# SYNTHETIC MARKET ABUSE: DEEPFAKE IMPERSONATION AND SECURITIES FRAUD

*Dr. Jasleen Kewlani & Rudraksh Singh Sisodia*[*]

ABSTRACT

The spread of generative Artificial Intelligence (AI) has triggered a paradigm shift in the financial crime environment, creating a new and very serious threat of the so-called Synthetic Market Abuse. It can be described as a major advancement in the sophistication and scale of white-collar crime, as AI-altered voice and deepfake video usage to impersonate corporate leaders and market manipulators has become a common practice. It was stated that the year 2025 was the year of the crisis of Synthetic Media, when the boundary between real and fake content has become more unclear than ever before, which offers an unprecedented opportunity to manipulate the market and commit fraud. The ultimate target of these activities is the common people, including those who have very limited financial resources to invest and dream for their future. Creating a space in the virtual world or misusing the existing virtual space for fraudulent aims has become very convenient today. The democratization of powerful AI tools has lowered the entry barrier for malicious actors, enabling even those with minimal technical expertise to engage in complex schemes that can destabilize financial markets and erode investor confidence, primarily giving them impetus to invest ignorantly. This paper aims to explore the industrialization and institutionalization of 'deceit and deception' through AI, examine case studies of synthetic market abuse, and analyse the profound sociological, legal and economic impact of this emerging threat; having a major focus on the Indian context. The paper suggests measures like strategizing a strong and unified Global Front against misuse of AI for manipulating investors and subjects by market abuse, with the help of creating, amending, and effectively implementing financial regulations. It is also necessary to pay close attention to the encouragement to research bodies; law experts; and Higher Education Institutions (HEIs) toward the design of Policy Documents, which could come in handy, to implement design resolution mechanisms which are effective, to control and curb Deepfake Impersonation and Securities Fraud, in the context of the social audit of the current laws and financial regulations.

**Keywords:** Synthetic Market Abuse, Deepfake Impersonation, Securities Fraud, Generative Artificial Intelligence, Financial Market Manipulation.

---

[*] Dr. Jasleen Kewlani is an Associate Professor of Sociology at Rajiv Gandhi National University of Law, Punjab and Rudraksh Singh Sisodia is a fourth-year student at Rajiv Gandhi National University of Law, Punjab. The views stated in this paper are personal.

## I. INTRODUCTION

With the emergence of generative Artificial Intelligence (‘**AI’**), the nature of financial fraud has radically changed and turned into an automated, scalable business enterprise instead of a manual, labour-intensive one. This industrialization of lies is defined by the fact that there are complex AI models that are used to produce very realistic synthetic media. The generated media

can then be used to influence market sentiment, cheat on transactions on a large scale and deceive investors.[1] With the availability of such technologies, sometimes under Deepfake-as-a-Service (‘**DaaS**’) services, criminals can impersonate trusted figures and publish fake information.[2] This has given rise to high-frequency manipulation schemes where AI-powered bots are capable of executing pump-and-dump schemes at machine speed, exploiting the high rate of the rapid flow of information in today’s 21st-century financial markets. The repercussions of this change are enormous because the conventional regulatory frameworks struggle to keep pace with this fast-evolving threat landscape. The conventional approach to financial fraud usually involved a large human capital, technical skills and resources, restricting its size and scope. Fraudsters had to manually create phishing emails and fake websites, while social engineering tactics relied on slow, labour-intensive methods to deceive victims.[3]

With the emergence of generative AI, such operations have become automated and faster, allowing one agent to organize multi-stage complex fraud operations that can involve thousands of victims at once. AI generates highly convincing phishing emails with perfect grammar and personalized content, realistic fake websites, and even deepfake videos and audio that are nearly indistinguishable from real ones. This automation dramatically increases both the efficiency and effectiveness of scams by exploiting

---

[1] Pi-Labs, *Digital Deception Epidemic: 2024 Report on Deepfake Fraud’s Toll on India* (2024), 31.

[2] Bobby Chesney and Danielle Citron, ‘Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security’ (December 2019) 107 California Law Review 1753 <www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security/> accessed 20 February 2026.

[3] Frank Pasquale, ‘A Rule of Persons, Not Machines: The Limits of Legal Automation’ (January 2019) 87 George Washington Law Review 1 <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=2094&context=faculty> accessed 22 February 2026.

psychological weaknesses and bypassing traditional defences. As a result, the threat has intensified sharply, operating at a scale and speed that law enforcement and financial institutions struggle to detect or stop.[4]

The paper is structured as follows. Part I traces the industrialization of financial deception through generative AI and DaaS. Part II critically discusses case studies on synthetic market abuse in India, uncovering structurally vulnerable points and underlying causes that are not part of the narrative. Part III places quantitative economic information into a causal framework that traces the routes between deepfake creation and systemic financial risk. Part IV contains a critical assessment of the current statutory text, the 2025 IT Rules, the BNS, 2023, and the BSA, 2023, revealing the grey areas of the law, the ambiguity of regulations, and the gaps in enforcement. Part V addresses the issue of intermediary liability and safe harbour regime. Part VI concludes by providing context-specific, operationalizable recommendations as well as an evaluation of how risky and unintended their consequences can be.

The use of AI in financial fraud has surged as the cost of producing convincing synthetic media has plummeted, from thousands of euros to just a few euros per minute of video.[5] This has made deceit cheaper and simpler to scale, resulting in the rise of new types of fraud, including the so-called lost pet scam, wherein fraudsters utilize AI-generated pictures of allegedly discovered pets to scam desperate owners into paying small recovery fees,

[4] Jack M Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (February 2018) 51 UC Davis Law Review 1149 <https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-3_Balkin.pdf> accessed 12 March 2026.

[5] Hilary J Allen, 'Driverless Finance' (2020) 10 Harvard Business Law Review 158 <https://journals.law.harvard.edu/hblr/wp-content/uploads/sites/87/2020/03/HLB101_crop.pdf> accessed 24 February 2026.

conveniently weaponizing emotions of the people.[6] Although such small-ticket scams are alarming, the greater danger lies with the deepfake-enabled investment schemes and identity spoofing, which can cost an individual or a company a lot of money. The industrialization of fake news has also spawned advanced systems of fraud-as-a-service, in which fraudsters are able to buy access to AI-driven devices and services, including deepfake creation applications, phishing kits, and money laundering networks on the dark web or in encrypted messaging applications.[7] This has resulted in a very efficient and criminal system which is difficult to crack since the criminals can easily shift to other fields and avenues once their operations are identified.[8]

### *A. Deepfake-as-a-Service (DaaS) and its Role in Democratizing Fraud*

The so-called Deepfake-as-a-Service ("**DaaS**") platforms, which are usually subscription services, offer consumers a collection of artificial intelligence-driven programs to make deepfakes, voice cloning, and synthetic identities.[9] As such, DaaS has caused an explosion of scams powered by deepfakes since criminals can make very believable impressions of corporate leaders, government officials and other trusted individuals with limited technical knowledge.

This has especially been reflected in the increase in CEO fraud and Business Email Compromise (**'BEC'**) attacks, in which fraudsters employ

---

[6] Frank Pasquale, *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Harvard University Press 2020).

[7] International Monetary Fund, *Global Financial Stability Report: Steadying the Course: Uncertainty, Artificial Intelligence, and Financial Stability* (22 October 2024) <www.imf.org/-/media/files/publications/gfsr/2024/october/english/textrevised.pdf> accessed 17 March 2026.

[8] OECD, *Assessing Potential Future Artificial Intelligence Risks, Benefits and Policy Imperatives* (OECD AI Papers No 27, 14 November 2024) <www.oecd.org/content/dam/oecd/en/publications/reports/2024/11/assessing-potential-future-artificial-intelligence-risks-benefits-and-policy-imperatives_8a491447/3f4e3dfb-en.pdf> accessed 2 March 2026.

[9] Pi-Labs, *Digital Deception Epidemic* (n 2).

deepfake audio or video to dupe workers into transferring money.[10] DaaS has also enabled the proliferation of cross-border fraudulent activities, as criminals can easily target their victims in other jurisdictions without being detected. The role of DaaS in the financial services industry cannot be overstated, and an increase in deepfake fraud of 1,740% in North America in 2022/23 alone, as well as a loss amounting to over 200 million in the 1st quarter of 2025 alone.[11] Deepfake fraud has also increased significantly in the Asia-Pacific (**'APAC'**) region by 1,530 % over the same time.[12] This is a fast-growing alert to the threat of DaaS and the necessity for financial institutions to build greater protections against AI-powered fraud, making policing and regulation challenging.

Generative AI combined with the High-Frequency Trading (**'HFT'**) algorithms has created what can now be described as a new and more dangerous variant of market manipulation: machine-speed Pump-and-dump.[13] In these operations, AI enables fraudsters to rapidly generate and spread synthetic hype, including deepfake videos or audio of corporate officials, fake announcements, and AI-driven social media bots, to artificially inflate asset prices at unprecedented scale.[14] Such algorithms are used to disseminate rumours and disinformation among the millions of users within minutes, leaving investors

---

[10] Satish Lalchand, and others, *Deepfake Banking and AI Fraud Risk* (Deloitte Center for Financial Services, 29 May 2024) <www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html> accessed 22 March 2026.

[11] McAfee, *Beware the Artificial Impostor:A McAfee Cybersecurity Artificial Intelligence Report* (May 2023) <www.mcafee.com/content/dam/consumer/en-us/resources/cybersecurity/artificial-intelligence/rp-beware-the-artificial-impostor-report.pdf?msockid=08cb4aa64d8a6bb633ea59274c786a29> accessed 20 May 2026.

[12] Pi-Labs, *Digital Deception Epidemic* (n 2).

[13] Viktoria Dalko and Michael H Wang, 'High-Frequency Trading: Deception and Consequences' (2018) 14(5) Journal of Modern Accounting and Auditing 271 <www.davidpublisher.com/Public/uploads/Contribute/5b1a2dbbe1a79.pdf> accessed 18 February 2026.

[14] Bank for International Settlements, *Digitalisation of Finance* (BCBS 575, May 2024) <www.bis.org/bcbs/publ/d575.pdf> accessed 30 March 2026.

crushed with millions of dollars in losses.[15] The application of AI in pump-and-dump schemes has also enabled the fraudsters to be much more efficient and harder to detect than the corresponding traditional schemes.[16]

### *B. Case Studies in Synthetic Market Abuse*

The following case analyses, across various jurisdictions, prove that the threat is indeed global, and a concerted response is urgently required. From exploitation of a famous industrialist to the imitation of the CEO of a large stock exchange, these cases have shown the susceptibilities of the modern financial system to AI-based fraud.

#### 1. THE NSE CEO DEEPFAKE: IMPERSONATING ASHISH KUMAR CHAUHAN FOR STOCK RECOMMENDATIONS

In the case of the deepfake impersonation of Ashishkumar Chauhan, the Managing Director and Chief Executive Officer (**'CEO'**) of the National Stock Exchange of India (**'NSE'**), a highly realistic deepfake video was created and circulated, showing an AI-generated version of Chauhan delivering a specific stock recommendation.[17] The video was crafted to deceive viewers into believing that the head of India's largest stock exchange was personally endorsing certain investment opportunities. This incident had various implications.[18] First, it exploited the high credibility and authority of

---

[15] Sensity AI, *The State of Deepfakes* (2024) <https://5865987.fs1.hubspotusercontent-na1.net/hubfs/5865987/SODF%202024.pdf> accessed 16 February 2026.

[16] Danielle Citron And Robert Chesney, 'Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics' (2019) 98(1) Foreign Affairs 147 <www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> accessed 20 March 2026.

[17] Press Trust of India, 'NSE warns investors against deepfake clips of its chief recommending stocks' *Business Standard* (New Delhi, 10 June 2024) <www.business-standard.com/markets/news/nse-warns-investors-against-deepfake-clips-of-its-chief-recommending-stocks-124061000836_1.html> accessed 13 March 2026.

[18] Jayshree P Upadhyay, 'After NSE, BSE cautions investors on CEO's deepfake videos' *Reuters* (Mumbai, 18 April 2024) <www.reuters.com/world/india/after-nse-bse-cautions-investors-ceos-deepfake-videos-2024-04-18/> accessed 24 February 2026.

a prominent figure in the Indian financial ecosystem, lending the fraudulent advice an air of legitimacy. Second, it demonstrated how deepfakes can be weaponized to manipulate markets and deliberately influence the price of specific securities. The case underscores the fact that even the most sophisticated market stakeholders remain vulnerable to AI--driven fraud. It raises serious questions regarding the adequacy of the existing regulatory and legal frameworks to address the risks in question.[19] The ease with which a top financial leader could be convincingly cloned serves as a stark reminder of the serious threat deepfakes pose to large financial institutions and the integrity of information they disseminate.

### 2. THE RELIANCE DEEPFAKE: MISUSING MUKESH AMBANI'S PERSONA TO PROMOTE FRAUDULENT SCHEMES

The other high-profile instance of synthetic market abuse was the misappropriation of the identity of Mukesh Ambani, Chairman and Managing Director of Reliance Industries, one of the largest conglomerates in India. In this case, a deepfake video was produced where Ambani was promoting a fake investment scheme. The video was widely spread on social media and other online platforms with the intention of trapping unsuspecting investors to part with their money.[20] The case is especially intriguing as the targeted figure is not only a highly successful business leader, but also a household name in India, and therefore carries a certain degree of public trust and power. The case highlights the cross-platform aspect of the threat because the fraudulent content was spread through numerous digital platforms, and it became

[19] Securities and Exchange Board of India, *Master Circular on Surveillance of Securities Market* (23 September 2024) <www.sebi.gov.in/legal/master-circulars/sep-2024/master-circular-on-surveillance-of-securities-market_86929.html> accessed 22 February 2026.

[20] Express News Service, 'Deepfake videos of Narayana Murthy, Mukesh Ambani: Bengaluru residents lose Rs 87 lakh in trading scam' *Indian Express* (Bengaluru, 5 November 2024) <https://indianexpress.com/article/cities/bangalore/deepfake-videos-narayana-murthy-mukesh-ambani-bengaluru-trading-scam-9654607/> accessed 4 April 2026.

challenging to contain and eliminate.[21] The case acts as a wake-up call to people about the necessity of raising public awareness regarding the risk of deepfakes, as well as verifying the reliability of any information in a matter of investment, particularly when said individual is a high-profile figure.

### 3. STRUCTURAL DRIVERS AND ROOT CAUSES: WHY INDIAN MARKETS REMAIN DISPROPORTIONATELY VULNERABLE

Critical analysis of these instances indicates that synthetic market abuse in India stems not only from technological sophistication but, more importantly, from deep structural vulnerabilities. First, trust asymmetry of financial culture makes India acutely vulnerable to identity-based fraud: the credibility of personalities like Mukesh Ambani or the NSE CEO is synthetically harnessed, creating an authority effect that India, with its rising numbers of first-generation retail investors (130 million demat accounts by 2024), does not possess the analytical infrastructure to challenge. Second, the institutional diffraction of regulatory power between SEBI, MeitY and the Ministry of Home Affairs has a jurisdictional blind spot where no single authority has overall responsibility over AI-based market fraud. This is especially evident in Chinese-supported deepfake networks. They are often hosted on overseas servers, which exploit gaps between domestic regulatory jurisdictions. Third, the structural perverse incentive calculus has also been produced by the fall in DaaS price. Generating an effective deepfake now costs mere euros, while potential gains from market manipulation can be enormous. This imbalance has rendered the deterrent effect of existing laws under the BNS and SEBI's enforcement toolkit largely ineffective.

[21] FSB, *The Financial Stability Implications of Artificial Intelligence* (n 1).

## II. THE ECONOMIC IMPACT OF SYNTHETIC HYPE

As emphasised before, the rapid propagation of deepfakes and the use of such technologies in the financial sector may result in huge and extensive economic damage. Manufacturing and dissemination of artificial hype or fake or misleading information developed by AI can destabilise the economy of markets, ruin investor confidence, and ultimately endanger the economy. The economic impact of this phenomenon cannot be equated to just a few cases of fraud; it is a systemic risk, and it can also have extensive consequences for the entire financial system.[22] This section will examine the economic impacts of synthetic hype, specifically the estimated loss of money in India, the potential threat to market integrity and investor confidence, and the potential economic disaster on a massive scale.

Deepfake fraud poses an enormous economic threat in India. According to cybersecurity firm Pi-Labs (2024), the country was projected to suffer losses of ₹70,000 crore (approximately $8.4 billion) due to deepfake scams in 2025 alone.[23] This sudden rise in the number of financial losses is, according to the report titled Digital Deception Epidemic: 2024 Report on Deepfake Fraud on Toll on India, attributed to the increasing availability and maturity of generative AI tools, which are now being used to commit a wide array of crimes, including financial fraud, identity theft, and the production of non-consensual adult material. Another point that was mentioned in the report is the appearance of the so-called Jamara 2.0, which is defined as the employment of deepfake to interfere with video-based Know Your Customer ("**KYC**") procedures, impersonate a business executive, and generate artificial

[22] OECD, *Assessing Potential Future AI Risks, Benefits and Policy Imperatives* (n 13).
[23] Pi-Labs, *Digital Deception Epidemic* (n 2).

evidence in a digital form.[24] This vulnerability has placed both individuals and financial institutions as the main targets of identity theft, fraudulent investments, and money laundering since the number of video KYC calls conducted per day was over 11 lakh in India alone. It is not a mere figure of 70,000 crore loss, but an indication of a serious burden on the Indian economy and with a wide-ranging implication on businesses, investors and people at large.[25]

### *A. The Threat to Market Integrity and Investor Confidence*

In addition to the immediate losses in terms of money, the application of deepfakes in securities fraud is a critical threat to market integrity and investor confidence. A well-functioning financial market is based on trust that the information on which investment decisions are made is accurate and reliable. The spread of synthetic media essentially compromises this trust because it has become increasingly difficult to draw the line between the real and the fake. When the investors cannot be certain that a video of an announcement made by the CEO is authentic or that the recommendation given by a financial analyst is true, their trust in the market is lost. This may cause several adverse effects, such as market volatility, a decrease in liquidity and a flight to safety because investors will be risk-averse.[26] This is the threat that has been identified by the International Monetary Fund ("**IMF**"), which has stated that the ill intent of AI, such as deepfakes, is a major threat to financial stability. Loss of investor confidence is a long, slow, insidious process, whose ultimate

[24] Reserve Bank of India, Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on August 14 2025) (withdrawn) <www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12893> accessed 25 February 2026.
[25] Bank for International Settlements, *Digitalisation of Finance* (n 19).
[26] International Monetary Fund, *Advances in Artificial Intelligence: Implications for Capital Market Activities* (Chapter 3 in *Global Financial Stability Report*, 22 October 2024) <www.elibrary.imf.org/display/book/9798400277573/CH003.xml> accessed 26 February 2026.

results may be disastrous, in terms of a weaker and less efficient financial system.

Given the high degree of interconnectedness in modern financial markets, a localized incident of synthetic market abuse can also produce far-reaching and unpredictable consequences.[27] A deepfake-induced flash crash in a single market could rapidly spread to others, triggering automated sell-offs, a sudden evaporation of liquidity, and a dangerous chain reaction. The IMF has cautioned against such events, suggesting that algorithmic trading programs tend to have risk management features that de-risk or shut down entirely in highly volatile times.[28] The possibility of a large-scale economic crisis is an obvious and imminent threat in the context of the current situation, and the necessity of a unified and active intervention of regulators, policymakers, and the financial sector is pronounced.

### *B. Causal Mechanisms and Systemic Risk: Beyond the Data*

The importance of the loss of an estimated 70,000 crores can hardly be understood without an analytical causal model. On the micro level, deepfake disinformation takes advantage of cognitive biases, including authority bias, social proof, and availability heuristic, to make economically irrational investment choices. On a meson scale, pools of misled investors have the effect of producing price momentum that is exponentially sensitive to high-frequency trading algorithms because HFT systems operate under the principle of pursuing price changes instead of questioning the information underpinning these changes, creating a feedback mechanism where artificial hype generates real market movement that, in turn, confirms the hype to

[27] United Nations Conference on Trade and Development, *Digital Economy Report 2024* (10 July 2024) <https://unctad.org/publication/digital-economy-report-2024> accessed 31 March 2026.
[28] IMF, *Advances in Artificial Intelligence* (n 31).

subsequent entrants. At the macro level, India is increasingly becoming entangled in the global capital markets due to the influx of FPI and index inclusion, such that when a synthetic market abuse event of adequate magnitude occurs, it may lead to cascading contagion effects with international spillover effects. The lack of an early-warning system to AI-created market disinformation as part of the Indian financial stability system constitutes a major regulatory failure that current regulatory frameworks have not been able to recognize, much less mitigate.

## III. STATUTORY RECOGNITION: ANALYZING THE 2025 INFORMATION TECHNOLOGY (IT) RULES AMENDMENT ON SYNTHETICALLY GENERATED INFORMATION

The Indian government has made a major step towards the regulation of this new form of content owing to the increasing threat of synthetic media. The Ministry of Electronics and Information Technology ("**MeitY**") has implemented changes in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[29], which seeks to capture the problems presented by the establishment and propagation of synthetically created information. The set of amendments, which were implemented in 2025[30], are a milestone in the history of the digital governance of India, as they offer the first codified legal basis to address the issues of deepfake and other types of AI-generated content. The following section of the paper offers an in-depth examination of the 2025 amendments to the IT Rules- including the new definitions, labelling requirements, and due diligence requirements they entail, while also comparing India's approach to

[29] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

[30] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, draft (17 October 2025).

these regulations with those adopted in other jurisdictions, and discusses the legal issues and judicial challenges they are likely to raise.

### *A. The 2025 MeitY Amendments: An Analysis of the New Regulatory Framework*

Released in October 2025[31], the 2025 amendments to the IT Rules propose a new holistic framework of regulation of handling information synthetically generated. The amendments strike the right balance between the necessity to safeguard the citizens against the dangers of deepfakes and falsehood, and the desire to encourage innovation in the field of AI. The major text of the amendments is a new definition of information synthetically generated, a labelling obligation of this content, and an increased due diligence responsibility for social media intermediaries. The amendments also have a new idea of shared responsibility where both content creators and hosting platforms have the burden of making sure that the synthetic media is duly labelled and does not infringe on any legislation.

A key foundation of the 2025 amendments to the IT Rules is the introduction of a formal legal definition for "synthetically generated information." According to the draft rules, this refers to any information that is artificially or algorithmically produced, developed, altered, or transformed using computer resources in a manner that creates a reasonable impression of being genuine or authentic. Such a definition is intentionally broad as well as encompassing a wide range of AI-generated material, including deepfake videos, voice clones, synthetic images, and even AI-generated text. A particularly important element is the "reasonable impression" standard, which introduces a subjective assessment. This allows the regulation to cover

[31] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, as notified and reflected in the consolidated rules updated on 10 February 2026.

material that is likely to mislead an ordinary user into believing it is real. However, such a subjective standard has been criticised as well, and the critics of the law[32] have also highlighted that a subjective standard can be applied in an inconsistent manner and that the measure can have a chilling effect on lawful ways of expression: satire and parody.

### *B. The 10% Visual Labelling Mandate for Deepfake Content*

One of the most significant and controversial provisions in the 2025 IT Rules amendments is the mandatory labelling of synthetically generated content. [33] The draft rules require visible labels covering at least 10% of the area for visual material [a]nd audible labels for 10% of the duration in audio.[34] They also mandate permanent metadata watermarks for traceability. [35]The purpose of such labelling is to allow users to distinguish between legitimate and AI-generated content, therefore reducing the possibility of deceiving users.[36] However, some critics have also condemned the threshold of 10%, stating that it is arbitrary and onerous to small platforms and content creators.[37] There is also a fear that the labelling requirement can be abused by unscrupulous individuals, and they may simply take out or alter the labels[38].

---

[32] Rishabh Dara, 'Intermediary Liability in India: Chilling Effects on Free Expression' (Centre for Internet and Society, 27 April 2012) <https://cis-india.org/internet-governance/chilling-effects-on-free-expression-on-internet> accessed 15 March 2026.

[33] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, r 4, GSR 775(E), Gazette of India, Extraordinary, Part II, s 3(i) 22 October 2025.

[34] ibid r 3(2)(b)(ii).

[35] ibid r 3(2)(c).

[36] ibid, Explanation to r 3(2).

[37] B Chandra and others, *Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency* (National Institute of Standards and Technology, 20 November 2024) <https://doi.org/10.6028/NIST.AI.100-4> accessed 13 March 2026.

[38] HM Government, *A pro-innovation approach to AI regulation: government response to consultation* (February 2024) <https://assets.publishing.service.gov.uk/media/65c1e399c43191000d1a45f4/a-pro-

### *C. Due Diligence Obligations for Significant Social Media Intermediaries (SSMIs)*

The amendments of the 2025 IT Rules impose important new due diligence requirements on Significant Social Media Intermediaries (**'SSMI'**), which are characterized as those platforms having over five million registered users in India[39]. In the new regulations, SSMIs must undertake some measures to curb the spread of fake-generated information, including: (i) User Declaration: Platforms must also obtain a declaration by users when they post their content on whether it is composed or modified with the assistance of AI or any other such synthetic method. (ii) Technical Verification: To determine the validity of user statements, platforms must undertake reasonable and proportionate technical interventions that contain automated detection tools. (iii) Prominent Labelling: The platforms should make sure that every content synthetically generated is clearly marked with an identifiable mark showing up visibly or audibly. (iv) Traceability: To make it traceable, platforms should have a permanent and unique metadata identifier or watermark on the content. (v) Takedown: Platforms must remove or disable access to any content that is found to be in violation of the rules.

Any non-observance of these duties may lead to failure to enjoy the protection of safe harbour provided in Section 79 of the IT Act, which would cause the platform to be subjected to any unlawful content that is hosted on its service.

### *D. India's Intermediary Liability Approach: A "Kill Switch" for Content*

innovation-approach-to-ai-regulation-amended-governement-response-web-ready.pdf> accessed 5 April 2026.

[39] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, r 2(1)(v).

The concept of intermediary liability underlies India's strategy of regulating synthetic media, and is aptly represented under the 2025 amendments of the IT Rules.[40] This model, also followed in countries like the United States, places primary responsibility on the platforms that host the content.[41] In this policy, Intermediaries enjoy safe harbour protection from liability for third-party content, provided they fulfil due diligence obligations, such as removing unlawful material upon gaining knowledge of it.[42] The 2025 changes to the IT Rules made these responsibilities more enforceable and allowed the platforms to become more proactive in identifying and eliminating the synthetically generated information.[43] Critics view this as a "content kill switch," as it effectively empowers platforms to take down any material deemed non-compliant. The underlying rationale is that platforms are best placed to monitor content on their services and should be held accountable for harms arising from their negligence.[44]

The 2025 IT Rules amendments have also encountered other legal objections and judicial reviews, especially on the effect it has on the freedom of speech and expression. The wide and subjective definition of the term synthetically generated information, its compulsory labelling prerequisites, and its increased due diligence risk of SSMIs have all been lamented as having the prospect of a chilling effect on online dialogue; some of the key ones have been covered in the current paper.

The other significant issue regarding the amendments to the IT Rules 2025 is that it may have a chilling effect on freedom of speech. The imprecise and

[40] Regulation (EU) 2024/1689 (Artificial Intelligence Act) art 3(1).
[41] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, r 2(1)(x).
[42] Communications Decency Act of 1996, 47 USC § 230(c)(1) (2018).
[43] Information Technology Act 2000, s 79(2)(c).
[44] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r 3(1)(b) (as amended).

opinionated definition of what constitutes information synthetically generated, in combination with the obligatory labelling and the risk of losing safe harbour protection, may result in the creation of a scenario where platforms and users are too mindful of their online expression, which will result in not violating the rules.[45] This may suffocate any valid means of expression, including satire, parody, and political criticism.

## IV. CRIMINAL LIABILITY UNDER BNS: SECTIONS 319 (PERSONATION) AND 353 (MISINFORMATION) IN A SECURITIES CONTEXT

With the emergence of deepfake technology, the Indian criminal justice system is faced with a novel and challenging number of issues. The capability to develop hyper-realistic, synthetic media that may realistically masquerade as actual people has set a new stage for criminal activities such as fraud, defamation, and manipulation of markets. To address this new menace, the Bharatiya Nyaya Sanhita **('BNS'),** 2023, also has a number of new provisions which are intended to tackle the issue of the digital era.[46]

Section 319 (Cheating by Personation) and Section 353 (Statements Conducing to Public Mischief) are two such sections that will be of particular importance to the problem of synthetic market abuse.[47] This section is a critical examination of the appropriateness and sufficiency of such provisions in deterring and penalizing the use of deepfakes in securities fraud. It additionally looks into the dynamic jurisprudence of the novel deepfake liability and interaction of the BNS and the IT Act, 2000. Sub-clause 353 of the BNS that is equivalent to Section 505 of the IPC, criminalizes the making, publishing, or circulating of any statement, false information, rumour, or report with the

[45] *Shreya Singhal v Union of India* (2015) 5 SCC 1 [118].
[46] Bharatiya Nyaya Sanhita 2023.
[47] ibid ss 319, 353.

intent to cause, or which is likely to cause, fear or alarm to the public, or to any section of the public, whereby any person may be induced to commit an offence against the State or against the public tranquillity.[48]

The part also punishes the formation or propagation of the sentiments of hostility, hate, or malice among the various religious, racial, linguistic, or regional communities. The penalty for these crimes is a jail term of up to three years and a fine or both. The law of Section 353 applied to financial markets is a dynamic and complicated field of law.[49] The BNS does not have a definition of the term public mischief, and the development of case law is likely to inform it.[50] The concept of public mischief might be applied in securities fraud as the distribution of false or misleading information that will most likely influence investors to make decisions that they would not have otherwise made. Nevertheless, the boundaries of the concept of public mischief are not inexhaustible, and probably courts will demand that the direct and foreseeable connection between the false information and the harm be demonstrated.

Although Section 353 is a possible avenue of prosecuting individuals who use deepfakes to induce financial market manipulation, it can be argued that there are reasons to suggest that this particular provision is not sufficient to prevent "synthetic hype" in the future. First, the part must comprehend an exhibiting of intent to cause, or probable cause of causing, fear or alarm in the populace. It is not apparent that the spread of fake data to manipulate the prices of a stock would satisfy this need. Second, the section does not explicitly concern itself with the application of synthetic media, and it might be difficult to apply its provisions to this new and fast-changing technology by the courts.

---

[48] ibid s 353.
[49] *Romesh Thappar v State of Madras* AIR 1950 SC 124, 602.
[50] *Ramji Lal Modi v State of Uttar Pradesh* AIR 1957 SC 620, 864.

Third, the penalty for the crime in Section 353 is comparatively light, with the highest penalties of three years' imprisonment. It is also feared that Section 353 might be misapplied by the enforcing agencies to suppress an honest criticism and dissent, just as the now-abolished Section 66A of the IT Act.[51] Section 66A, which the Supreme Court declared unconstitutional in 2015, criminalised the sending of any "offensive" message through a computer or communication device. The provision was widely criticised for its vague and overbroad language and was frequently misused to arrest individuals for posting critical comments against politicians and public figures. Although Section 353 is more narrowly drafted than Section 66A, concerns remain that it could still be misused to target legitimate political or economic commentary. This may send a chilling effect on free speech, and it may inhibit the role of the population to hold strong institutions accountable.

Section 319 of the BNS, which corresponds to Section 416 of the IPC, criminalizes cheating by personation.[52] The section states that "whoever cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both." The section defines "personation" as "the act of pretending to be some other person, or of knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.[53] Any activity of using deepfakes as a means of deceiving C-suite executives with the aim of influencing stock prices would come squarely under the understanding of the term as cheating by personation. The process of creating and sharing a deepfake of a CEO, say, would entail the act of impersonation of the CEO, and the desire to make investors purchase or sell a specific stock

[51] *Shreya Singhal v Union of India* (2015) 5 SCC 1 [96].
[52] Bharatiya Nyaya Sanhita 2023, s 319.
[53] ibid s 3(40).

would amount to the element of cheating.[54] Nevertheless, a number of obstacles are expected to arise when prosecutors take cases under Section 319. To begin with, it can be challenging to show that the accused had the intention of cheating, rather than just performing a prank or a political satire. Second, a causal connection between the deepfake and subsequent financial loss may be hard to determine, especially in a turbulent and uncertain market.[55]

Section 319 is not the only area of law where proving intent and causation in a synthetic media case is difficult. These are the issues that are prevalent in any form of financial fraud. Nevertheless, it can become even harder to obtain the required evidence with the help of AI and other high technologies. To give an example, one may find it hard to determine the source of a deepfake video, and it may be hard to recognize the people standing behind the creation and distribution of the video.[56] Encryption and other privacy-enhancing technology may make it even more difficult to investigate and prosecute such cases.

### *A. The Evolving Jurisprudence on Deepfake Liability*

The legal framework on deepfake liability in India is still evolving. While the Bharatiya Nyaya Sanhita (**'BNS'**) and the IT Act provide a starting point for prosecuting those who misuse deepfakes, many critical questions remain unanswered and will ultimately have to be settled by the courts. This section examines the emerging jurisprudence on deepfake liability and highlights the key legal issues likely to arise in the coming years.

---

[54] Indian Penal Code 1860, s 415.

[55] Chandra and others, *Reducing Risks Posed by Synthetic Content* (n 42).

[56] United Nations Office on Drugs and Crime, *Emerging threats in Southeast Asia – Exploitation of AI and automation in the regional cybercrime landscape* (29 September 2025) <www.unodc.org/unodc/frontpage/2025/September/emerging-threats-in-southeast-asia--exploitation-of-ai-and-automation-in-the-regional-cybercrime-landscape.html> accessed 29 March 2026.

### *B. Context-Specific Recommendations and Critical Assessment*

In addition to broader reforms, three practical measures are proposed. First, SEBI must impose AI Disclosure Obligations upon material corporate communications of listed companies: any AI-assisted video, audio, or image must bear a cryptographically verifiable watermark listed in a SEBI-operated public registry, which speaks directly to the source of trust asymmetry that deepfake frauds take advantage of. Second, the current FSDC inter-regulatory framework should be extended with a new SEBI-MeitY Joint Enforcement Protocol, which would provide a co-regulatory mechanism of real-time evidence-sharing, and a rapid-track synthetic content takedown authority, in order to allow SEBI to impose binding removal orders on SSMIs, based on imminent harm to markets, and without requiring the standard Section 79 notice-and-takedown procedure. Third, CERT-In must create a National Deepfake Forensics Laboratory, in collaboration with the IIT system, which could act as the nodal authority in deepfake-related proceedings, and a forensic infrastructure that the BSA, 2023, assumes but which is currently not offered by any institution.[57]

These suggestions are not risk-free. Mandatory labelling and AI disclosure requirements have the risk of producing asymmetry in compliance, favoring less well-resourced platforms and creators, and potentially giving digital speech concentration to incumbent companies. The takedown mechanism has been fast-tracked without strong judicial checks and balances and may be repeated, the so-called chilling effect of now-latent Section 66A of the IT Act since it regulates legitimate financial commentary. Automated deep fake detection tools should be deployed on a large scale only with consequence-appropriate surveillance and data-protection protections, and with

[57] HM Government, *A pro-innovation approach to AI regulation* (n 43).

proportionality safeguards and autonomous auditing requirements. Lastly, legislation requirements exceeding institutional capacity development are likely to spur a false illusion of safety, which is ironic, more vulnerable between the instalment between the enforcement infrastructure development cycle and its maturity.[58]

### *C. The Need for Judicial Interpretation of BNS Provisions in the Digital Age*

The stipulations of the BNS do not have a clear purpose of dealing with the challenges of the digital era.[59] This, in turn, necessitates judicial interpretation to define the way these provisions would be interpreted to apply to the cases involving synthetic media. Indicatively, the courts will have to determine whether the term personation in Section 319 encompasses the use of deepfakes and whether the term public mischief in Section 353 encompasses the spread of fake news with the intent of controlling the price of stock.[60] The court cases that will be ruled on such matters will largely determine the capacity of law enforcement agencies to fight the increasing menace of fraud through synthetic media.

### *D. The Role of Precedent in Shaping Future Enforcement*

The cases that the courts resolve in the preliminary cases regarding deepfake liability will form valuable precedents that will be applied in the future. Such precedents will guide the work of the law enforcement agencies and prosecutors, and they will assist in the process of the law creation in this sphere. It is thus imperative that courts should be cautious and deliberate about

[58] Chandra and others, *Reducing Risks Posed by Synthetic Content* (n 42).
[59] Bharatiya Nyaya Sanhita 2023, ss 319, 353.
[60] *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 153.

the cases and the court should be sensitive to the fact that their ruling may have a long-term effect on the legal scene.

### *E. The Interplay Between the BNS and the IT Act, 2000*

Two distinct documents that can be used to solve the problem of deepfake liability are the BNS and the IT Act, 2000, which differ in many ways.[61] The general criminal law framework is offered by the BNS, and the IT Act offers specific provisions, which are applicable in cybercrime.[62] More should be clarified on how the two laws can interrelate with each other and when one should prosecute under one law as opposed to the other. This will require an analysis of the facts of each case that are specific, and more general policy objectives of the two laws.

### *F. Legal Grey Areas, Regulatory Ambiguities, and Enforcement Lacunae*

Regardless of their legislative purpose, the BNS, 2023 and the 2025 IT Rules contain major grey spaces that hinder their effectiveness in reality. The former is a matter of definitional ambiguity: the standard of content of the 2025 IT Rules, which is that it reasonably appears to be authentic or true, is subjective in nature and introduces an interpretative ambiguity, which encompasses political satire and lawful financial commentary, which would also lead to constitutional objection under Article 19(1)(a) as construed in *Shreya Singhal v. Union of India*. It is this flaw of definition that will eventually be resolved by the courts, rather than regulators, and the result will significantly influence the future of digital expression in India.

---

[61] Information Technology Act 2000, s 79(1).

[62] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, r 4, GSR 775(E), Gazette of India, Extraordinary, Part II, s 3(i) 22 October 2025.

The second grey area is the jurisdictional fragmentation. The division of regulatory responsibilities between SEBI, MeitY, Home Affairs, and the RBI, with no single coordination mechanism, creates conflicting enforcement priorities and allowable coverage loopholes, especially in cross-border activities where the speed of AI-driven market manipulation is slower than the MLAT processes. In the current form of the BNS, 2023 does not provide any extraterritorial jurisdiction against AI-generated content, which means that law enforcement agencies in India have no statutory means to pursue offenders acting in a different jurisdiction.

The third obstacle is forensic attribution. Even in cases of detected deepfake fraud, it is technically challenging to track synthetic media to a particular offender. India does not have specific deepfake forensic infrastructure at either the CERT-In or the NIA, in the sense that the progressive evidentiary framework of BSA assumes the capacity to detect and attribute deepfakes, which is not yet available to any domestic organization[63]. Lastly, the narrowing scope problem: the 2025 IT Rules were written in terms of the state of the art in deepfake technology, and do not address the new modalities of the phenomenon, such as real-time voice synthesis, AI-assisted financial analysis, or agentic systems of fraud, a structural feature of AI regulation that cannot be addressed through periodic revision but through adaptive regulation.

## V. SAFE HARBOUR IN PERIL: SSMI OBLIGATIONS AND THE LOSS OF IMMUNITY FOR AI- ENABLED FRAUD

One of the most important aspects of the modern internet is the law regulating the liability of the online intermediaries for user-created content. In India, the framework is primarily based on the provision of the Information

[63] United Nations Office on Drugs and Crime, *Emerging threats in Southeast Asia* (n 61).

Technology Act, 2000, Section 79[64] that has provided a safe harbour to the intermediaries in the country, as they are not liable under some circumstances in which the third-party contents appear. However, that has significantly shifted with the 2025 revisions of the IT Rules that impose additional and stricter obligations on Significant Social Media Intermediaries (SSMI) regarding the synthetically generated information. This has raised essential issues about the future of the safe harbour protection in India and the potential to hold the platforms to the AI-powered fraud. This part will examine the safe harbour in Section 79 of the IT Act, which is a new requirement for SSMIs and potential loss of immunity on a site that fails to satisfy their requirement.[65]

### *A. The Safe Harbour Provision under Section 79 of the IT Act*

In Section 79 of the IT Act, the intermediaries are given a safe harbour, in which they are not to be held responsible for any third-party information, data or communication link that is provided, hosted or made available by them. But this immunity is not absolute, and it does have a series of conditions. The middleman should not have started the transmission, chosen the recipient of the transmission, or chosen or altered the information in the transmission. The intermediary also has to practice due diligence in the process of performing its obligations under the Act, and also has a duty to observe such other provisions as the Central Government may specify in this regard.

### *B. The Conditions for Immunity for Intermediaries*

Section 79 of the IT Act has made the terms of immunity in an attempt to ensure that intermediaries are only used as neutral channels of information and are not involved in creating or propagating illegal content.[66] The condition that

[64] Information Technology Act 2000, s 79 (India).
[65] ibid s 79(1).
[66] Information Technology Act 2000, s 79.

the intermediary has not taken the initiative to send the transmission, or choose the recipient, or alter the information, is aimed at making sure that the intermediary is not a publisher or speaker of the content. The due diligence requirement, in its turn, is aimed at providing the intermediary with reasonable means of ensuring that the illegal content is not being spread through its platform. The rules that have been stipulated by the Central Government in this section present a more specific pattern to the due diligence responsibilities of the intermediaries.[67]

### *C. The "Notice and Takedown" Regime*

One of the sections of the safe harbour regime in the IT Act is the notice and takedown regime of Section 79.[68] In this regime, a middleman has to take down or otherwise hamper access to any illegal content when he has actual knowledge that this content is present on its platform. The real knowledge can be acquired upon a court order or a notification by the government agency.[69] The intermediary should be quick in deleting the content, and the inability to do so may lead to the forfeiture of safe harbour. It has attracted considerable controversy, and it has been argued that the regime currently places an unfair burden on intermediaries and is prone to censoring legitimate content.

### *D. The Impact of the 2025 IT Rules on Safe Harbour*

The amendments of the IT Rules of 2025 have made a great impact on the safe harbour framework, as it places and enforce new and more rigorous due diligence requirements on SSMIs. These commitments, which involve the necessity to acquire user expression on synthetic material, implement technical tools to validate these expressive, and conspicuously label all

[67] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, GSR 139(E).
[68] ibid.
[69] ibid.

synthetic material, outweigh the customary system of notice and takedown. Violation of such requirements may lead to the abrogation of safe harbour coverage, and the platform will be engaged in the criminal misconduct that is hosted on its service. That has raised a question mark, that the new rules would lead to the situation when platforms are left with no option but to undertake proactive content moderation, which can have a chilling effect on free speech.

### *E. The Obligations of Significant Social Media Intermediaries (SSMIs)*

The new requirements on SSMIs posed by the amendments of the 2025 IT Rules are likely to involve them as more active participants in combating the spread of synthetically created information. These requirements are a major shift in the historic regime of notice and takedown and are indicative of an increasing trend to hold platforms more responsible for the content they are hosting.

#### 1. A. THE REQUIREMENT FOR "REASONABLE AND APPROPRIATE TECHNICAL MEASURES"

The 2025 IT Rules demand that SSMIs implement technical measures, which are reasonable and appropriate to identify and delete synthetically generated information.[70] This is a major break with the much older and more traditional notice and takedown regime, where the platforms only needed to do something in response to actual knowledge of illegal content received. The new requirement imposes more competition on platforms to actively check their services as synthetic media. But the phrase reasonable and appropriate is not specified in the rules and will probably become the focus of numerous debates and litigation. The benefit of the platforms will be the creation and

[70] ibid.

implementation of a technical solution that would be efficient in identifying the synthetic media, without also labelling a substantial portion of the legitimate content.

#### 2. THE ROLE OF AUTOMATED TOOLS IN DETECTING SYNTHETIC CONTENT

At this point, automated tools would most likely be instrumental in assisting SSMIs to adhere to their new requirements in the 2025 IT Rules. One can scan big amounts of content with these tools to detect manipulation in the form of discrepancies in lighting, shadows, and facial expression. Nevertheless, all these tools are not so effective and cannot always determine authentic and fake content. Platforms will be faced with the challenge to come up with and implement automated tools that are accurate and efficient. The automated tools also have an issue of false positives, thus the possibility of loss of valid content.

#### 3. THE BURDEN OF VERIFYING USER DECLARATIONS

The IT Rules of 2025 demand that SSMIs request the user to declare every time they upload the content whether their message was written or edited with the help of AI or any other synthetic tool. Platforms are also required by the rules to put up tea-tincture technical measures that are reasonable and proportionate to confirm the correctness of these declarations. This heavily burdens the platforms because it will require them to create and deploy systems to check user claims on a large scale. Platforms will find it difficult to check such statements without violating the privacy of their customers as well. The overall load of authentication of user statements is probably one of the main problems that platforms will face in adherence to the new regulations.

### *F. The Loss of Immunity for AI-Enabled Fraud*

The amendments of the 2025 IT Rules have increased the chances of immunity loss to those platforms that do not meet their new requirements. This has brought controversy on how platforms and individual perpetrators of AI-enabled fraud should be held liable.

### 1. THE ARGUMENT FOR PIERCING THE CORPORATE VEIL OF INTERMEDIARIES

They claim that the safe harbour clause in the IT Act, Section 79, ought to be lifted in situations of AI-based fraud, and that the sites must be held directly responsible for the damages as a result of the synthetic media.[71] The point is that platforms have ceased to become a neutral conduit of information, but they are getting actively engaged in the creation and sharing of content using both their algorithms and recommendation systems. It is argued that because platforms fail to take sufficient measures to prevent the spread of synthetic media, they should be liable for negligence.

### 2. THE POTENTIAL FOR SHARED LIABILITY MODELS

Others insist that a shared liability model will be more suitable in AI-enabled fraud cases.[72] In this model, the platform would be liable along with the perpetrator individually who caused the harm by the synthetic media. The liability of the platform would consist in its inability to perform its due diligence duty, whereas the liability of the individual who carried the fraudulent content would be judged by their personal contribution to the generation and sharing of the scamming content. A shared liability model would offer a fairer analysis of how the liability should be distributed and

[71] *Shreya Singhal v Union of India* (2015) 5 SCC 1.

[72] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065> accessed 12 March 2026.

would make both platforms and individuals responsible in terms of committing AI-enabled fraud.

### 3. THE GLOBAL DEBATE ON PLATFORM ACCOUNTABILITY FOR AI-GENERATED CONTENT

The question of whether platforms should be held responsible or not regarding AI-generated content does not originate in India. It is an international controversy that is occurring in several jurisdictions, including the European Union[73] and the United States.[74] The result of this debate will be of interest in the future of the internet and control of online information. The dilemma presented by policymakers is to strike a balance between the necessity to safeguard users to ensure they are not hurt and the necessity not to destroy the open and free internet. The liability of the platform is likely to become a prime feature of the future policy and legal debate regarding the regulation of the artificially created content.

## VI. EVIDENCE AND ADMISSIBILITY: AUTHENTICATING SYNTHETIC MEDIA UNDER THE BHARTIYA SAKSHYA ADHINIYAM (BSA), 2023

The proliferation of deepfake technology has created a new and significant challenge for the legal system: what should be done to confirm digital evidence in man-made media. The possibility of creating audio, video and images that are fake but hyper-realistic has made it more difficult to tell which works are the original works and which are the counterfeit ones. It has great implications for the admissibility of digital evidence in a court because the credibility and authenticity of such evidence are doubted. The current legislation is the

[73] ibid.
[74] 47 USC § 230 (2018).

Bharatiya Sakshya Adhiniyam, 2023[75] (or the new name of the Indian Evidence Act, 1872), which has modulated the new set of rules in the admissibility of electronic and digital records. This section will contain the challenge of demonstrating deepfakes in the court, the provisions of the BSA, 2023 and the future of deepfake detection and authentication.

### *A. The Challenge of Authenticating Deepfakes in Court*

The authentication of deepfakes in a court is a challenging task. The deep fakes now are hyper- realistic, and it is in fact hard to tell the fake and the real by the human eye. This has taken the case to a point where even the expert witness would not, at times, be in a position to make a clear judgment of the validity of a particular piece of digital evidence.[76] The issue of detecting deepfakes is also augmented by the fact that the software is dynamically shifting; consequently, it is difficult to uncover the technology and keep pace.

#### 1. THE RELIABILITY OF DIGITAL EVIDENCE

The reliability of digital evidence has always been an issue in the legal system. The availability of digital files allowing duplication, editing and deletion at an extremely low rate has made it highly difficult to maintain a chain of custody, along with ensuring the integrity of the evidence. The emergence of deepfake technology has further contributed to these problems, since nowadays one can create very realistic fakes that are difficult to identify. One of the challenges that the legal system will face is the need to find new methods of certifying digital evidence that will take into consideration the risks presented by deepfakes.

---

[75] Bharatiya Sakshya Adhiniyam 2023.

[76] WeProtect Global Alliance, 'Deepfakes: A Human Challenge' (31 July 2024) <www.weprotect.org/wp-content/uploads/Deepfakes_A-Human-Challenge_PA-Report_v3.pdf> accessed 2 April 2026.

#### 2. THE NEED FOR EXPERT TESTIMONY AND FORENSIC ANALYSIS

The reliability of digital evidence has been an issue of concern to the legal system. The ease with which it is possible to copy, modify and delete digital files has made it highly difficult to have a chain of custody as well as ensure that the evidence is intact. The emergence of deepfake technology has just contributed to the problems since fakes can now be made very realistic and undetected. The legal system has the burden of devising new methods of examination of digital evidence that can consider the risks of deepfakes.

#### 3. THE ADMISSIBILITY OF AI-GENERATED EVIDENCE

The other more challenging question that will be forced to be addressed by the legal framework would be the admissibility of AI-made evidence. As AI keeps improving in the future, it is possible to anticipate that the application of AI-generated evidence in the court will rise. This can include, among others, AI to generate financial transaction reports or to filter large amounts of data. It will be hard to establish a framework in which the admissibility of AI-generated evidence will make it reliable and accurate for the legal system.

## VII. THE BHARATIYA SAKSHYA ADHINIYAM (BSA), 2023: A NEW FRAMEWORK FOR DIGITAL EVIDENCE

The new model on admissibility of electronic and digital records will be a new model named the Bharatiya Sakshya Adhiniyam (**'BSA'**), 2023, which replaced the Indian Evidence Act, 1872.[77] The fact that the BSA was introduced is a giant leap in the legal recognition of digital evidence, and the attitude towards the problems of synthetic media provided by the BSA is more contemporary and comprehensive.

### *A. The Provisions for Electronic and Digital Records*

[77] Bharatiya Sakshya Adhiniyam 2023.

There are a number of provisions in the BSA, 2023, which apply to the admissibility of electronic and digital records. Section 61 of the BSA provides that electronic or digital records will have the same legal enforceability and validity as records will paper-based records.[78] Section 62 provides that section information in an electronic record shall be deemed a document, and shall be admissible evidence, without the additional evidence of the original.[79] These provisions have provided a good legal basis for the admissibility of digital evidence before the court.

### *B. The Standard for Proving the Authenticity of Digital Evidence*

BSA, 2023, is also a standard that defines the required standard for establishing the authenticity of digital evidence. Evidence that can prove the authenticity of an electronic record may concern the identity of the person who created the record, the accuracy of the method applied in the creation of the record, and the integrity of the method applied in the creation of the record, provided under section 63 of the BSA.[80] This standard is less rigid than the traditional one that was used to show the authenticity of paper-based records, and it is more appropriate in a digital evidence setting.

### *C. The Role of Hash Values and Metadata in Establishing Chain of Custody*

The BSA, 2023, also recognises the importance of the hash values and metadata used in the chain of custody determination of the digital evidence. A hash value refers to a unique computerized fingerprint derived from a file. When a file is modified in any manner, the hash value will be different. This

[78] ibid s 61.
[79] ibid s 62.
[80] ibid s 63.

renders hash values a handy tool in the authentication of the integrity of a digital file.

Metadata is information that is stored within a file, and it gives information regarding the file, including creation date and time, device created, and application used to create it. Metadata may be a valuable instrument to define the authenticity of an electronic file.

## VIII. THE FUTURE OF DEEPAKE DETECTION AND AUTHENTICATION

The future of deepfake detection and authentication will probably feature the continuation of the arms race between deepfake creators and the detection technology developers. The more advanced deepfake technology is developed, the harder it will be to detect the forgeries with the help of traditional techniques. This will require new and more sophisticated detection technologies to be created. Various high-end detection technologies are being created to fight the menace of deepfakes. These technologies are based on a wide range of methods to identify the evidence of manipulation, including the analysis of the smallest discrepancies in faces, movements of the eyes and light, which are usually visible in deepfakes. Machine learning is also used in some of these technologies to detect patterns of deepfakes that cannot be detected using the human eye. These enhanced technologies in fraud detection will play an important role in combating deepfake fraud.

The internet is global; hence, the risk of deepfake fraud cannot be limited to a particular jurisdiction. This is why it becomes necessary to create international deepfake authentication standards. Such standards would offer a global basis for detecting and authenticating deepfakes, and would assist in successfully making sure that evidence can be accepted in global courts.

Governments, industry, and academia will have to coordinate their efforts to develop international standards of deepfake authentication.

## IX. CONCLUSION: BRIDGING THE LIABILITY GAP AND SAFEGUARDING ECONOMIC STABILITY

The 2025 crisis of synthetic media has revealed the abysmal inefficiencies of the contemporary financial apparatus in a novel and pernicious variety of white-collar crime. Impersonation of C-suite executives and market manipulation using AI-modified voices and deepfake videos is a paradigm shift in the character of financial fraud, which current legal and regulatory frameworks are failing to resolve. This paper has explored the so-called liability gap of Bharatiya Nyaya Sanhita (**'BNS'**), 2023, and the 2025 IT Rules, and has found that these instruments, while a step in the right direction, are insufficient to deter the kind of high-frequency, machine-speed market manipulation that is now possible.[81] It has further discussed the international character of the threat, which has necessitated the need to have a global response towards it. This conclusion sums up the focal findings of the study, justifies a more aggressive and responsive regulation strategy, and makes an appeal to a worldwide and coordinated effort of measures against the threat of synthetic market abuse.

The studies have also established that the current legal frameworks (both in India and in other areas of the world) are not suitable to handle the peculiarities of synthetic market abuse. The Criminal law and securities regulation tools used in the traditional set-up are not well-suited to deal with the pace, magnitude, and complexity of AI-based fraud. The liability gap that has now been created is a serious menace to the integrity of the market and investor trust, and the basic structure of our regulation of the financial system

[81] Bharatiya Nyaya Sanhita 2023.

is seriously amiss. The discussion of the BNS and the 2025 IT Rules has shown that they have several limitations in their capability to work with synthetic hype. The BNS provisions, however, are not specifically oriented towards the issues of synthetic media, and they are expected to be applied to deepfake fraud cases, with a complex and demanding task. Even though the 2025 IT Rules are a positive move towards the regulation of synthetic media, the rules have a narrow scope and minimal impact. Under the context of the discussion manifested in the paper, the following recommendations are being proposed to ensure the situation is workable to safeguard society and economic institutions against Synthetic Market Abuse: Deepfake Impersonation and Securities Fraud.

### *A. The Need for an Inter-Ministerial Coordinating Body for AI Fraud*

The comparative looks at the approaches to regulation in the world reveals that a united and all-inclusive reaction is necessary to the danger of synthetic market abuse in India. The modern legal and regulatory framework is disjointed and is not sufficient to address the issues of the digital age. There is a need to have a new body that is able to combine the experience of different government agencies and generate a holistic and proactive strategy to combat the AI-based financial crime. This paragraph is a proposal to establish an Inter-Ministerial Coordinating Body of AI Fraud, its proposed structure and its mandate.

#### 1. THE RATIONALE FOR A COORDINATED RESPONSE

Synthetic market abuse is a complex and multidimensional problem, which requires a concerted effort on the part of an immense number of governmental bodies. The Ministry of Finance, the Home Affairs, the Ministry of Electronics and Information Technologies and the Securities and Exchange Board of India (**'SEBI'**) are all in the battle against this menace. However,

currently, these agencies cannot collaborate in a structured manner in order to develop a common strategy. This has resulted in a disjointed and uncoordinated response to the problem, which has proved to be ineffective in discouraging and punishing deepfake offenders who use them to commit financial fraud. This gap could be resolved through the creation of an Inter-Ministerial Coordinating Body on AI Fraud that can facilitate the exchange of information among these agencies, coordinate their activities, and come up with a collective approach to this issue.

#### 2. THE PROPOSED STRUCTURE AND MANDATE OF THE BODY

It would be one of the high-level bodies to be headed by the finance minister, referred to as the Inter-Ministerial Coordinating Body on AI Fraud. It would also include the officials of the Ministry of Home Affairs, the Ministry of Electronics and Information Technology, the Ministry of Law and Justice and SEBI. This would place the burden on the body to develop a national strategy for combating AI-driven financial crime, and it would do the same for implementing it. The plan would involve different actions, which would include:

- Strengthening the legal and regulatory framework for combating AI-driven financial crime
- Enhancing the capacity of law enforcement agencies to investigate and prosecute these crimes
- Promoting public awareness of the risks of synthetic media

#### 3. THE ROLE OF INTERNATIONAL COOPERATION AND INFORMATION SHARING

Synthetic market abuse is a problem on the international level, and it needs an international solution. The establishment of an Inter-Ministerial

Coordination Body on AI Fraud would be one such platform through which India can coordinate with other countries and international organisations to develop a universal solution to the issue. The body would take the initiative of disseminating information and best practices to other nations and to organise Indian response to transnational terrorist financial crime. The organisation would also work with international organisations such as the IMF and the World Bank to develop global standards on the regulation of AI and to bring more countries on board in the war on AI-generated financial.

### 4. THE NEED FOR A HOLISTIC AND MULTI-FACETED APPROACH

This lack of legal frameworks proves that there is a need to have an increasingly cynical and multi-faceted approach to the regulation of synthetic market abuse. This approach should entail the combination of legal, technological and educational measures. The legal aspect of the problem of synthetic media demands the development of new laws that are developed specifically in reference to the issue. On the technological side, more advanced detection and authentication technology needs to be developed. The educational sphere is one area where a greater number of individuals need to be informed about the harmfulness of synthetic media and the necessity of verifying the quality of information.

The danger of synthetic market abuse is not an issue of tomorrow; it is a current and increasing menace to the financial markets of the world. Even the instances of deepfake fraud that are already known about are a sobering notification of the possibility that this technology can result in major economic harm. The estimated 1.5-3 billion dollars of losses in India and other nations act as a wake-up call to the policymakers and regulators of the country. It is time to make a move prior to the risk of synthetic market abuse becoming a systemic risk to the global financial system.

### *B. The Path Forward: A Call for Proactive and Adaptive Regulation*

The way out must be a transition from a reactive to a proactive and adaptive attitude to the management of AI-based financial crime. This would mean looking to the future to see threats that are likely to arise, developing new regulatory tools and systems, and inculcating a culture of collaboration between government, industry, and academia.

#### 1. THE IMPORTANCE OF A RISK-BASED APPROACH TO AI-REGULATION

The regulation of AI in the future has to be grounded on a risk-based approach to address the various and evolving risks posed by synthetic media. Its methodology must focus on the specific threats of the different types of AI systems and applications, and should be adaptable to the forthcoming changes in the technology. Such a risk-based approach would enable regulators to deploy their resources more productively and would not result in a one-size-fits-all approach that would suppress innovation.

#### 2. THE NEED FOR CONTINUOUS MONITORING AND ADAPTATION OF LEGAL FRAMEWORKS

Intense dynamism in the change of technology implies that the legal regulations regarding the control of AI are to be regularly observed and modified. It also demands investment in continuous research and development, and a desire to re-examine and modify the current legislation and policies. It would be an important step in this regard to have a special institution like the proposed Inter-Ministerial Coordinating Body on AI Fraud.

#### 3. THE ROLE OF PUBLIC-PRIVATE PARTNERSHIPS IN COMBATING AI-DRIVEN FRAUD

The threat of AI-driven financial crime will require the use of public-private partnerships. The business sector possesses an arsenal of experience

and capabilities that can be utilized to work on this problem, and it is in a good place to create and implement new technologies to detect and stop deepfake fraud. The state, on the other hand, is free to exercise its legal powers and regulatory powers to enforce the law and to bring to book those who defy the law. The best fighting method to deal with this new menace will be a collaborative approach that would incorporate the best of the two sectors.

Synthetic market abuse is a worldwide menace that can only be solved worldwide. The cross-national character of the internet and the simplicity of the creation and distribution of deepfakes across borders create a situation where a single country cannot fight the menace on their own. An international reaction is necessary to ensure the integrity of the global financial system as well as to protect the interests of investors. The number of already identified cases of cross-border deepfake fraud is a good sign of how international the threat is. Malicious actors often use the tactic of using servers in one country to attack victims in another country. The ease and anonymity of the internet have rendered it a challenge for law enforcement to locate and punish the perpetrators of these crimes. The problem of cross-border deepfake fraud being inevitable implies that a purely domestic system of regulation will not be efficient. The world should have a combined international stand against artificial market exploitation for several reasons. First, it would enable the sharing of intelligence and best practices across countries. Second, it would make the prosecution and investigation of cross-border crimes easier. Third, it would assist in playing an even playing field for businesses and investors. The formation of a global treaty concerning transnational economic crime, as suggested in this paper, would be a milestone towards forming a unified global front against this new menace.

The era of AI will imply the need to reconsider the manner in which we go about the regulation of finance. The conventional means of control can no longer be adequate to deal with the problems of AI-based financial crime. It should be more adaptive, collaborative, and proactive. It will involve making an investment in innovation, being open to considering a new regulatory framework, and recognising that the future of financial regulation will be constituted by the present discourse between technology and the law.[82] Our ability to overcome this challenge in the future will form the foundation of our financial system, and this will entail a holistic approach that draws on legal, judicial, financial, commercial, as well as technological systems and structures as a whole.

[82] Council of Europe, *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No 225, 17 May 2024) <https://rm.coe.int/1680afae3c> accessed 20 February 2026.