INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE WEAPONISATION OF ARTIFICIAL INTELLIGENCE IN DAILY LIFE FINTECH CRIMES: AN EXHAUSTIVE ANALYSIS OF THE INDIAN LANDSCAPE (2024-2025)

AUTHOR - PROF. (DR.) SHEPHALI YADAV* & PRADEEP KUMAR SINGH**

* HEAD & DEAN, FACULTY OF LAW, DR. SHAKUNTALA MISRA NATIONAL REHABILITATION UNIVERSITY, LUCKNOW

** RESEARCH SCHOLAR, FACULTY OF LAW, DR. SHAKUNTALA MISRA NATIONAL REHABILITATION UNIVERSITY, LUCKNOW

BEST CITATION - PROF. (DR.) SHEPHALI YADAV & PRADEEP KUMAR SINGH, THE WEAPONISATION OF ARTIFICIAL INTELLIGENCE IN DAILY LIFE FINTECH CRIMES: AN EXHAUSTIVE ANALYSIS OF THE INDIAN LANDSCAPE (2024-2025), INDIAN *JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (14) OF 2025, PG. 1060-1072, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The rapid adoption of Artificial Intelligence (AI) in the financial technology (FinTech) sector has led to two primary outcomes in India. While AI has improved financial inclusion, speed, and efficiency, it has also enabled criminals to carry out more advanced and automated financial crimes. This paper examines the role of AI in the rise of everyday FinTech-related crimes in India during the period 2024–2025. The proliferation of Fraud-as-a-Service (FaaS) platforms, the growing use of deepfake technology in 'Digital Arrest' schemes, and the sociological problem of cyber-slavery in Southeast Asia, which facilitates extensive online fraud operations, are among the major trends that are the focus of this study. It also analyses India's current legal and regulatory framework, including the Digital Personal Data Protection (DPDP) Act, 2023, the Bharatiya Nyaya Sanhita (BNS), 2023, and RBI guidelines and compares them with global standards such as the European Union AI Act. The paper identifies significant gaps in Indian laws regarding AI-driven financial crimes. To increase resilience against risks facilitated by AI, the report suggests technological, legal, and societal measures in its conclusion. According to the report, human trust and perception are now the primary targets of contemporary cybercrime, indicating that knowledge and regulation are equally crucial as technological defences.

Keywords: *Artificial Intelligence, FinTech Crime, Deepfakes, Digital Arrest, Fraud-as-a-Service, Money Laundering, Cyber Slavery, RBI Guidelines, DPDP Act.*

1. Introduction: The Algorithmic Shift in Financial Crime

With a projected market capitalisation of $150 billion by 2025, the Indian FinTech industry is a global model of successful digital public infrastructure. [2080] More than 530 million previously unbanked people now have easier access to banking thanks to programs like the Jan Dhan Yojana and the Unified Payments Interface (UPI), which have created a digital footprint comparable to that of the entire European Union.[2081] Driven by the Jan Dhan-Aadhaar-Mobile (JAM) trinity, this significant change has brought millions of people into the formal economy, simplifying direct benefit payments and providing real-time, round-the-

[2080] "India Fintech Market Size, Share & 2030 Trends Report," *Mordor Intelligence*, 2025*available at*: https://www.mordorintelligence.com/industry-reports/india-fintech-market (last visited December 24, 2025).

[2081] *Global Fintech Fest 2024*,.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

clock financial services in both rural and urban areas.

However, this rapid digitisation has expanded the attack surface for financial crimes, transitioning the threat landscape from rudimentary phishing attempts—characterised by grammatical errors and blatant deceit—to highly sophisticated, AI-driven social engineering attacks. The period between 2024 and 2025 marks a critical inflexion point where 'daily life' financial crimes—scams targeting individuals in their homes via personal devices—have been industrialised through Artificial Intelligence. The sophistication of these attacks is no longer defined by the hacker's coding ability but by their access to Generative AI (GenAI) tools capable of mimicking human behaviour, voice, and appearance with high fidelity.

1.1 The Democratisation of Deception

The integration of AI into criminal workflows represents a 'democratisation of deception'. Previously, executing a convincing voice phishing attack required a skilled actor who could mimic authority or a specific dialect. Today, the rise of Large Language Models (LLMs) allows fraudsters to generate grammatically perfect, context-aware phishing scripts in multiple regional Indian languages, effectively overcoming the linguistic barriers that previously served as red flags for potential victims.[2082]

Furthermore, the commercialisation of 'Fraud-as-a-Service' (FaaS) on encrypted platforms like Telegram has turned cybercrime into a modular industry. In this underground economy, specific AI tools—such as those for real-time face swapping or voice cloning—can be rented for nominal fees, thereby lowering the barrier to entry for non-technical criminals.[2083] This has led to a proliferation of attacks that are not only more convincing but also scalable, allowing small criminal groups to target thousands of individuals simultaneously with personalised, AI-generated narratives.

1.2 The Scope of the Crisis

The financial and psychological toll of this algorithmic crime wave is staggering and growing exponentially. In the first quarter of 2024 alone, reports indicate that Indians lost approximately ₹120.30 crore specifically to 'digital arrest' scams, a particularly pernicious form of coercion facilitated by digital tools.[2084] The broader landscape of digital fraud is even more alarming; the Reserve Bank of India (RBI) reported that fraud losses in the first half of the fiscal year ending March 2024 grew by a factor of eight compared to the previous year, amounting to over ₹21,000 crore.[2085]

These figures, while shocking, likely represent only a fraction of the actual cost. The nature of these crimes—often involving humiliating scenarios such as accusations of involvement in pornography or narcotics rings—leads to significant underreporting due to victim shame and social stigma. Consequently, the actual economic impact of AI-enabled FinTech crime in India may be significantly higher than official statistics suggest, threatening not only individual financial stability but also the aggregate trust in India's digital financial ecosystem.

2. The Technological Arsenal: Mechanisms of AI-Driven Deception

The application of AI in financial crime has evolved from passive data harvesting to active, real-time impersonation and manipulation. This section dissects the primary technological mechanisms employed by syndicates to breach the 'human firewall', categorising them by the specific AI modalities utilised.

[2082] Mar Negreiro, 'Scam calls in times of Generative AI' (2025).
[2083] Jill Robb, "Emerging Threats of AI-Enabled Fraud in 2025" *Point Predictive*, 2025*available at*: https://pointpredictive.com/emerging-threats-of-ai-enabled-fraud/ (last visited December 14, 2025).
[2084] Rohin Pujari, "India - From Clicks To Cuffs: Understanding Digital Arrest In The Indian Legal Landscapes." *Conventus Law*, 2025*available at*: https://conventuslaw.com/report/india-from-clicks-to-cuffs-understanding-digital-arrest-in-the-indian-legal-landscapes/ (last visited December 14, 2025).
[2085] "Data shows Indian fraud cases tripled in 2024, "*available at*: https://www.biocatch.com/press-release/indian-fraud-cases-tripled-in-2024 (last visited December 14, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

2.1 Generative AI and Deepfakes: The Erosion of Sensory Trust

The most potent weapon in the modern fraudster's arsenal is the deepfake—synthetic media generated by neural networks such as Generative Adversarial Networks (GANs). These systems consist of two competing neural networks: a generator that creates fake content and a discriminator that attempts to distinguish it from real content. Through millions of iterations, the generator learns to produce images, video, and audio that are indistinguishable from reality to the human eye and ear.

2.1.1 Video Deepfakes and Real-Time Impersonation

Deepfake video technology has graduated from pre-rendered clips to real-time applications. Fraudsters now utilise 'live swap' software that allows them to superimpose the faces of trusted authority figures—such as police officers, judges, or bank executives—onto their own faces during live video calls.

In high-profile instances within India, fraudsters have impersonated the Chief Justice of India, DY Chandrachud, conducting fake virtual court hearings to intimidate victims into transferring funds.[2086] These 'digital arrests' rely heavily on the visual authority of the impersonated official to induce a state of panic, bypassing the victim's rational scrutiny. The technology has advanced to the point where real-time video manipulation is possible with minimal latency, allowing scammers to nod, speak, and react naturally during a video call, creating a 'hyper-realistic' deception that is extremely difficult for an untrained individual to detect.

2.1.2 Voice Cloning (Vishing 2.0)

Traditional voice phishing (vishing) involved human actors attempting to sound authoritative or distressed. AI-enabled vishing utilises voice synthesis tools (e.g., Vall-E, ElevenLabs) to clone a specific person's voice using as little as three seconds of sample audio.[2087] This capability has birthed two distinct and highly effective scam typologies:

1. **The 'Grandparent' Scam:** Criminals scrape short audio clips of a victim's relative from social media (Instagram Stories, Facebook videos). They use this audio to clone the relative's voice and call the victim, claiming a crisis—such as an accident, arrest, or kidnapping—and demanding immediate financial assistance. The familiarity of the voice bypasses the victim's skepticism.
2. **Executive Impersonation:** In the corporate sector, AI voice clones of CEOs or CFOs are used to authorise fraudulent wire transfers. This 'Deepfake Executive Fraud' represents an evolved variant of Business Email Compromise (BEC), moving from text-based deception to audio-visual manipulation. In one global instance, a finance director was tricked into wiring $25 million after a video call where every other participant was a deepfake of his colleagues.[2088]

2.2 AI-Enhanced Social Engineering and Phishing

Beyond sensory manipulation, AI has revolutionised the scale, personalisation, and efficacy of social engineering—the psychological manipulation of people into performing actions or divulging confidential information.

- **Polymorphic Phishing:** Traditional phishing emails often share common signatures (text patterns, subject lines) that spam filters can easily block. Generative AI tools can now create thousands of unique variations of a phishing email, altering the syntax and structure while retaining the

[2086] Dwayne Oxford, "What are digital arrests, the newest deepfake tool used by cybercriminals?" *Al Jazeeraavailable at*: https://www.aljazeera.com/news/2024/10/11/what-are-digital-arrests-the-newest-deepfake-tool-used-by-cybercriminals (last visited December 14, 2025).

[2087] "The Anatomy of a Deepfake Voice Phishing Attack: How AI-Generated Voices Are Powering the Next Wave of Scams," *Group-IBavailable at*: https://www.group-ib.com/blog/voice-deepfake-scams/ (last visited December 25, 2025).

[2088] Perry Carpenter, "AI, Deepfakes, and the Future of Financial Deception" (U.S. Securities and Exchange Commission, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

malicious intent. This 'polymorphic' nature allows attackers to evade signature-based detection systems.[2089]

- **Psychological Profiling and 'Spear Phishing':** By analysing data scraped from social media profiles (LinkedIn, Facebook, X), AI algorithms can build detailed psychological profiles of potential targets. They can identify a target's recent purchases, travel history, family connections, and professional stressors. This data is used to generate highly personalised 'spear phishing' messages that reference specific, credible details—such as a recent conference attended or a specific vendor used—to create a high-trust narrative.
- **Romance Chatbots and 'Pig Butchering':** Automated AI chatbots can maintain romantic relationships with thousands of victims simultaneously. These bots, powered by LLMs, can engage in deep, emotionally resonant conversations over months, 'grooming' the victim. Once trust is established, the conversation steers toward fraudulent investment schemes—a tactic known as 'pig butchering' (fattening the victim before slaughter). The AI ensures that the fraudster never forgets a detail about the victim's life, maintaining the illusion of a genuine connection.

2.3 Synthetic Identity Fraud

Criminals utilise AI to create 'synthetic identities' by combining honest (stolen) and fake information. This technique is particularly effective in bypassing Know Your Customer (KYC) regulations, which serve as gatekeepers to the formal financial system.

- **Generative ID Creation:** AI can generate realistic photographs of non-existent people or alter existing ID documents to match a different face. This allows fraudsters to open 'mule' bank accounts that are used to launder money, as the identity used to open the account does not actually exist or is a composite that cannot be traced to a single individual.[2090]
- **Morphing Attacks:** In a more advanced technique known as 'morphing,' an image is manipulated to resemble two different people simultaneously—the criminal and a legitimate ID holder. This allows a criminal to use a legitimate ID card to bypass facial recognition checks at automated border gates or digital banking onboarding systems.

[2089] Simon Moseley, "Automating Deception: AI's Evolving Role in Romance Fraud" *CETaS Briefing Papers* (2025).

[2090] "More than 50% of fraud involves the use of artificial intelligence," *Feedzaiavailable at*: https://www.feedzai.com/inthenews/more-than-50-of-fraud-involves-the-use-of-artificial-intelligence/ (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Table 1: Typology of AI-Enabled FinTech Crimes

Crime Category	AI Technology Used	Mechanism of Action	Target Outcome
Digital Arrest	Real-time Video Deepfakes (Face Swapping)	Impersonation of Law Enforcement (CBI/Police) on video calls.	Coerced transfer of life savings to 'verification' accounts.
Vishing 2.0	Voice Cloning / Text-to-Speech (TTS)	Cloning the voice of relatives or CEOs from short audio samples.	Emergency fund transfer or corporate wire fraud.
Pig Butchering	LLM-driven Chatbots / Sentiment Analysis	Long-term grooming via romantic/social scripts to build trust.	Investment in fake crypto platforms (high value).
Synthetic Identity	GANs (Image Generation) / Morphing	Creation of fake ID documents and faces for KYC bypass.	Creation of mule accounts for money laundering.
Phishing	LLMs (Text Generation)	Polymorphic email generation; translation to regional languages.	Credential harvesting (Banking passwords, OTPs).

3. The 'Digital Arrest' Epidemic: A Case Study in Psychological Warfare

The 'Digital Arrest' scam has emerged as the defining financial crime of the 2024-2025 period in India. It represents a convergence of technical capability (deepfakes) and sociological vulnerability (cultural deference to authority), resulting in a crime that is as much psychological as it is financial.

3.1 Anatomy of the Scam: The Script

The modus operandi of a Digital Arrest scam follows a consistent, chilling script designed to isolate the victim and induce a state of cognitive paralysis. The scam unfolds in distinct phases:[2091]

1. **The Trigger (The Hook):** The victim receives a call, often an automated IVR, claiming to be from a courier company (FedEx, DHL) or a telecom regulator (TRAI). The message states that a parcel addressed to the victim has been intercepted, containing illegal goods

[2091] "NITI AAYOG, India | Digital Arrest: The Modern-Day Cyber Scam by Major Sadhna Singh, Consultant, NITI Aayog," *available at*: https://www.niti.gov.in/node/1642 (last visited December 25, 2025); "Locked on Video: Inside India's Chilling Digital Arrest Scam | Tookitaki," *available at*: https://www.tookitaki.com/blog/locked-on-video-inside-indias-chilling-digital-arrest-scam (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

(MDMA drugs, fake passports, tiger skins) or that their mobile number/Aadhaar is linked to money laundering activities.

2. **The Escalation (Authority Transfer):** The call is quickly transferred to a 'higher official,' posing as an officer from the Central Bureau of Investigation (CBI), the Enforcement Directorate (ED), or the Narcotics Control Bureau. To establish credibility, the fraudsters may share forged ID cards and 'official' letters with the victim's correct personal details.
3. **The Digital Panopticon (Isolation):** The victim is coerced into joining a video call (typically via Skype or WhatsApp). They are ordered to keep their camera on 24/7, effectively placing them under 'digital house arrest.' They are strictly forbidden from contacting family, friends, or local police, under the threat that doing so would compromise 'national security' or lead to the immediate arrest of their loved ones.
4. **The Deepfake Theatre:** During the video call, the victim is presented with a curated environment. The background may resemble a police station or a courtroom. Deepfake technology is often used to simulate a high-ranking officer or even a judge conducting a 'hearing.' In some cases, a fake virtual court session is convened, complete with a deepfake of the Chief Justice of India delivering a 'verdict'.
5. **The Financial Extraction:** To 'prove their innocence,' 'verify their assets,' or post 'bail,' the victim is forced to transfer their funds—often their entire life savings—to a 'secret supervision account' or 'RBI verification account.' They are promised a refund after the verification is complete. Once the transfer is made, the screen goes black, and the money vanishes.

3.2 Real-Life Examples in the Indian Context

The prevalence of these scams is evidenced by numerous high-value cases reported across Indian metros:

- **The Bengaluru Case (₹32 Crore):** In one of the largest reported individual losses, a 57-year-old software engineer in Bengaluru was kept under digital surveillance for nearly six months. Fraudsters posing as CBI officials coerced her into making 187 bank transfers, resulting in a loss of ₹32 crore. The extended duration of this scam highlights the sophisticated psychological conditioning employed by the criminals.[2092]
- **The Vardhman Group Case (₹7 Crore):** The head of the Vardhman Group in Ludhiana was targeted in a virtual courtroom scam. The fraudsters used a deepfake of the Chief Justice of India, DY Chandrachud, in a fake Supreme Court hearing to legitimise their demands, leading to a loss of ₹7 crore. This case demonstrates that high-profile executives are as vulnerable as private individuals.[2093]
- **The 'Narco-Parcel' Scam (Chandigarh):** A woman in Chandigarh lost ₹11 lakh after being convinced her Aadhaar was linked to a narcotics parcel destined for Beijing. She was shown forged FIR documents and forced to transfer money as 'bail' while being monitored on video.[2094]
- **The Retired RBI Employee (Hyderabad):** Even those with financial literacy are not immune. A retired RBI employee transferred ₹49 lakh over several days, driven by the fear of immediate arrest and social reputation damage.[2095]

3.3 The Sociology of Victimhood: Why It Works

The effectiveness of the Digital Arrest scam lies in its exploitation of specific psychological and cultural vulnerabilities:

- **Authority Bias:** In the Indian cultural

[2092] "Bengaluru techie loses Rs 32 crore to fraudsters because of a parcel," *The Economic Times*, 17 November 2025.
[2093] "A Call, Digital Arrest, Rs 7 Crore Transferred: How Vardhman Boss Was Duped," *www.ndtv.com*.
[2094] "Digital Arrest Scam in India – Protect Yourself from Fraudsters," 2025*available at*: https://www.ujjivansfb.bank.in/banking-blogs/personal-finance/digital-arrest-scam-india (last visited December 25, 2025).
[2095] *Ibid.*

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

context, there is a deep-seated deference to, and fear of, law enforcement and judicial authority. The sight of a uniform or a courtroom setting triggers an automatic response to compliance.

- **The Amygdala Hijack:** By presenting an immediate, high-stakes threat (arrest, drug trafficking charges), the scammers induce a 'fight or flight' response. This physiological state, known as an amygdala hijack, overrides the prefrontal cortex—the part of the brain responsible for rational analysis and critical thinking. The victim is literally unable to think clearly.[2096]
- **Isolation:** By prohibiting the victim from speaking to others, scammers remove the 'reality check' mechanism. A spouse or friend might spot the fraud immediately, but in isolation, the victim's reality is entirely defined by the voice in the earphone.[2097]
- **Shame and Reputation:** The accusations often involve crimes with high social stigma (drugs, money laundering). The fear of public humiliation drives the victim to comply silently to 'make the problem go away'.[2098]

4. The Industrial Infrastructure of Crime: Fraud-as-a-Service (FaaS)

The rise of AI-enabled crime is not merely a collection of isolated incidents but the output of a robust, corporate-like underground economy. This 'Fraud-as-a-Service' (FaaS) model allows criminal syndicates to scale their operations globally.

4.1 The Telegram Ecosystem

Encrypted messaging apps, particularly Telegram, have become the primary marketplace for FaaS. The platform's anonymity and bot capabilities make it an ideal hosting ground for criminal vendors.

- **Marketplace Growth:** Monitoring of fraud channels on Telegram revealed a seven-fold increase in conversations related to AI and deepfakes between 2023 and 2024, growing from 47,000 to over 350,000 messages.[2099]
- **Service Offerings:** Vendors sell 'turnkey' fraud kits. For instance, 'Haotian AI' offers sophisticated face-changing software supported by a dedicated R&D team of programmers. Other services include 'Deepfake Voice Cloning' for executive impersonation and automated phishing bots that can bypass Two-Factor Authentication (2FA) by intercepting OTPs.
- **Recruitment and Organisation:** These channels are also used to recruit the 'workforce' for these scams. 'Coders' build the bots, 'Refunders' act as fake customer support agents, and 'Workers' are recruited to post ads or manage interactions. The structure mirrors a legitimate IT enterprise, complete with marketing teams, technical support, and even 'mentors' to train new scammers.

4.2 The Dark Web Economy

The tools and data required to commit these crimes are available for purchase on dark web marketplaces. The pricing reflects the commoditisation of cybercrime:

[2096] *Ibid.*
[2097] Alyxandra Cazanis et al., "Falling into a Black Hole: A Qualitative Exploration of the Lived Experiences of Cyberscam Victim-Survivors and Their Social Support Networks" *Victims & Offenders* 1–20 (2025).
[2098] Luke Balcombe, "The Mental Health Impacts of Internet Scams," 22 *International Journal of Environmental Research and Public Health* 938 (2025).
[2099] Jill Robb, "Emerging Threats of AI-Enabled Fraud in 2025" *Point Predictive*, 2025*available at*: https://pointpredictive.com/emerging-threats-of-ai-enabled-fraud/ (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Table 2: Dark Web Price Index for Cybercrime Assets (2025 Estimates)

Asset / Service	Estimated Price (USD)	Utility in FinTech Crime
Credit Card Details (with CVV)	$10 - $40	Direct theft; purchasing server infrastructure.
Online Bank Login (India)	$200 - $1,000+	Used as 'mule' accounts to receive stolen funds.
Verified Crypto Account (KYC'd)	$120 - $1,170	Converting stolen fiat currency into USDT/Bitcoin.
High-Quality Deepfake Video Service	$20 - $50 per minute	Creating custom videos for 'Digital Arrest' or CEO fraud.
Indian Aadhaar/PAN Database Dump	< $0.01 per record	Bulk data for targeting and psychological profiling.
AI Voice Cloning Tool (Subscription)	$20 - $30 / month	Generating audio for vishing and family emergency scams.

Source: Consolidated data from Privacy Affairs, Dark Web Price Index 2025, and Point Predictive.

4.3 The Mule Account Economy

Money laundering is the lifeblood of these scams. The proceeds of crime are layered through a web of 'mule accounts'—bank accounts rented or stolen from legitimate users.

- **Recruitment:** Recruiters target vulnerable populations—students, the unemployed, and individuals in rural areas—offering commissions (typically 5-10%) for 'renting' their bank accounts. These account holders often unwittingly become accomplices to federal crimes.
- **Layering and Integration:** Funds are rapidly moved through multiple domestic accounts to obfuscate the trail. Finally, the money is converted into cryptocurrency (primarily USDT) via P2P exchanges and transferred to wallets controlled by syndicates abroad, making recovery by Indian law enforcement nearly impossible due to jurisdictional boundaries.[2100]

5. Geopolitics of Fraud: 'Digital Slavery' and Cross-Border Syndicates

The operational hubs for these crimes have shifted from domestic hotspots to transnational compounds, creating a complex humanitarian and law enforcement challenge that extends beyond India's borders.

5.1 The 'Golden Triangle' Scam Compounds

A significant portion of the 'Digital Arrest' and investment scams targeting Indians originates from Southeast Asia—specifically the lawless border regions of Cambodia, Myanmar, and Laos (the 'Golden Triangle').

- **Cyber Slavery:** Thousands of Indian

[2100] "Lucknow's 'mule account' menace: How local youths are fuelling global cyber fraud network," *TaxTMIavailable at*: https://www.taxtmi.com/news?id=52067 (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

nationals have been lured to these countries with promises of high-paying tech jobs (e.g., 'Data Entry Operators' or 'Customer Support Executives' in Thailand). Upon arrival, they are trafficked across borders into militarised compounds (e.g., KK Park in Myanmar) controlled by Chinese syndicates.[2101]

- **Forced Criminality:** These victims are stripped of their passports and forced to work 12-14 hours a day, perpetrating cyber fraud against their own fellow citizens. They act as the 'face' or 'voice' of the scam, reading scripts generated by AI. Victims who fail to meet financial targets face brutal punishment, including physical torture, starvation, and electric shocks.[2102]
- **Scale:** The UN estimates that over 100,000 people are trapped in scam centres in Myanmar alone, with another 100,000 in Cambodia. While Indian agencies have repatriated hundreds, thousands remain trapped in what is termed 'digital slavery,' coerced into fueling the very crime wave targeting India.[2103]

5.2 Domestic Hotspots: The 'New Jamtara'

Within India, the geography of cybercrime is also shifting. While Jamtara in Jharkhand was the original hub of phishing, new epicenters have emerged.

- **The Mewat-Mathura-Bharatpur Triangle:** This region, straddling the borders of Haryana, Uttar Pradesh, and Rajasthan, has overtaken Jamtara as the new capital of cyber fraud. The area is characterised by low literacy rates and high youth unemployment, driving populations toward cybercrime as a primary livelihood.[2104]
- **Operational Advantages:** The region's unique location at the tri-junction of three states creates a 'black spot' for mobile networks and law enforcement jurisdiction. Criminals can easily cross state lines to evade local police, and mobile signals often bounce between towers in different states, making precise geolocation difficult.[2105]
- **Specialisation:** Unlike Jamtara's focus on simple KYC fraud, gangs in the Mewat region have specialised in 'sextortion' and blackmail, utilising AI tools to morph victims' faces onto pornographic clips to extort money.

6. Regulatory Landscape and Policy Gaps

India's legal and regulatory response to AI-driven financial crime is a patchwork of evolving statutes and guidelines. While governance frameworks are strengthening, significant gaps remain in addressing the specific nuances of Generative AI.

6.1 The Reserve Bank of India (RBI) Response

The RBI has established a robust governance framework for digital finance, but it lacks specific technical safeguards to address AI-driven threats.

- **Governance Strengths:** The *Master Direction on Digital Lending (2025)* and *Outsourcing Guidelines* enforce strict accountability. Regulated entities (REs) are held strictly liable for the actions of their Lending Service Providers (LSPs) or outsourcing vendors. The guidelines also mandate clear audit trails and prohibit the use of 'dark patterns' in digital lending interfaces.
- **Technical Weaknesses:** However, the framework largely fails to implement specific technical and model-level safeguards. There is a critical lack of binding requirements for:

[2101] *India Repatriates 270 Citizens Who Fled Myanmar Cyber Scam Hub | Vantage With Palki Sharma*, 2025.
[2102] *Miraculous Story of 7 Indians Who Escaped from a Cambodia Scam after Days of Torture*, 2025.
[2103] *India Repatriates 270 Citizens Who Fled Myanmar Cyber Scam Hub | Vantage With Palki Sharma*, 2025.
[2104] Admin, "Anatomy of Violence in the Hithero peaceful Nuh" *Centre for Study of Society and Secularism*, 2023*available at*: https://csss-isla.com/fact-finding-reports/anatomy-of-violence-in-the-hithero-peaceful-nuh/ (last visited December 25, 2025).
[2105] "Techie murder: Snatched phones used for frauds," *The Times of India*, 24 November 2020.

- Mandatory algorithmic fairness audits to detect bias.
- Model robustness testing against adversarial attacks (data poisoning).
- Specific technical controls to detect deepfakes during Video Customer Identification Processes (V-CIP).
- The RBI's focus remains heavily on *process* governance rather than *technology* verification.

6.2 The Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act is India's primary data protection law, but its application to AI is limited compared to global standards, such as the GDPR.

- **Consent Framework:** The Act requires informed consent for the processing of personal data, which technically encompasses biometric data used to create deepfakes.
- **Critical Gaps:**
  - **Automated Decision Making:** Unlike the GDPR, the DPDP Act does not explicitly regulate 'automated decision-making' or provide a 'right to explanation' for AI-driven decisions. This leaves individuals with limited recourse if an AI model unfairly denies them credit or flags them for fraud.
  - **Publicly Available Data:** The Act exempts personal data made publicly available by the user. This creates a significant loophole for AI companies and fraudsters to scrape social media data (photos, voice clips) to train deepfake models without consent.

6.3 Criminal Law: IT Act vs. Bharatiya Nyaya Sanhita (BNS)

- **Information Technology (IT) Act, 2000:** Sections 66C (identity theft) and 66D (cheating by impersonation) are the primary tools used to prosecute online fraud. However, the Act predates modern AI and lacks specific provisions defining or criminalising the creation of synthetic media.
- **Bharatiya Nyaya Sanhita (BNS), 2023:** The new criminal code, replacing the IPC, includes provisions for 'forgery' and 'defamation' (Section 356) that can be applied to deepfakes. However, proving the 'intent to harm' via synthetic media remains legally complex, and there is no specific section addressing 'digital arrest' or 'virtual impersonation'.

6.4 Comparative Analysis: India vs. EU AI Act

The European Union's AI Act represents the global gold standard for AI regulation. A comparison highlights the areas where India's framework requires strengthening.

Table 3: Regulatory Comparison - India vs. EU on AI & Deepfakes

Feature	EU AI Act (Article 50)	India (DPDP Act / IT Act / BNS)	Gap Analysis
Transparency	Mandates distinct labelling/watermarking of all AI-generated content (deepfakes).	No explicit mandate for labelling synthetic content. Advisory only.	High risk of user deception in India due to a lack of visual warnings.
High-Risk AI	Strict conformity assessments for AI	No specific classification or	Financial AI models are deployed

	in critical sectors (banking, biometric ID).	pre-deployment assessment for 'High-Risk' AI.	without rigorous safety testing.
Right to Explanation	Explicit right for users to know why an algorithmic decision was made.	No statutory right to explanation for automated decisions.	'Black box' lending and fraud detection remain opaque to consumers.
Deepfake Liability	Specific obligations for providers of GenAI models.	Liability relies on general forgery/defamation laws.	Difficulty in prosecuting the *creators* of deepfake tools vs. the *users*.

Source: Analysis of EU AI Act text and Indian statutes.[2106]

[2106] Juris Centre, "Legal Dimensions of Deepfake Technology: Privacy, Consent, and Criminal Liability" *Juris Centre*, 2025*available at*: https://juriscentre.com/2025/07/27/legal-dimensions-of-deepfake-technology-privacy-consent-and-criminal-liability/ (last visited December 25, 2025); "AI Act Service Desk - Article 50: Transparency obligations for providers and deployers of certain AI systems," *available at*: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-50 (last visited December 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

7. Prevention and Mitigation Strategies

Combating the hydra-headed monster of AI-enabled FinTech crime requires a synchronised, multi-layered approach involving technology, regulation, and public awareness.

7.1 Technological Solutions[2107]

- **Indigenous Deepfake Detection:** Indian research institutes are spearheading the development of detection tools. Projects like 'Saakshya' (IIT Jodhpur/Madras) and 'AI Vishleshak' (IIT Mandi) are creating multi-agent frameworks to detect deepfakes and forged signatures by analysing artefacts in audio-visual streams that are invisible to the human eye.
- **Zero Trust Architecture:** Banks must move beyond perimeter defence to a 'Zero Trust' model. Every user, device, and transaction must be continuously verified and monitored for accuracy and security. This involves using 'behavioural biometrics'—analysing how a user types, swipes, or holds their phone—to detect if a bot or a coerced victim is accessing an account.
- **Liveness Detection:** Enhancing V-CIP with 'passive liveness' checks is crucial. These systems can distinguish between a live person and a deepfake video feed by analysing micro-reflections in the eyes or blood flow patterns in the skin (photoplethysmography), which current deepfakes struggle to replicate perfectly.

7.2 Regulatory Recommendations

- **Mandatory AI Audits:** The RBI should mandate regular 'algorithmic audits' for financial institutions. These audits must test AI models for bias, robustness, and vulnerability to adversarial attacks, ensuring that the AI used for fraud detection cannot be fooled by its own algorithms.
- **Specific Deepfake Legislation:** India needs specific legislation to criminalise the *creation* and *distribution* of non-consensual deepfakes, separate from general fraud or defamation laws. This should include a 'strict liability' framework for platforms that knowingly host FaaS tools.
- **Cross-Border Cooperation:** Given the transnational nature of these crimes, India must strengthen extradition treaties and real-time intelligence sharing with ASEAN nations (Cambodia, Laos, Myanmar, Thailand) to dismantle the scam compounds in the Golden Triangle. A joint task force focusing on 'human trafficking for cybercrime' is essential.

7.3 Consumer Awareness and Cyber Hygiene

- **'Stop, Verify, Report':** Public awareness campaigns must shift from 'do not share OTPs' to 'do not trust your eyes/ears.' Citizens must be trained to verify 'emergency' calls by hanging up and calling the person back on their known number.
- **Digital Arrest Protocols:** A massive, nationwide campaign is needed to educate the public on a single, absolute truth: **Law enforcement agencies (CBI, ED, Police) NEVER conduct interrogations or demand money via video calls (Skype/WhatsApp).** Any such request is, by definition, a scam.

8. Future Outlook: 2026-2030

Looking ahead, the convergence of AI with other emerging technologies poses new, exponential risks.

- **Metaverse Fraud:** As banking enters the metaverse and immersive 3D environments, 'deepfake avatars' could

[2107] "IndiaAI Scales Up Safe AI Efforts with Cutting-Edge Solutions for Deepfake Detection, Bias Mitigation and AI Penetration Testing," *available at*: https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2175698 (last visited December 25, 2025); Aakash Chaudhary, "RBI's Cybersecurity Mandates 2025: Securing India's Digital Banks" *JISA Softech Pvt Ltd*, 2025*available at*: https://www.jisasoftech.com/rbis-cybersecurity-mandates-2025-securing-indias-digital-banks/ (last visited December 25, 2025).

impersonate bank tellers or advisors in virtual branches, conducting fraud in a spatially immersive setting.

- **Automated Mule Recruitment:** AI agents could autonomously recruit and manage mule networks through social media bots, eliminating the need for human recruiters and enabling the mule network to self-propagate at a speed that human investigators cannot match.
- **Quantum Threats:** The eventual rise of quantum computing could break current encryption standards (RSA/ECC) used to secure UPI and banking transactions. This necessitates an urgent migration to Post-Quantum Cryptography (PQC) to secure India's digital financial backbone before 'Q-Day' arrives.

9. Conclusion

The rise of AI in daily life and FinTech crimes represents a fundamental shift in the threat landscape. We have moved from an era of 'hacking machines'—exploiting code vulnerabilities—to an era of 'hacking humans'—exploiting cognitive and sensory vulnerabilities. The 'Digital Arrest' scam exemplifies this evolution; it is a crime that requires no malware on the victim's device, no stolen password, only the successful manipulation of their perception of reality.

While India's digital infrastructure (UPI, Aadhaar) is robust and world-leading, the regulatory and technical safeguards protecting the *users* of this infrastructure are playing catch-up. The commoditisation of AI via 'Fraud-as-a-Service' means that these attacks will only become cheaper, more personalised, and more prevalent.

Addressing this crisis requires a paradigm shift. Regulations must evolve from 'data protection' to 'identity protection.' Banking security must evolve from 'authentication' to 'intent verification.' Moreover, most importantly, the narrative must shift from blaming the 'gullible victim' to recognising that in the age of hyper-realistic AI, **seeing is no longer believing.**