthorised access" and "damage" under ss. 43 and 66 of the IT Act
AI as a semi-autonomous agent	System acts under limited human control	Agentic AI that performs transactions, spreads defamation or launches attacks beyond the user's instructions	Attribution of mens rea and the "responsibility gap"

The first two categories already dominate Indian crime data. WormGPT and FraudGPT, underground tools marketed in 2023 as large language models free of safety restrictions, show how AI capability is now sold as a service to offenders without technical skill.¹⁴ The third category is expanding as AI systems are integrated into banking, policing and identity verification. Security bodies now recognise prompt injection, training-data poisoning and model theft as distinct attack vectors against AI applications.¹⁵ Adversarial machine learning can also defeat the facial-recognition and fraud-detection models on which Indian financial institutions increasingly rely.¹⁶

The fourth category poses the most profound theoretical questions. According to Hallevy, criminal law can approach AI through three models: AI as an innocent agent of a human perpetrator; liability for the natural and probable consequences of deploying the system; and,

¹⁴Daniel Kelley, "WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks", *SlashNext*, July 13, 2023.

¹⁵OWASP Foundation, *OWASP Top 10 for Large Language Model Applications* (OWASP, 2025).

¹⁶Apostol Vassilev, Alina Oprea, Alie Fordyce and Hyrum Anderson, *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*, NIST AI 100-2 E2023 (National Institute of Standards and Technology, Gaithersburg, 2024).

most contentiously, direct liability of the AI entity as an independent criminal actor.¹⁷ Abbott, in contrast, advocates legal neutrality between human and AI conduct while keeping liability with natural and legal persons.¹⁸ Current Indian law, which recognises corporate but not machine criminal liability, permits only the first two models.¹⁹

III. AI-Assisted Cyber Crime: New Forms of Cyber Crime in India

A. Deepfake impersonation and voice-cloning fraud

Deepfake impersonation is the most obvious AI-assisted crime. Criminals replicate the voice of a relative to demand immediate financial help, or make videos of corporate executives, celebrities and politicians promoting bogus investment schemes. Abroad, the engineering firm Arup lost about US\$25 million in 2024 when an employee in Hong Kong attended a video call in which all other participants, including the company's chief financial officer, were deepfakes.²⁰ In India, a fake video of a well-known actress went viral and led to the arrest of its creator in January 2024, while deepfakes of Union Ministers and businessmen have been used to promote fictitious investment platforms.²¹ Since investment scams account for about three-quarters of reported fraud losses, synthetic celebrity endorsements are a key cause of financial loss.²²

B. Synthetic authority: the rising threat of "digital arrest"

In a "digital arrest" scam, criminals impersonate officers of the CBI, the Enforcement Directorate, the police or the judiciary, keep the victim under continuous video surveillance and demand payments under threat of arrest. AI tools make these schemes far more believable by generating fake court orders with stamps and signatures, creating "police station" backgrounds, and producing synthetic voices and scripts in the victim's own language. Acting on the complaint of a senior-citizen couple from Ambala who were duped of more than ₹1

¹⁷Gabriel Hallevy, "The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control" 4 *Akron Intellectual Property Journal* 171 (2010).

¹⁸Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, Cambridge, 2020).

¹⁹Radha Ranjan: Jivantika Gulati, "Catalytic Role of Artificial Intelligence in Ameliorating Criminal Justice System: A Critical Analysis," in *Empowerment and Equality: Navigating Human Rights Law in a Complex World* (2023), pp. 47–54.

²⁰Kathleen Magramo, "British engineering giant Arup revealed as \$25 million deepfake scam victim", *CNN*, May 17, 2024.

²¹"Rashmika Mandanna deepfake video: Delhi Police arrest main accused", *The Hindu*, January 20, 2024; "Delhi HC bars unauthorised use of Aishwarya Rai Bachchan's name, image", *The Federal*, September 11, 2025, available at: <https://thefederal.com/category/news/delhi-high-court-protects-aishwarya-rai-bachchan-personality-rights-deepfakes-206214> (last visited on October 4, 2026).

²²*Supra* note 3.

crore through forged orders of the Court itself, the Supreme Court registered *In Re: Victims of Digital Arrest Related to Forged Documents* and noted that such offenders had siphoned off more than ₹3,000 crore across the country.²³ On December 1, 2025, the Court entrusted a pan-India investigation to the CBI, directed intermediaries to furnish traffic and content data, and allowed the freezing of accounts traceable to such offences.²⁴ The Department of Telecommunications subsequently issued SIM-binding directions to messaging applications to curb VoIP-based frauds.²⁵

C. AI-generated phishing and social engineering

Phishing messages were once easy to spot because of spelling errors and awkward phrasing, but generative models remove those telltale signs. Scam operations, run from large cities and small towns alike, produce customised emails, SMS and WhatsApp messages in Hindi, Tamil, Bengali or any other language, while chatbots sustain long "romance" or "task" scams with thousands of victims simultaneously. Business email compromise has become far more successful because AI can replicate the writing style of a particular executive.²⁶ The result is a fall in the cost of deception and a rise in its effectiveness.

D. AI-assisted malware and intrusion

AI helps offenders to write malicious code, alter it to escape detection, search networks for weak points and automate credential-stuffing attacks. The most powerful commercial models have built-in safeguards, but these are bypassed through "jailbreak" prompts or by using unrestricted open-weight models.²⁷ The threat to critical information infrastructure, already protected under s. 70 of the IT Act, increases correspondingly.

E. Synthetic sexual imagery, sextortion and gendered harm

"Nudify" applications and face-swap tools create sexually explicit pictures of real women from

²³"SC tells CBI to probe pan-India digital arrest scam, role of bank staff", *The Tribune*, December 1, 2025, available at: <https://www.tribuneindia.com/news/cybercrimeindia/sc-tells-cbi-to-probe-pan-india-digital-arrest-scam-role-of-bank-staff> (last visited on October 4, 2026).

²⁴*In Re: Victims of Digital Arrest Related to Forged Documents*, SMW (CrI.) No. 3 of 2025, order dated December 1, 2025 (Supreme Court of India), available at: <https://indiankanoon.org/doc/67470969/> (last visited on October 4, 2026).

²⁵"Digital Arrests: MHA Proposes SOP Before Supreme Court, RBI To Consider Staff Accountability & Liability Framework", *LiveLaw*, February 10, 2026, available at: <https://www.livelaw.in/top-stories/supreme-court-digital-arrest-scam-suo-motu-mha-status-report-sop-rbi-cbi-dot-meity-victim-compensation-liability-framework-522549> (last visited on October 4, 2026).

²⁶*Supra* note 5.

²⁷*Supra* notes 5 and 13.

ordinary photographs. These images are weaponised for harassment, revenge and extortion, with deeply gendered consequences.²⁸ Even when viewers know that an image has been manipulated, the reputational and psychological damage to the victim is real. Women lodged about 4.63 lakh financial cyber fraud complaints involving ₹3,764.51 crore in 2025 alone,²⁹ while non-financial abuse such as synthetic intimate imagery is widely believed to be under-reported.³⁰

F. AI-generated child sexual abuse material

Generative image models can produce child sexual abuse material without any real child being photographed. Indian law is better placed on this front than many jurisdictions, because the definition of "child pornography" inserted into the Protection of Children from Sexual Offences Act, 2012 in 2019 expressly includes digital or computer-generated images indistinguishable from an actual child.³¹ The Supreme Court has also suggested replacing the term with "child sexual exploitative and abuse material" (CSEAM) and held that viewing, possession or storage with the requisite intention may constitute an offence.³²

G. Electoral and public-order deepfakes

Fake audio and video of political leaders can go viral before elections or in times of communal tension. During the 2024 general election, the Election Commission of India directed political parties to take down deepfake content within three hours of it coming to their knowledge.³³ Such content may attract offences under the BNS relating to statements conducing to public mischief and imputations prejudicial to national integration, but the speed of viral dissemination makes post-facto prosecution an imperfect cure.³⁴

²⁸Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 *California Law Review* 1753 (2019).

²⁹"Over 1 lakh senior citizens, 4.63 lakh women lodged financial cyber fraud complaints amounting to Rs 7,769 crore in 2025: Govt", *ANI*, August 5, 2026, available at: <https://www.indiasnews.net/news/279223790/over-1-lakh-senior-citizens-463-lakh-women-logged-financial-cyber-fraud-complaints-amounting-to-rs-7769-crore-in-2025-govt> (last visited on October 4, 2026).

³⁰Radha Ranjan: Pallavi Singh, "Cyber Crime Against Women in Cyber Space: A Critical Analysis of Indian Legislations," *Kanpur Philosophers*, Vol. X, Issue I(A) (2023).

³¹The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), s. 2(1)(da), inserted by the Protection of Children from Sexual Offences (Amendment) Act, 2019 (Act 25 of 2019).

³²*Just Rights for Children Alliance v. S. Harish*, 2024 SCC OnLine SC 2611.

³³Election Commission of India, Advisory on Responsible and Ethical Use of Social Media Platforms by Political Parties and Candidates, May 6, 2024.

³⁴Radha Ranjan & Jivantika Gulati, "The Sexual Harassment against Women in Cyber Space: Concept, Reality and the Law," *Kashmir Journal of Legal Studies*, Vol. X, No. 1 (2023), pp. 79–90

H. Attacks on AI systems

Finally, AI systems are themselves targets. Data poisoning can embed hidden behaviour in training data, repeated queries can result in model extraction, and prompt-injection attacks can trick AI agents into disclosing sensitive information or executing unauthorised actions.³⁵ As banks, insurers and government departments deploy AI for credit decisions, fraud screening and citizen services, such attacks will become a novel but important vector of cybercrime.³⁶

IV. The Existing Legal Framework

In India, AI-enabled cybercrime is regulated through scattered, technology-neutral provisions in different statutes rather than through an overarching law on AI. Table 2 links the principal forms of conduct identified in Part III to the provisions likely to be invoked.

Table 2: AI-enabled conduct and applicable Indian law

AI-enabled conduct	IT Act, 2000	Bharatiya Nyaya Sanhita, 2023	Other law
Deepfake or voice-clone fraud	ss. 66C, 66D	ss. 318, 319 (cheating; cheating by personation)	BNS s. 111 where organised
"Digital arrest"	s. 66D	ss. 204 (personating a public servant), 308 (extortion), 336, 340 (forgery; forged electronic records)	Telecommunications Act, 2023, s. 42
Synthetic intimate imagery	ss. 66E, 67, 67A	ss. 77, 78, 79, 294, 356	Indecent Representation of Women (Prohibition) Act, 1986
AI-generated CSAM	s. 67B	s. 294	POCSO Act, 2012, ss. 2(1)(da), 13–15

³⁵*Supra* notes 14 and 15.
³⁶ R. Sabareesh, Deependra Nath Pathak, Radha Ranjan, Ramachandran Devi Prasanna, P. Shalini & Eijaz Khan Bellary, “AI-Driven Fraud Detection in Banking: Enhancing Transaction Security,” *Journal of Informatics Education and Research*, Vol. 4, Issue 3 (2024).

AI-enabled conduct	IT Act, 2000	Bharatiya Nyaya Sanhita, 2023	Other law
Electoral or communal deepfakes	s. 69A (blocking)	ss. 197, 353, 356	Representation of the People Act, 1951
AI-assisted hacking or malware	ss. 43, 66, 66F, 70	s. 111	CERT-In Directions, 2022
Unauthorised use of personal data for training or cloning	ss. 66C, 72A	s. 319	DPDP Act, 2023, ss. 8, 33
Commercial use of a celebrity's name or likeness	ss. 66C, 66D	s. 319	Copyright Act, 1957, ss. 38A, 38B; common-law personality rights

A. The Information Technology Act, 2000

The IT Act is still the backbone of India's cyber law.³⁷ Section 66C punishes the fraudulent use of another person's electronic signature, password or "any other unique identification feature", which arguably includes a person's voice or facial biometrics. Section 66D punishes cheating by personation using a computer resource and is among the provisions most frequently invoked in deepfake and voice-clone fraud. Section 66E prohibits capturing or transmitting images of a person's private area without consent, and ss. 67, 67A and 67B deal with obscene, sexually explicit and child sexual abuse material in electronic form. Sections 75, 79, 84B and 85 deal respectively with extraterritorial application, intermediary safe harbour, abetment and offences by companies.

The Act has three limitations in the AI context. First, its offences are framed around a human actor "using a computer resource", not around autonomous or generative systems. Secondly, the principal fraud-related offences carry a maximum of three years' imprisonment and are therefore bailable,³⁸ a penalty structure that grossly underestimates the industrial scale on which such fraud now occurs. Thirdly, s. 66E covers only actual images of a private area, so synthetic imagery that was never captured at all does not fall squarely within it.

³⁷The Information Technology Act, 2000 (Act 21 of 2000), ss. 43, 66, 66C, 66D, 66E, 66F, 67, 67A, 67B, 75, 79, 84B and 85.

³⁸*Id.*, s. 77B.

B. The Bharatiya Nyaya Sanhita, 2023

The BNS defines "document" to include electronic and digital records, so the forgery of AI-generated court orders or identity documents falls under ss. 336 and 340.³⁹ Section 111 includes "cyber-crimes" committed by organised crime syndicates within the offence of organised crime, a serious offence of particular relevance to the scam compounds that conduct AI-driven fraud from overseas. Cheating by personation (s. 319), personating a public servant (s. 204), extortion (s. 308), defamation (s. 356), voyeurism (s. 77) and stalking (s. 78) can all be committed with the help of AI. The Sanhita also applies to any person outside India who commits an offence targeting a computer resource located in India.⁴⁰ It is worth noting, however, that the BNS does not mention synthetic media anywhere, and all its offences require proof of a human mental element.

C. The Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023

The BNSS strengthens the procedural framework for digital offences. It allows FIRs to be lodged electronically and registered irrespective of territorial jurisdiction, makes forensic investigation at the crime scene compulsory for offences punishable with seven years' imprisonment or more, provides for summons to produce electronic communication devices and permits proceedings in electronic mode.⁴¹ The BSA treats electronic records as documents and primary evidence, and requires a certificate in the prescribed form, one part of which is signed by an expert, for the admission of electronic records.⁴² These provisions create the legal channel through which synthetic media enters a court, but they do not say how its authenticity is to be tested.

D. The Digital Personal Data Protection Act, 2023

The DPDP Act requires data fiduciaries to adopt reasonable security safeguards and to report personal data breaches, and provides for penalties of up to ₹250 crore.⁴³ The Digital Personal Data Protection Rules, 2025, notified in November 2025, bring the Act into force in phases,

³⁹The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 2(8), 77, 78, 111, 204, 308, 318, 319, 336, 340 and 356.

⁴⁰*Id.*, s. 1(5)(c).

⁴¹The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), ss. 94, 173, 176(3) and 530.

⁴²The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 2(1)(d), 57, 61 and 63.

⁴³The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 3(c)(ii), 8(5), 8(6), 17(1)(c) and 33, read with the Schedule.

with the substantive obligations applying from May 2027.⁴⁴ Two features limit its value against AI-enabled crime. The Act does not apply to personal data made publicly available by the data principal, which places the photographs and voice clips that people post on social media, the raw material of most deepfakes, largely beyond its protection. It also exempts processing for the prevention, detection and investigation of offences, which raises additional concerns about AI-powered surveillance.

E. The IT Rules, 2021 and the 2026 amendments on synthetic content

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 are India's first binding regulation aimed at AI-generated content.⁴⁵ They define "synthetically generated information" as audio, visual or audio-visual information that is artificially or algorithmically created or modified so as to appear real and is likely to be perceived as indistinguishable from a natural person or real-world event, excluding routine good-faith editing and enhancement. Intermediaries offering tools that can generate such content must implement reasonable technical measures against unlawful use, label lawful synthetic content prominently, and embed permanent metadata or similar provenance markers, including a unique identifier, which users may not remove. Significant social media intermediaries must obtain a user declaration on whether content is synthetic and verify it through technical means. The amendments also shorten takedown timelines and provide that a platform which voluntarily removes unlawful content does not lose its safe harbour. In its own explanatory note, MeitY clarifies that text alone, such as a false article written by a chatbot, is not synthetically generated information.⁴⁶

F. Other instruments

The CERT-In Directions of April 28, 2022 oblige service providers and other entities to report specified cyber incidents within six hours and to maintain logs for 180 days.⁴⁷ The

⁴⁴The Digital Personal Data Protection Rules, 2025, notified by the Ministry of Electronics and Information Technology in November 2025; "Enforcement of the DPDP Act and Notification of the DPDP Rules", *Shardul Amarchand Mangaldas & Co.*, November 27, 2025, available at: <https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/> (last visited on October 4, 2026).

⁴⁵*Supra* note 9, rr. 2(1)(wa) and 3.

⁴⁶Ministry of Electronics and Information Technology, *Frequently Asked Questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026* (Government of India, New Delhi, 2026), available at: <https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf> (last visited on October 4, 2026).

⁴⁷Indian Computer Emergency Response Team, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000, No. 20(3)/2022-CERT-In, dated April 28, 2022.

Telecommunications Act, 2023 prohibits obtaining SIM cards by deception and the misleading use of telecommunication identifiers.⁴⁸ Against voice clones and deepfakes of public figures, performers' rights under the Copyright Act, 1957 and the common-law right of personality are also invoked.⁴⁹ Finally, the India AI Governance Guidelines lay down seven principles and propose an AI Governance Group, a Technology and Policy Expert Committee and an AI Safety Institute, but they are voluntary and create no offences.⁵⁰

V. The Judicial Response

Indian courts have yet to decide a criminal case turning on the autonomous behaviour of an AI system. Their decisions nonetheless shape the field on four fronts: speech and intermediary liability; privacy; electronic evidence; and, most recently, personality rights and synthetic fraud.

A. Speech, intermediaries and the bounds of proactive policing

In *Shreya Singhal v. Union of India*, the Supreme Court struck down s. 66A of the IT Act because its vague terms, such as "annoyance" and "inconvenience", could sweep in protected speech, and it read down s. 79 so that an intermediary obtains "actual knowledge" only through a court order or a notification by the appropriate government.⁵¹ This holding remains relevant to any effort to make platforms or AI providers police synthetic content on their own. However, in *Sabu Mathew George v. Union of India*, the Court directed search engines to implement auto-blocking of advertisements for sex determination, acknowledging that technical filtering may be required where a statute prohibits specific content.⁵² In *Google India Private Limited v. Visakha Industries*, the Court held that s. 79 as it stood before 2009 did not protect intermediaries against criminal defamation, illustrating that safe harbour is a statutory privilege whose scope depends on its precise text.⁵³ The 2026 rules on synthetic content will be tested against these precedents.

B. Privacy and proportionality

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court held that privacy,

⁴⁸The Telecommunications Act, 2023 (Act 44 of 2023), s. 42.

⁴⁹The Copyright Act, 1957 (Act 14 of 1957), ss. 38A and 38B.

⁵⁰*Supra* note 8.

⁵¹*Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁵²*Sabu Mathew George v. Union of India*, (2018) 3 SCC 229.

⁵³*Google India Private Limited v. Visakha Industries*, (2020) 4 SCC 162.

including informational privacy and the right to control one's image and identity, is a fundamental right under Article 21, and that any State interference must satisfy the tests of legality, legitimate aim and proportionality.⁵⁴ This ruling provides constitutional support for treating non-consensual deepfakes as an infringement of dignity and privacy. It also restrains the State from using AI for mass surveillance, facial recognition and predictive policing in the name of combating cybercrime.

C. Electronic evidence

In *Anvar P.V. v. P.K. Basheer*, the Court ruled that secondary electronic evidence cannot be admitted without the certificate prescribed under s. 65B of the Indian Evidence Act, 1872,⁵⁵ and a three-judge Bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* affirmed that the certificate is mandatory unless the original device is produced.⁵⁶ This requirement is now reflected in s. 63 of the BSA, with an additional expert component. These decisions were designed to preserve the integrity of a record's source, not to determine whether it depicts the truth. A fully certified video may still be a deepfake.

D. Personality rights and AI-generated likeness

The High Courts have evolved a robust civil jurisprudence against the misappropriation of a person's identity through AI. In *Amitabh Bachchan v. Rajat Nagi*, the Delhi High Court granted an omnibus injunction against unauthorised use of the actor's name, voice and likeness,⁵⁷ and in *Anil Kapoor v. Simply Life India* it expressly restrained the use of AI tools, deepfakes and face-morphing to misappropriate the actor's persona.⁵⁸ In *Arijit Singh v. Codible Ventures LLP*, the Bombay High Court restrained AI platforms from cloning the singer's voice, noting the threat to a performer's livelihood.⁵⁹ In 2025 the Delhi High Court went further, granting a "dynamic+" injunction in *Sadhguru Jagadish Vasudev v. Igor Isakov* against deepfake videos used to promote scams,⁶⁰ and, in *Aishwarya Rai Bachchan v. Aishwaryaworld.com*, directing the removal of AI-generated sexual content and deepfakes while holding that unauthorised appropriation of a person's identity violates the right to live with dignity.⁶¹ These remedies are

⁵⁴*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

⁵⁵*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

⁵⁶*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

⁵⁷*Amitabh Bachchan v. Rajat Nagi*, 2022 SCC OnLine Del 4110.

⁵⁸*Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914.

⁵⁹*Arijit Singh v. Codible Ventures LLP*, 2024 SCC OnLine Bom 2445.

⁶⁰*Sadhguru Jagadish Vasudev v. Igor Isakov*, 2025 SCC OnLine Del 3804.

⁶¹*Aishwarya Rai Bachchan v. Aishwaryaworld.com*, CS(COMM) 956/2025, order dated September 9, 2025 (Delhi High Court).

quick, but they are civil in nature, available mainly to public figures with the resources to litigate, and dependent on platform compliance.

E. "Digital arrest" and the supervisory role of the Supreme Court

The suo motu proceedings in *In Re: Victims of Digital Arrest Related to Forged Documents* are among the most important judicial engagements with technology-enabled fraud. The Court has entrusted the investigation to the CBI, allowed it to probe the role of bank officials in opening mule accounts under the Prevention of Corruption Act, 1988, directed intermediaries to hand over traffic and content data, and permitted the freezing of accounts traceable to cybercrime even without an FIR.⁶² In July 2026, the Court suggested that Parliament define "digital arrest" in the penal law as a distinct offence carrying harsher punishment.⁶³ This is a clear judicial signal that the general offences of cheating and extortion no longer adequately reflect the seriousness of technology-facilitated impersonation.

F. Corporate criminal liability

The law on corporate criminal liability is central because AI systems are developed and deployed by companies. In *Standard Chartered Bank v. Directorate of Enforcement* and *Iridium India Telecom Ltd. v. Motorola Inc.*, the Supreme Court held that a company can be prosecuted and that the mental state of the persons who control it can be attributed to the company.⁶⁴ In *Aneeta Hada v. Godfather Travels and Tours Private Limited*, however, the Court ruled that a director can be prosecuted vicariously only if the company itself is arraigned as an accused.⁶⁵ These principles determine whether, and in what circumstances, an AI developer or deployer could be held criminally liable for foreseeable misuse of its system.

VI. Legal Issues and Concerns

A. The definitional vacuum

No Indian statute defines artificial intelligence, a deepfake or AI-generated content. The definition of "synthetically generated information" appears only in subordinate legislation directed at intermediaries rather than offenders, and it omits text entirely. Prosecutors must therefore fit AI-enabled conduct into general offences designed for human deception. This

⁶²*Supra* note 22.

⁶³*Supra* note 7.

⁶⁴*Standard Chartered Bank v. Directorate of Enforcement*, (2005) 4 SCC 530; *Iridium India Telecom Ltd. v. Motorola Inc.*, (2011) 1 SCC 74.

⁶⁵*Aneeta Hada v. Godfather Travels and Tours Private Limited*, (2012) 5 SCC 661.

leads to inconsistent registration: the same voice-clone crime may be prosecuted under s. 66D of the IT Act, under s. 319 of the BNS, or under both. A statutory vocabulary is necessary for framing specific offences, aggravating sentences and generating accurate crime statistics, since the NCRB cannot presently isolate AI-enabled cases.

B. Mens rea, attribution and the responsibility gap

Criminal liability is predicated on a guilty act and a guilty mind. Where a human uses AI as a tool, the AI is legally no different from a screwdriver, and the human's intention suffices. The challenge arises at either end of the chain. At one end, an agentic system may produce a harmful outcome that its user did not specifically intend, for example by generating false statements about another person or executing unauthorised transactions while pursuing an otherwise lawful goal. At the other end, a developer may release a model knowing that some users will misuse it, without knowing who, how or when. Neither situation fits the paradigms of dishonest intention and knowledge that are prerequisites for cheating and most IT Act offences respectively.⁶⁶

Indian law has partial tools. Under the doctrine of innocent agency, the AI acts merely as an extension of whoever directs it. Corporate criminal liability allows the intention of a company's directing mind to be imputed to the company, and s. 85 of the IT Act places liability on persons in charge of a company's business. Abetment under s. 84B of the IT Act and under the BNS may reach those who knowingly supply tools for committing crimes. What the law lacks is an offence of reckless or grossly negligent deployment of a high-risk AI system, which would criminalise culpable indifference without subjecting legitimate innovation to strict liability.

C. Responsibility of developers, deployers and intermediaries

It is unclear whether a generative AI provider is an "intermediary" at all. An intermediary under s. 2(1)(w) of the IT Act receives, stores or transmits records on behalf of another person, whereas a generative model creates new content in response to a prompt, behaving more like an author or publisher than a conduit. If it is not an intermediary, it cannot claim the safe harbour in s. 79; if it is, its obligations are limited to due diligence. The 2026 amendments sidestep the question by imposing obligations on intermediaries that "offer" tools for creating synthetic content, but subordinate legislation cannot determine a person's status under the parent Act.

⁶⁶*Supra* notes 6 and 16.

The amendments also sit uncomfortably with *Shreya Singhal*. Requiring platforms to verify user declarations through technical means, or to prevent unlawful synthetic content, may amount to the kind of proactive monitoring the Court warned against. Civil-society groups have criticised the definition as overbroad, the labelling requirements as compelled speech and the reliance on detection tools as technically unsound.⁶⁷ These are not arguments against regulation; they indicate that parliamentary legislation with clear standards is required, rather than an ever-expanding body of delegated rules.

D. Evidentiary challenges

AI creates a double problem of proof. Fabricated evidence may be offered as real, and genuine evidence may be dismissed as fabricated, a phenomenon Chesney and Citron call the "liar's dividend".⁶⁸ The certificate under s. 63 of the BSA concerns the origin and integrity of an electronic record, not whether its content reflects reality. Deepfake detection tools give probability-based outputs, are less accurate against newer generation techniques and have rarely been validated for Indian languages and faces. Courts will need standards for expert evidence on synthetic media, for the weight to be given to provenance metadata, and for allocating the burden of proof when a party alleges fabrication.

Institutional capacity aggravates the problem. Section 176(3) of the BNSS makes forensic investigation compulsory, adding pressure on laboratories already suffering from backlogs, and only a limited number of laboratories have been notified as Examiners of Electronic Evidence under s. 79A of the IT Act. The Centre has set up National Cyber Forensic Laboratories at New Delhi and in Assam and an evidentiary laboratory in Hyderabad, and has provided funding for State forensic capacity,⁶⁹ but these pale before the volume of digital evidence generated by over eighty thousand registered cybercrimes a year.

E. Jurisdiction and cross-border enforcement

Much AI-enabled fraud aimed at Indians originates in scam compounds in Southeast Asia, relies on servers in third countries and moves its proceeds through cryptocurrency. The Solicitor General informed the Supreme Court that digital arrest cases were originating from

⁶⁷Internet Freedom Foundation, "IT Intermediary Amendment Rules, 2026 contradict their purpose", February 12, 2026, available at: <https://internetfreedom.in/it-intermediary-amendment-rules-2026-contradict-their-purpose/> (last visited on October 4, 2026).

⁶⁸*Supra* note 26.

⁶⁹*Supra* note 11.

locations such as Myanmar and Thailand.⁷⁰ Section 75 of the IT Act and s. 1(5) of the BNS claim extraterritorial jurisdiction, but jurisdiction without cooperation is of little practical value. Mutual legal assistance is slow, and India is not a party to the Budapest Convention. India signed the United Nations Convention against Cybercrime on September 25, 2026, but ratification and implementing legislation are still needed before it can serve as a basis for cooperation.⁷¹

F. Penal proportionality

The three-year maximum for identity theft and cheating by personation under the IT Act, combined with bailability, does little to deter organised operations that defraud thousands of people. The BNS provides heavier penalties for cheating and organised crime, but there is no aggravating element for the use of AI or the synthetic impersonation of public authorities. The Supreme Court's suggestion of a separate "digital arrest" offence reflects this gap. At the same time, sentencing reform must avoid over-criminalising satire, parody, artistic use and research, which are legitimate uses protected under Article 19(1)(a).

G. Privacy, surveillance and due process

The fight against AI crime may itself undermine rights. Law-enforcement agencies increasingly use facial recognition, social-media analytics and predictive tools, and processing for the investigation of offences is exempt under the DPDP Act. Blocking powers under s. 69A and the shorter takedown timelines under the IT Rules create a danger of over-removal without notice or hearing. *Puttaswamy* demands that such restrictions be prescribed by law, serve a legitimate aim, be proportionate and be accompanied by procedural safeguards.⁷² An AI crime framework lacking independent oversight would merely substitute one harm for another.

H. Victims, gender and access to remedies

The current system favours the powerful. A celebrity can obtain a dynamic injunction within days, while an ordinary woman whose synthetic intimate image circulates on messaging groups

⁷⁰"Inclined to entrust CBI with investigation of all digital arrest cases: Supreme Court", *The Tribune*, October 27, 2025, available at: <https://www.tribuneindia.com/news/india/inclined-to-entrust-cbi-with-investigation-of-all-digital-arrest-cases-supreme-court/amp> (last visited on October 4, 2026).

⁷¹United Nations Convention against Cybercrime, adopted by General Assembly resolution 79/243 of December 24, 2024; "India Just Signed the World's First Global Cybercrime Treaty", *CyberPeace Foundation*, September 2026, available at: <https://cyberpeace.org/resources/blogs/india-just-signed-the-worlds-first-global-cybercrime-treaty-a-global-rulebook-for-a-borderless-crime> (last visited on October 4, 2026).

⁷²*Supra* note 49.

usually faces police reluctance, slow takedown and social ostracism. Stolen money can generally be recovered only if the victim reports quickly and the bank cooperates, and victims often need a court order to get their money back. Victim compensation under s. 396 of the BNSS is rarely invoked for cyber fraud. The Parliamentary Standing Committee on Home Affairs has recommended stronger prevention, coordination and capacity in its report on cybercrime,⁷³ yet a victim-centred, gender-sensitive procedure for AI-enabled abuse still does not exist.

I. Federalism and institutional capacity

"Police" and "public order" are State subjects under the Seventh Schedule, so the investigation of AI-enabled cybercrime depends on the uneven capability of State cyber cells. Coordination through the I4C, the National Cyber Crime Reporting Portal (NCRP) and the CBI's role in digital arrest cases helps, but it scarcely resolves the mismatch between nationally organised offending and locally organised policing. That cybercrime conviction rates remain in low single digits is the best evidence that substantive law is only part of the problem.

VII. Comparative and International Perspectives

No jurisdiction has a complete answer to AI-enabled crime, but Table 3 shows how the approaches of other jurisdictions can inform a model for India.

Table 3: Comparative frameworks for AI-driven crime

Jurisdiction	Key instruments	Approach	Lesson for India
European Union	Artificial Intelligence Act, Regulation (EU) 2024/1689	Horizontal, risk-based law; prohibited practices; transparency duty to disclose deepfakes; fines up to €35 million or 7% of global turnover	A statutory, risk-tiered framework provides legal certainty that delegated rules cannot

⁷³Department-related Parliamentary Standing Committee on Home Affairs, *Two Hundred Fifty-Fourth Report on Cyber Crime – Ramifications, Protection and Prevention* (Rajya Sabha Secretariat, New Delhi, 2025).

Jurisdiction	Key instruments	Approach	Lesson for India
United States	TAKE IT DOWN Act, 2025; FCC ruling on AI voices in robocalls, 2024; State deepfake laws	Harm-specific federal and State measures; platform takedown duties for intimate imagery	Targeted offences for the most serious harms can be enacted swiftly
United Kingdom	Online Safety Act 2023; Data (Use and Access) Act 2025	Platform duty of care; specific offences for sharing and creating intimate deepfakes	Creation, not only distribution, of non-consensual sexual deepfakes should be an offence
China	Deep Synthesis Provisions, 2023; Measures for Labelling AI-Generated Synthetic Content, 2025	Provider registration, real-name verification, mandatory explicit and implicit labels	Provenance and labelling work best when imposed at the generation stage
International	Budapest Convention, 2001; UN Convention against Cybercrime, 2024; Council of Europe Framework Convention on AI, 2024	Harmonised offences and cross-border evidence sharing; human-rights safeguards for AI	Ratification with domestic safeguards is needed to tackle transnational fraud

A. The European Union

The EU AI Act categorises AI systems by their level of risk. It bans certain practices outright, such as manipulative techniques that materially distort behaviour and cause significant harm, and the untargeted scraping of facial images to build recognition databases. It requires those who deploy systems capable of generating deepfakes to disclose that the content is artificially generated or manipulated, with exceptions for evidently artistic or satirical work and for

authorised law-enforcement use.⁷⁴ The Act is regulatory rather than criminal, leaving criminal offences to Member States, but its definitions and risk categories supply the vocabulary that India presently lacks.

B. The United States

The United States has no general AI statute. Instead, it has responded to specific harms. The TAKE IT DOWN Act of 2025 makes it an offence knowingly to publish non-consensual intimate imagery, including computer-generated "digital forgeries", and requires covered platforms to remove such content within forty-eight hours of a valid request.⁷⁵ In 2024, the Federal Communications Commission held that AI-generated voices are "artificial" voices under the Telephone Consumer Protection Act, making unsolicited voice-clone robocalls unlawful.⁷⁶ Many States have also adopted laws on election deepfakes and synthetic sexual imagery.

C. The United Kingdom

The Online Safety Act 2023 created duties of care for platforms and inserted offences into the Sexual Offences Act 2003 for sharing, or threatening to share, intimate photographs or films, including images that merely appear to show a person.⁷⁷ The Data (Use and Access) Act 2025 went further by criminalising the creation of a purported intimate image of an adult without consent.⁷⁸ The British model demonstrates that, for the most harmful categories, criminal law can target the act of creation and not only its dissemination.

D. China

China regulates synthetic media at the point where it is generated. The Deep Synthesis Provisions, effective from January 2023, require providers to verify users' identities, label synthetic content and retain records, while the Measures for Labelling AI-Generated Synthetic Content, effective from September 2025, call for both visible labels and embedded metadata.⁷⁹ India's 2026 amendments adopt the notion of embedded provenance, but without China's

⁷⁴*Supra* note 10, arts. 5, 50 and 99.

⁷⁵Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), Pub. L. No. 119-12 (2025) (United States).

⁷⁶Federal Communications Commission, *Declaratory Ruling in the Matter of Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, CG Docket No. 23-362, FCC 24-17 (February 8, 2024).

⁷⁷Online Safety Act 2023 (United Kingdom), s. 188, inserting s. 66B into the Sexual Offences Act 2003.

⁷⁸Data (Use and Access) Act 2025 (United Kingdom).

⁷⁹Cyberspace Administration of China, Provisions on the Administration of Deep Synthesis of Internet-based Information Services (effective January 10, 2023); Cyberspace Administration of China and others, Measures for Labelling Artificial Intelligence-Generated Synthetic Content (effective September 1, 2025).

licensing model, which would be difficult to reconcile with Indian constitutional protections for speech and privacy.

E. International instruments

Although the Budapest Convention of 2001 remains the most important treaty on substantive cyber offences and evidence exchange, India has declined to accede to it, partly because it was negotiated without India's participation.⁸⁰ The United Nations Convention against Cybercrime, adopted by the General Assembly on December 24, 2024 and opened for signature in Hanoi in October 2025, is the first universal treaty on cybercrime and electronic evidence.⁸¹ India's signature in September 2026 is significant, but rights organisations have warned that the Convention's wide powers of cooperation must be balanced by strong domestic safeguards. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, opened for signature in 2024, complements this with a rights-based approach.⁸²

VIII. Recommendations

India need not abandon its technology-neutral offences, which already cover most AI-aided conduct. What it requires is focused legislation, procedural reform and institutional capacity that fill the gaps discussed in Part VI.

- 1. Enact statutory definitions.** The IT Act, or its proposed successor, the Digital India Act, should define "artificial intelligence system", "synthetic media" and "deepfake", so that offences, labelling duties and crime statistics share a common vocabulary that also covers text-based deception.
- 2. Create targeted offences.** New offences should cover (a) making or disseminating non-consensual synthetic sexual imagery, whether or not a real image was captured; (b) impersonating a public authority, court or investigating agency through synthetic media, including "digital arrest", as an aggravated offence; and (c) knowingly supplying AI tools designed or marketed for committing offences. Satire, parody, scholarship and journalism should be expressly protected.

⁸⁰Council of Europe, Convention on Cybercrime, ETS No. 185 (Budapest, November 23, 2001).

⁸¹United Nations Office of Legal Affairs, "The United Nations Convention against Cybercrime opens for signature in Hanoi", October 2025, available at: <https://www.un.org/ola/en/news/united-nations-convention-against-cybercrime-opens-signature-hanoi> (last visited on October 4, 2026).

⁸²Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 (Vilnius, September 5, 2024).

3. **Treat AI-use as an aggravating factor.** Committing cheating, extortion, forgery or organised crime at scale with the aid of AI should be a statutory aggravating circumstance, and the maximum punishment under ss. 66C and 66D of the IT Act should be revisited for organised, high-value or repeat offending.
4. **Clarify developer and deployer liability.** Legislation should define when generative AI providers qualify as intermediaries, impose risk-based duties of care on providers of high-risk systems, and make it an offence recklessly to deploy a high-risk AI system that causes death or other serious harm, with a due-diligence defence for those who follow recognised safety standards.
5. **Give provenance and labelling a statutory footing.** The labelling and metadata obligations now found in the IT Rules should be moved into primary legislation, aligned with open technical standards for content provenance, and accompanied by independent review of detection accuracy.
6. **Update the law of evidence for synthetic media.** The BSA should be supplemented by rules on authenticating audio-visual evidence, weighing provenance metadata and dealing with allegations that evidence is synthetic. More laboratories should be notified as Examiners of Electronic Evidence under s. 79A of the IT Act, with dedicated deepfake-forensics units.
7. **Strengthen investigative capacity.** Every district should have a trained cyber police station, State forensic laboratories should receive ring-fenced funding, and the police should be equipped with AI tools for detecting mule accounts, synthetic media and coordinated fraud, subject to audit and oversight.
8. **Build victim-centred remedies.** Victims should be able to request the removal of synthetic intimate imagery through a single national window, with hash-matching across platforms completed within hours. Banks should follow a uniform, time-bound refund procedure, and courts should invoke victim compensation under s. 396 of the BNSS more extensively.
9. **Complete international engagement.** India should ratify the UN Convention against Cybercrime with domestic safeguards for privacy and free expression, conclude arrangements with the countries where scam compounds are located, and negotiate faster data-sharing agreements with major platform jurisdictions.
10. **Protect rights within the framework.** Every new power to block, surveil or police with the aid of AI should satisfy the *Puttaswamy* test of legality, necessity and

proportionality, with notice, reasoned decisions, independent review and periodic transparency reports.

- 11. Invest in awareness and research.** Public campaigns should build simple verification habits, such as call-back protocols and family code words, and the NCRB should record AI-enabled offences as a separate category to support evidence-based policy.

IX. Conclusion

AI has not so much created new wrongs as industrialised age-old ones. Cheating, extortion, forgery, sexual exploitation and defamation now occur at a scale, speed and level of realism beyond anything India's cyber law, built largely between 2000 and 2008, was designed to address. The new criminal laws of 2023, the DPDP Act and the 2026 amendments on synthetic content are welcome steps, and Indian courts have shown judicial creativity in safeguarding dignity and personality against AI misuse. Yet the framework remains piecemeal, rests heavily on delegated legislation, is uncertain about who is liable when AI is built and deployed, and is weak in proof, cross-border enforcement and victim support.

This paper argues that India should move from a strictly technology-neutral approach to a calibrated, harm-specific one. That means statutory definitions of AI and synthetic media, a narrow set of targeted offences and aggravating factors, risk-based obligations for developers and deployers, up-to-date rules of evidence, and a substantial increase in forensic and investigative capacity. These steps must be grounded in constitutional protections of privacy, dignity and freedom of expression, so that the response to AI-facilitated crime does not itself create arbitrary power. Only if these reforms proceed together can India's legal system keep pace with a technology that would otherwise continue to outstrip it.