The Face of Fraud: A Comparative Analysis of Deepfake Regulations in the EU AI Act vs. India's IT Rules

Dr. Manisha Jaydatt Gajre
Assistant Professor, Tolani Motwane Institute of Law, Adipur

Abstract—**We are living in an era where "seeing is believing" is no longer a safe maxim. Deepfake technology has graduated from the fringes of internet subculture to become a sophisticated engine for financial fraud, identity theft, and democratic disruption. As of 2026, legal systems around the globe are scrambling to define the boundaries of "digital personhood" and assign liability for algorithmic mimicry. This paper offers a narrative analysis of two distinct legal philosophies: the European Union's attempt to regulate the tool (the "Product Safety" model) versus India's attempt to regulate the platform (the "Intermediary Liability" model). The argument presented here is that while Europe offers superior preventative measures through transparency mandates, India provides a more agile "kill switch" for content removal. However, both systems currently leave a dangerous "liability gap" when it comes to financial fraud, leaving the individual victim to foot the bill for AI-driven crimes.**

I. INTRODUCTION: THE DEATH OF TRUTH IN THE DIGITAL AGE

In late 2023, the corporate world was shaken by a heist that seemed ripped from the pages of a science fiction novel. A finance worker in Hong Kong was duped into transferring $25 million to scammers. The weapon wasn't a gun or a hack; it was a video conference call. Every other face on the screen including the company's Chief Financial Officer was a deepfake, a digital puppet masterfully mimicking the voices and faces of trusted colleagues. This incident was a watershed moment. It signalled that synthetic media was no longer just about humiliating celebrities or spreading political lies; it had become a weapon of high-stakes economic warfare.

The challenge we face today is not just technological; it is deeply jurisprudential. Our current laws on forgery, impersonation, and fraud were drafted for a physical world. They rely on the assumption that a human face is a unique biometric identifier, unchangeable and unstillable. But Generative AI has shattered that assumption. We are now grappling with a "legal lag," where the technology moves at the speed of light while the law moves at the speed of bureaucracy.

This paper seeks to untangle the complex web of regulations emerging in response to this crisis. We will look specifically at the two heavyweights of digital regulation: the European Union, which views AI as a product to be tamed, and India, which views the internet as a chaotic highway that needs policing. By comparing these two approaches, we can begin to understand whether the best defence against digital fraud is to arrest the toolmaker or to punish the messenger.

II. THE TECHNICAL REALITY: HOW THE LIE IS MANUFACTURED

To understand why the law is struggling, we must first understand the machine it is trying to regulate. Deepfakes are not merely "edited videos" in the traditional sense. They are the product of Generative Adversarial Networks (GANs).

Imagine two AI systems locked in a room. One is the "Forger" (the Generator), trying to create a fake image of a human face. The other is the "Detective" (the Discriminator), trying to spot the fake. They play this game millions of times a second. The Forger gets better until the Detective can no longer tell the difference. The result is a synthetic piece of media that is mathematically indistinguishable from reality to the naked eye.

For a lawyer or a judge, this creates an evidentiary nightmare. If a video surfaces of a CEO admitting to tax fraud, or a politician inciting a riot, how do we verify its authenticity? If the forgery is perfect, traditional evidence laws collapse. This technical nuance dictates the regulatory response: if humans can't spot the fake, the law must mandate that the machines label themselves. This necessity for "provenance" is where the European and Indian paths diverge.

III. THE EUROPEAN APPROACH: REGULATING THE FACTORY

The European Union has long been the world's digital strict parent. With the EU AI Act, Brussels has decided to tackle deepfakes by going upstream straight to the developers who build these tools. The philosophy here is "Safety by Design." Just as we don't allow car manufacturers to sell vehicles without seatbelts, the EU argues we shouldn't allow AI developers to release tools without safeguards.

The cornerstone of this defence is Article 50. It essentially strips away the anonymity of AI. It mandates that any system generating synthetic audio, video, or text must ensure the output is machine-readable and clearly labelled as "artificially manipulated." This is a powerful preventative measure. It operates on the logic that if a user sees a "Contains AI" watermarked on a video, the potential for fraud is neutralized. The EU is effectively trying to inoculate the population against deception before it even spreads.

However, the Armor has a chink. In its zeal to protect freedom of expression, the EU Act includes exemptions for "artistic, creative, or satirical purposes." While legally necessary to prevent censorship, practically, this creates a Trojan Horse. A fraudster caught creating a deepfake of a public figure can easily claim it was "parody" or "social commentary." This forces the legal system into a subjective debate about art versus fraud, buying the criminal valuable time while the damage is already done.

IV. THE INDIAN APPROACH: POLICING THE HIGHWAY

India, with its billion-plus internet users, does not have the luxury of purely academic regulation. The sheer volume of data consumed in India means that once a deepfake starts spreading, it can incite violence or crash stock markets within minutes. Consequently, India's approach is far more reactive and aggressive. It focuses less on the creation of the deepfake and more on its distribution.

The primary weapon in India's legal arsenal is the Information Technology Rules, 2021 (updated through 2025). These rules fundamentally change the relationship between the state and social media giants. The government has drawn a line in the sand: platforms like Facebook, YouTube, and X (formerly Twitter) are no longer just passive pipelines. They are "intermediaries" with a duty of care.

Rule 3(1)(b)(v) is the specific provision that does the heavy lifting. It prohibits the hosting of any content that "impersonates another person." But a law is only as good as its enforcement. India enforces this by holding a gun to the head of the platforms: the threat of losing "Safe Harbor." If a platform fails to exercise "due diligence" in catching deepfakes, it loses its immunity under Section 79 of the IT Act. This means the CEO of a social media company could theoretically be arrested for a deepfake posted by a teenager in Mumbai.

The most effective part of the Indian model, however, is the "24-Hour Takedown" mandate. For content involving nudity or morphed images (a common form of deepfake harassment), platforms must remove the content within 24 hours of a complaint. This is a "kill switch" that the EU bureaucracy often lacks. It prioritizes the victim's dignity over procedural delays.

V. COMPARATIVE ANALYSIS: PREVENTION VS. CURE

When we place these two frameworks side by side, a clear contrast emerges in their legal DNA. The European model is akin to vaccination it tries to stop the virus (the deepfake) from ever becoming dangerous by weakening it with labels and transparency. It is a noble, "upstream" solution.

The Indian model is akin to surgery it accepts that the patient is already infected and tries to cut out the tumour (the content) as fast as possible. It is a messy, "downstream" solution, but often necessary in emergencies.

But both systems hit a brick wall when faced with the "Dark Room" of the internet: Encryption.

Most financial deepfake fraud today doesn't happen on a public Facebook wall; it happens on private WhatsApp or Telegram calls. In these encrypted spaces, the EU's watermarks are useless if the recipient doesn't have the software to read them. Similarly, India's platform liability rules are toothless because the platform itself cannot "see" the call to moderate it without breaking end-to-end encryption a step that raises massive privacy concerns. This is the blind spot where the law fails. The fraudster hides in the privacy that the law itself protects.

VI. THE LIABILITY GAP: WHERE THE VICTIM STANDS ALONE

Perhaps the most disturbing finding of this research is the complete lack of recourse for the financial victim. Let's go back to our initial example of the finance worker.

If you are tricked by a deepfake into transferring your life savings to a scammer, who reimburses you?

- The Bank? They usually refuse, citing "user negligence." After all, you authorized the transfer; the bank's security wasn't breached, your mind was.
- The Platform? In India, they will claim they are just the messenger. In the EU, they will point to the fact that the call was private.
- The AI Developer? Good luck suing an open-source developer on GitHub who released the code for free.

We have created a "Liability Gap." We have criminalized the act of fraud (under the new Bharatiya Nyaya Sanhita in India), and we have regulated the market of AI (in the EU), but we have not created a safety net for the individual. The victim is left holding the empty bag, caught between a tech giant claiming immunity and a criminal hiding behind a VPN.

VII. CONCLUSION: A CALL FOR A HYBRID MODEL

The battle against the "Face of Fraud" cannot be won with a single legal ideology. The rigid, compliance-heavy approach of Europe is too slow for the viral speed of the internet. The reactive, takedown-heavy approach of India is too late for the instant nature of financial theft.

The future of digital regulation must be a Hybrid Model. India needs to adopt the EU's strict "watermarking" standards. Every piece of AI-generated content originating in or entering India's digital borders should carry a cryptographic signature. This would allow our phones and browsers to automatically flash a "Potential Fake" warning during a video call, stopping the fraud before the money is transferred.

Conversely, the world needs the agility of India's grievance redressal mechanisms. The concept of having a local officer responsible for taking down harmful content within hours is the only way to minimize damage in a hyper-connected world.

Ultimately, we need to introduce a new concept into tort law: "Strict Liability for Deceptive Tech." If a company profits from releasing a tool that can clone voices, they must contribute to an insurance pool for victims of voice-clone fraud. Until we attach a financial cost to the creation of these tools, the law will remain a toothless spectator, and the face of fraud will continue to change faster than we can recognize it.

REFERENCES

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

[2] The Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).

[3] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended vide Notifications dated 2022, 2023, and 2025), Ministry of Electronics and Information Technology (MeitY), Government of India.

[4] The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament, 2023 (India) (Sections 318, 319, and 336).

[5] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).

[6] Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4.5.2016.

[7] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[8] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

[9] Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023, Delhi High Court (Interim Order dated Sept 20, 2023).

[10] Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107, 1753.

[11] Floridi, L. (2023). The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford University Press.

[12] Ministry of Electronics and Information Technology (MeitY), Advisory on Due Diligence by Intermediaries regarding Deepfakes, Government of India (November 7, 2023).

[13] NITI Aayog, National Strategy for Artificial Intelligence: #AIForAll, Government of India (2018).

[14] European Parliament Research Service (EPRS), Artificial Intelligence Act: Briefing on EU Legislation in Progress, PE 698.792 (2024).

[15] Vakul Sharma & Seema Sharma, Information Technology Law and Practice, 7th Edition (2024), Universal Law Publishing.

[16] CNN Business, “Finance Worker Pays Out $25 Million After Video Call With Deepfake CFO,” (February 4, 2024).

[17] Internet Freedom Foundation (IFF), Analysis of the IT Rules Amendments 2023: Fact Checking and Deepfakes, IFF Working Papers (2023).