International Journal of Research Radicals in Multidisciplinary Fields (IJRRMF), ISSN: 2960-043X
Volume 5, Issue 2, July-December, 2026, Available online at: www.researchradicals.com

Deepfakes, Corporate Fraud and Securities Markets: Emerging Challenges for Corporate and Cyber Law

Monika Giri

M.A. LL.M.

ABSTRACT

The rapid advancement of artificial intelligence (AI), particularly generative AI and deepfake technologies, has created new dimensions of risk for corporate governance, financial integrity and securities markets. Deepfakes can manipulate audio, video, images and digital communications to impersonate corporate executives, fabricate announcements, distort market information and influence investor behaviour. Their increasing accessibility presents significant challenges for corporate and cyber law because conventional mechanisms of fraud detection, authentication, disclosure and liability may be inadequate to address technologically sophisticated deception. This paper examines the emerging relationship between deepfakes, corporate fraud and securities-market misconduct, with particular emphasis on the legal and regulatory challenges arising from AI-generated misinformation.

It analyses how deepfakes may facilitate insider trading, market manipulation, fraudulent corporate disclosures, phishing, executive impersonation, unauthorised transactions and reputational harm. The study further evaluates the adequacy of existing corporate and cyber-law frameworks, particularly the Companies Act, 2013, Securities and Exchange Board of India (SEBI) regulations, Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, alongside emerging international approaches to AI governance and digital fraud. The paper argues that effective regulation requires a coordinated framework combining corporate accountability, cybersecurity safeguards, AI-generated-content detection, platform responsibility, investor protection and technologically informed evidentiary standards. It concludes that deepfake-enabled corporate fraud represents not merely a technological threat but a multidimensional legal challenge requiring adaptive regulation, stronger disclosure mechanisms and enhanced institutional capacity to preserve market confidence and corporate transparency.

Keywords: Deepfakes; Corporate Fraud; Securities Markets; Cyber Law; Artificial Intelligence.

INTRODUCTION

The rapid development of artificial intelligence ("AI"), machine learning and generative AI has fundamentally altered the manner in which information is created, disseminated and consumed. Among the most significant technological developments is the emergence of "deepfakes", referring broadly to synthetic or manipulated audio-visual content generated or modified through AI techniques so as to imitate real persons, events or communications. While deepfake technology has legitimate applications in entertainment, education, advertising and digital communication, its misuse has created serious legal and regulatory concerns. The ability to reproduce a corporate executive's face, voice, mannerisms or communication style with increasing realism creates a new avenue for deception, impersonation and fraud. In the corporate environment, such technology can be employed to fabricate statements attributed to chief executive officers, directors, financial advisers or regulators, thereby creating false impressions regarding corporate performance, mergers, acquisitions, financial results, regulatory approvals or investment opportunities. The resulting harm is particularly serious in securities markets because market prices are highly sensitive to information and investor perceptions.[1]

The problem becomes more significant because contemporary securities markets operate within an information-intensive digital environment in which corporate announcements, interviews, investor communications and social-media posts can rapidly influence investment decisions. A fabricated video showing the chief executive of a listed company announcing exceptional profits, a major acquisition or a strategic restructuring may circulate across social-media platforms within

[1] Securities and Exchange Commission, North American Securities Administrators Association & Financial Industry Regulatory Authority, *Artificial Intelligence (AI) and Investment Fraud: Investor Alert* (25 January 2024), explaining that AI-generated audio, images and videos can be used to impersonate company executives and disseminate false information for securities-price manipulation, available at: SEC Investor Alert on Artificial Intelligence and Investment Fraud (accessed 2 August 2026).

minutes. Investors who perceive the communication as authentic may buy or sell securities before the information is verified, thereby generating artificial price movements. The United States Securities and Exchange Commission ("SEC"), together with the North American Securities Administrators Association and the Financial Industry Regulatory Authority, has expressly warned investors that AI can be used to create deepfake videos and audio, impersonate corporate executives and disseminate false information capable of manipulating securities prices.[2] The regulatory concern therefore extends beyond conventional cybercrime because deepfakes can directly interfere with the informational foundations upon which efficient and fair securities markets depend.

Deepfake-enabled fraud also transforms traditional corporate impersonation and social-engineering attacks. Earlier forms of cyber fraud frequently relied upon forged emails, stolen passwords, phishing websites or written instructions. Deepfake technology can add an apparently authentic human identity to the fraudulent communication. A fraudster may impersonate a chief financial officer and instruct an employee to transfer corporate funds, imitate a director during a virtual meeting, or create a false video message supposedly approving a transaction. The danger lies in the psychological authority attached to familiar faces and voices. Consequently, conventional authentication based merely on visual or auditory recognition is increasingly inadequate. The Securities and Exchange Board of India ("SEBI") has also recognised deepfake-related financial fraud as an emerging investor-protection concern and provides educational material warning investors about fabricated videos and other AI-enabled financial scams.[3]

Deepfakes, Corporate Fraud and Manipulation of Securities Markets

The intersection between deepfakes and corporate fraud raises important questions concerning the meaning of deception, fraudulent intent, material misrepresentation and market manipulation. In India, the SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003 ("PFUTP Regulations") provide a particularly important regulatory foundation. Regulation 3 prohibits fraudulent dealings in securities and the use of manipulative or deceptive devices in connection with securities. Regulation 4 further prohibits manipulative, fraudulent and unfair trade practices and encompasses conduct capable of creating a false or misleading appearance of trading and the dissemination of information that is untrue or not believed to be true.[4] The continuing development of the PFUTP framework is significant because SEBI's regulatory architecture must remain capable of responding to technologically sophisticated methods of market deception. The PFUTP Regulations were most recently amended on 5 December 2025, illustrating the continuing evolution of India's securities-market regulatory framework.[5]

Deepfakes can potentially fall within this regulatory framework when fabricated content is intentionally disseminated to influence the price of securities or investor behaviour. For example, an AI-generated video falsely depicting the managing director of a listed company announcing a significant contract may cause investors to purchase shares at artificially inflated prices. Conversely, a fabricated announcement concerning regulatory action, financial losses, insolvency or resignation of key management personnel could trigger panic selling and an artificial decline in the market price. Where such conduct is accompanied by trading undertaken by the creator or collaborators of the deepfake, the relationship between technological manipulation and securities-market fraud becomes particularly direct. The essential legal difficulty is not necessarily the absence of broad prohibitions against fraudulent conduct; rather, it concerns attribution, proof of intention, identification of the creator, preservation of digital evidence and establishment of the causal relationship between synthetic content and market impact.

Corporate law provides another layer of protection against fraudulent conduct. Section 447 of the Companies Act, 2013 defines fraud broadly in relation to the affairs of a company and covers acts, omissions, concealment of facts and abuse of position committed with an intention to deceive, obtain undue advantage or injure the interests of the company, shareholders, creditors or other persons.[6] Section 448 further imposes liability where a person knowingly makes a

[2] Ibid., noting that fraudsters may employ AI-generated audio and video to impersonate corporate executives and spread false information capable of influencing securities prices (accessed 2 August 2026).
[3] Securities and Exchange Board of India, *SEBI Investor Education – DeepFake and Financial Fraud*, SEBI Investor, available at: SEBI Investor Education Resources on Deepfake Financial Fraud (accessed 3 August 2026).
[4] Securities and Exchange Board of India, *Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003*, regs. 3–4, available at: SEBI PFUTP Regulations, 2003 (accessed 3 August 2026).
[5] Securities and Exchange Board of India, *Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003*, last amended 5 December 2025, available at: SEBI PFUTP Regulations – Latest Amended Version (accessed 4 August 2026).
[6] The Companies Act, 2013, No. 18 of 2013, § 447, India Code, defining fraud in relation to the affairs of a company and prescribing punishment for fraud, available at: India Code – Section 447, Companies Act, 2013 (accessed 4 August 2026).

materially false statement or knowingly omits a material fact in a return, report, certificate, financial statement, prospectus or other document required under the Act.[7] These provisions become relevant where AI-generated material is incorporated into corporate communications, investor disclosures or documentation, or where directors, officers or other persons knowingly use manipulated information to deceive investors or obtain an advantage.

The Companies Act also recognises the seriousness of fraudulent inducement in securities transactions. Section 36 addresses fraudulent inducement of persons to invest money and covers knowingly or recklessly making false, deceptive or misleading statements or deliberately concealing material facts for the purpose of inducing persons to acquire, dispose of, subscribe for or underwrite securities.[8] Thus, deepfake-enabled corporate fraud may potentially intersect with company-law liability where synthetic information is deliberately deployed as part of an investment solicitation or corporate transaction. The legal challenge, however, lies in adapting established concepts of responsibility to circumstances in which the person appearing to communicate may have neither created nor authorised the communication.

Cyber-Law Challenges, Regulatory Gaps and the Need for an Integrated Framework

The cyber-law dimension of deepfake-enabled corporate fraud is equally significant. The Information Technology Act, 2000 contains provisions that can become relevant where deepfake operations involve identity theft, impersonation or computer-based cheating. Section 66C addresses fraudulent or dishonest use of another person's electronic signature, password or unique identification feature, while section 66D criminalises cheating by personation through a communication device or computer resource.[9] These provisions can provide a legal basis in cases where an offender digitally impersonates a corporate officer or another individual for fraudulent purposes. Nevertheless, the statutory framework predates contemporary generative AI and was not specifically designed to address synthetic media capable of reproducing a person's face, voice and behavioural characteristics with exceptional realism.

The regulatory environment has nevertheless begun to respond to the synthetic-media problem. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have undergone significant amendments, including amendments notified in February 2026 concerning synthetically generated information ("SGI").[10] The evolving framework reflects an increasing emphasis on identification, transparency and intermediary responsibilities concerning AI-generated content. Such developments are particularly relevant to securities markets because a deepfake may originate outside a regulated financial intermediary but may nevertheless rapidly reach millions of investors through social-media platforms.

The Digital Personal Data Protection Act, 2023 also assumes relevance where the creation of deepfakes involves the unauthorised processing of personal data, including identifiable facial or other personal information. The Act seeks to regulate the processing of digital personal data while recognising the need to balance individual data protection with lawful data processing.[11] Although the statute is not a dedicated deepfake law, its principles may contribute to a broader legal framework concerning the acquisition and processing of personal information used to create synthetic identities.

The principal challenge, therefore, is fragmentation. Deepfake-enabled securities fraud can simultaneously involve corporate law, securities regulation, cybercrime, data protection, intermediary regulation and evidentiary law. A single fabricated video may constitute impersonation, misinformation, securities manipulation and reputational harm depending upon its purpose, dissemination and consequences. Enforcement agencies must consequently establish mechanisms for rapid verification of corporate communications, preservation of metadata and digital evidence, coordinated investigation between SEBI and cybercrime authorities, and effective cooperation with social-media intermediaries and technology

[7] The Companies Act, 2013, No. 18 of 2013, § 448, concerning liability for knowingly making materially false statements or omitting material facts in documents required under the Act, available at: India Code – Section 448, Companies Act, 2013 (accessed 4 August 2026).
[8] The Companies Act, 2013, No. 18 of 2013, § 36, concerning fraudulent inducement of persons to invest money through false, deceptive or misleading statements or concealment of material facts, available at: The Companies Act, 2013 – Official Text (accessed 5 August 2026).
[9] The Information Technology Act, 2000, No. 21 of 2000, §§ 66C–66D, India Code; section 66C concerns identity theft and section 66D concerns cheating by personation through a communication device or computer resource, available at: India Code – Information Technology Act, 2000 (accessed 5 August 2026).
[10] Ministry of Electronics and Information Technology, Government of India, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, as amended, including provisions concerning synthetically generated information, available at: MeitY – Information Technology Rules, 2021 (accessed 5 August 2026).
[11] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Ministry of Electronics and Information Technology, Government of India, available at: Digital Personal Data Protection Act, 2023 – Official Text (accessed 5 August 2026).

providers. Investor education is equally important because deepfake technology undermines the traditional assumption that visual or auditory evidence is inherently reliable.[12]

The emerging legal landscape therefore requires a shift from a purely content-based approach towards a technologically informed system of accountability. Corporate entities should develop authenticated communication channels, multi-factor verification mechanisms and internal protocols for responding to fabricated executive communications. Stock exchanges and regulators may need stronger systems for rapidly verifying suspicious corporate announcements and communicating authentic information to investors. Intermediaries should also develop mechanisms capable of identifying and responding to synthetic financial content without unnecessarily suppressing legitimate expression. Ultimately, the central challenge is to preserve the integrity of securities markets in an environment in which the distinction between genuine and artificially generated information is increasingly difficult to establish. Deepfakes consequently represent not merely a new form of cyber deception but a structural challenge to corporate transparency, investor protection, market integrity and the evidentiary assumptions underlying modern financial regulation.

RESEARCH OBJECTIVES

1.
2. To examine the emerging role of deepfake technology in facilitating corporate fraud, securities-market manipulation and cyber-enabled financial deception, with special reference to the Indian legal framework.
3. To critically evaluate the adequacy of existing corporate, securities and cyber laws in addressing deepfake-related misconduct and suggest measures for strengthening investor protection, corporate accountability and market integrity.

RESEARCH METHODOLOGY

The present study adopts a mixed research methodology to examine the emerging challenges posed by deepfakes, corporate fraud and securities-market manipulation. The research primarily relies upon secondary sources, including statutes, regulations, judicial decisions, regulatory circulars, government reports, policy documents, academic articles, books and authoritative online resources. Particular emphasis is placed on the Companies Act, 2013, Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, SEBI Act, 1992, and SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003. Relevant international regulatory developments are also examined comparatively to identify emerging approaches to AI-generated fraud and synthetic media. The study analyses selected contemporary cases, regulatory interventions and deepfake-related incidents to understand their implications for corporate governance, investor protection and securities-market integrity. The collected material is critically analysed through a descriptive, comparative and interpretative approach to identify legal gaps and propose appropriate reforms for addressing deepfake-enabled corporate and cyber fraud.

ANALYSIS AND FINDINGS

1. Deepfakes as an Emerging Instrument of Corporate Fraud and Securities-Market Manipulation

The first objective of the study is to examine the emerging role of deepfake technology in facilitating corporate fraud, securities-market manipulation and cyber-enabled financial deception. The doctrinal analysis indicates that deepfakes have transformed conventional fraud from a predominantly text-based or identity-based activity into a technologically sophisticated form of synthetic impersonation. Artificial intelligence can now generate convincing audio, images and videos capable of reproducing the appearance and voice of corporate executives, investment professionals and public officials. The United States Securities and Exchange Commission ("SEC") has specifically warned that fraudsters may use AI-generated videos to impersonate the chief executive officer of a company and announce false corporate information in order to manipulate the price of securities.[13] This development is particularly significant because securities markets are fundamentally dependent upon the timely availability and perceived authenticity of information.

The potential market consequences are substantial. A fabricated announcement that a listed company has obtained a major contract, achieved extraordinary profits, acquired another company or received regulatory approval may create artificial

[12] Securities and Exchange Board of India, *SEBI Investor Education Resources*, addressing deepfake videos, fake stock tips and digitally enabled investment fraud, available at: SEBI Investor Education Portal (accessed 5 August 2026).

[13] U.S. Securities and Exchange Commission, North American Securities Administrators Association & Financial Industry Regulatory Authority, *Artificial Intelligence (AI) and Investment Fraud: Investor Alert*, noting that fraudsters may use AI-generated audio and video to impersonate corporate executives and manipulate stock prices, available at: Investor.gov – Artificial Intelligence and Investment Fraud (accessed 2 August 2026).

optimism among investors. Conversely, a fabricated announcement concerning insolvency, regulatory investigation, resignation of senior management or financial losses may trigger panic selling. In both situations, the deepfake becomes an instrument for manipulating market expectations. The problem is intensified by social-media platforms, where information can reach a large number of investors before a listed company, stock exchange or regulator has an opportunity to authenticate it. The SEC has accordingly identified AI-enabled investment fraud and deepfake impersonation as emerging threats to investors.[14]

The Indian regulatory framework already contains sufficiently broad principles to potentially capture many forms of deepfake-enabled securities fraud. Regulation 3 of the Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003 ("PFUTP Regulations") prohibits fraudulent dealings, manipulative or deceptive devices, schemes or artifices to defraud and conduct that operates as fraud or deceit in connection with securities.[15] The definition of "fraud" under the Regulations is also extensive and includes knowing misrepresentation, concealment of material facts, false statements and misinformation affecting the market price of securities.[16] Therefore, the fact that a fraudulent communication is created through generative AI rather than through conventional methods should not, by itself, prevent regulatory intervention.

The Supreme Court's decision in *SEBI v. Rakhi Trading Pvt. Ltd.* provides an important jurisprudential foundation for this approach. The Court emphasised that "fairness, integrity and transparency" constitute hallmarks of the Indian securities market and upheld regulatory intervention against transactions designed to create artificial market activity.[17] The Court further recognised that apparently legitimate screen-based transactions can constitute manipulative conduct when the surrounding circumstances establish a meeting of minds and a predetermined strategy.[18] The principle is particularly relevant to deepfakes because technological sophistication cannot convert an otherwise fraudulent purpose into legitimate market activity. If a synthetic video or audio communication is deliberately created and disseminated to generate an artificial market response, the underlying conduct may fall within the logic of the PFUTP framework.

A further illustration is found in *SEBI v. Kanaiyalal Baldev Patel*, concerning front-running and the misuse of confidential trading information. The matter demonstrates the willingness of securities authorities and courts to examine the substance of conduct rather than merely its formal appearance. In 2024, the SEBI Special Court, Mumbai convicted Kanaiyalal Baldev Patel under section 24(2) of the SEBI Act and imposed three years' simple imprisonment and a fine of ₹10 lakh.[19] Although the case did not involve deepfakes, its significance for the present study lies in the principle that sophisticated methods of obtaining or exploiting market-sensitive information can attract serious liability where they undermine market integrity. Deepfake-enabled manipulation similarly requires regulators to examine the purpose, source, dissemination and trading consequences of synthetic information rather than concentrating exclusively on the technological mechanism through which the content was produced.

2. Corporate-Law Liability and Deepfake-Induced Deception

The second dimension concerns the relationship between deepfakes and corporate fraud under Indian company law. The Companies Act, 2013 contains several provisions that can potentially address fraudulent conduct involving AI-generated communications. Section 447 provides a broad statutory definition of fraud and prescribes substantial punishment where fraud is established.[20] The provision is particularly relevant to deepfake-enabled corporate misconduct because fraud under

[14] Ibid.; see also U.S. Securities and Exchange Commission, *Beware of Fraudsters Impersonating Investment Professionals and Firms – Investor Alert*, 11 December 2024, available at: Investor.gov – Investment Professional Impersonation Alert (accessed 2 August 2026).

[15] Securities and Exchange Board of India, *SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003*, regs. 3–4, available at: SEBI – PFUTP Regulations, 2003 (accessed 2 August 2026).

[16] Ibid., reg. 2(1)(c), defining "fraud" to include knowing misrepresentation, concealment of material facts, false statements and misinformation affecting the market price of securities (accessed 2 August 2026).

[17] *Securities and Exchange Board of India v. Rakhi Trading Pvt. Ltd.*, (2018) 13 SCC 753, Supreme Court of India, available at: SEBI v Rakhi Trading – Supreme Court Judgment (accessed 3 August 2026).

[18] Ibid. The Supreme Court held that non-genuine and synchronised transactions capable of creating artificial market activity may constitute manipulative and deceptive devices notwithstanding their execution through an apparently anonymous screen-based trading system (accessed 3 August 2026).

[19] *SEBI v. Kanaiyalal Baldev Patel*, SEBI Special Case No. 1592 of 2021, Judgment dated 23 April 2024, SEBI Special Court, Mumbai; the accused was convicted under section 24(2) of the SEBI Act and sentenced to three years' simple imprisonment with a fine of ₹10 lakh, available at: SEBI – Judgment in Kanaiyalal Baldev Patel (accessed 3 August 2026).

[20] The Companies Act, 2013, No. 18 of 2013, § 447, *Punishment for Fraud*, India Code, available at: India Code – Section 447, Companies Act 2013 (accessed 3 August 2026).

company law is not restricted to conventional documentary forgery. Acts, omissions, concealment and abuse of position may fall within its scope when accompanied by the requisite fraudulent intention.

Section 448 of the Companies Act becomes relevant where false statements or material omissions are knowingly incorporated into documents required under the legislation.[21] In a hypothetical deepfake scenario, a fabricated executive communication might subsequently be used to support a misleading corporate disclosure, investor communication or other statutory document. Liability would then potentially arise independently of the technical process used to create the original synthetic content. Similarly, section 36 concerning fraudulent inducement of persons to invest may become relevant where deceptive representations are deliberately employed to induce investors to acquire or subscribe to securities.

The legal challenge, however, becomes considerably more complicated where the person whose face or voice appears in the deepfake neither created nor authorised the communication. Traditional corporate accountability mechanisms generally assume that a communication can be attributed to the individual or entity appearing to make it. Deepfakes undermine this assumption. A fabricated video may appear to be an official statement by a managing director even though the director had no knowledge of its creation. Consequently, regulators and courts must distinguish between the apparent speaker, the actual creator, persons who disseminated the content, persons who traded upon it and intermediaries that hosted or amplified it.

The case study of the Arup deepfake fraud demonstrates this attribution problem particularly clearly. In 2024, employees at the Hong Kong office of the British engineering company Arup were deceived during a video conference in which fraudsters used AI-generated representations of senior executives and colleagues. Approximately HK$200 million, equivalent to about US$25 million, was transferred through multiple transactions.[22] The incident did not constitute securities-market manipulation in the narrow sense, but it provides an important corporate-fraud case study because the attack exploited the authority and trust associated with senior management. The incident demonstrates that deepfakes can bypass traditional employee authentication mechanisms by manufacturing an apparently legitimate corporate environment rather than merely sending a fraudulent email.

The Arup case has direct implications for corporate governance. First, corporate policies based solely on recognition of a senior executive's face or voice are increasingly unreliable. Secondly, financial controls must operate independently of digital identity. Thirdly, high-value transactions should require secondary authentication through an independently verified communication channel. Finally, corporate boards and audit committees should recognise AI-enabled impersonation as an enterprise-risk issue rather than treating it solely as an information-technology problem.

3. Cyber-Law Framework and Evidentiary Challenges

The third area of analysis concerns the adequacy of Indian cyber law. Sections 66C and 66D of the Information Technology Act, 2000 provide important statutory tools. Section 66C addresses identity theft, whereas section 66D addresses cheating by personation through a communication device or computer resource.[23] A deepfake in which a fraudster impersonates a corporate executive could therefore potentially attract section 66D where the statutory ingredients of cheating and personation are established.

Nevertheless, the Information Technology Act was enacted in 2000, long before contemporary generative AI systems could produce highly realistic synthetic media. Its provisions are consequently technology-neutral rather than deepfake-specific. This creates both an advantage and a limitation. Technology-neutral provisions can potentially cover new forms of cybercrime without constant legislative amendment, but they may not adequately address questions relating to synthetic-media provenance, labelling, platform responsibilities, algorithmic generation and the evidentiary authentication of AI-generated content.

India's regulatory response has recently become more technologically specific. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were amended in February 2026 to introduce provisions

[21] The Companies Act, 2013, § 448, relating to punishment for false statements, available through India Code, available at: India Code – Companies Act, 2013 (accessed 3 August 2026).
[22] *Arup deepfake fraud case*, involving the use of AI-generated representations of corporate executives during a video conference and the transfer of approximately US$25 million from the company's Hong Kong office, reported by the *Financial Times*, available at: Financial Times – Arup Deepfake Fraud Case (accessed 4 August 2026).
[23] The Information Technology Act, 2000, No. 21 of 2000, §§ 66C–66D, India Code, concerning identity theft and cheating by personation using a communication device or computer resource, available at: India Code – Information Technology Act, 2000 (accessed 4 August 2026).

concerning "synthetically generated information" ("SGI").[24] The amended framework defines SGI in relation to artificially or algorithmically created, generated, modified or altered audio, visual or audio-visual information that appears reasonably authentic or true.[25] The regulatory approach is significant because it recognises that synthetic content itself presents a regulatory problem rather than merely treating the resulting unlawful act as ordinary cybercrime.

The policy materials surrounding the SGI framework have emphasised labelling, visibility, metadata and technical measures for identifying synthetic content.[26] These requirements can become particularly important in securities markets. If an AI-generated corporate video carries an appropriate synthetic-content indicator, investors may be less likely to treat it as an authentic corporate announcement. However, labelling alone cannot solve the problem where malicious actors deliberately remove or circumvent such indicators. Effective regulation therefore requires cooperation among technology platforms, listed companies, stock exchanges, regulators and law-enforcement agencies.

Evidence represents another major challenge. In conventional fraud, an investigator may establish authorship through emails, documents, IP addresses, financial records or witness testimony. In deepfake cases, the content itself may initially appear to constitute evidence against an innocent person because the person's face and voice are reproduced. Courts therefore require technologically competent forensic evidence capable of establishing whether a particular recording is genuine, manipulated or AI-generated. Metadata, source-device information, creation history, server logs, platform records and expert forensic analysis may become increasingly important in establishing authenticity and attribution.

The problem also intersects with privacy and data protection. Deepfake creation frequently requires access to a person's photographs, videos, voice recordings or other identifying information. The Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognised privacy as a constitutionally protected fundamental right and emphasised the importance of informational privacy.[27] The misuse of an individual's biometric or identifying characteristics to create synthetic representations can therefore raise issues extending beyond fraud and reputation to personal autonomy and informational control.

4. Case Studies and Comparative Regulatory Lessons

International experience provides useful comparative lessons. The Arup incident demonstrates the danger of deepfake-enabled internal corporate fraud, while SEC investor alerts demonstrate the securities-market dimension of AI impersonation. The SEC has warned that fraudsters may impersonate investment professionals, create fraudulent websites and use social media to target investors.[28] This indicates that deepfake fraud is not confined to listed-company announcements but may also operate through fake investment advisers, brokers and financial professionals.

A particularly important regulatory development is the European Union's approach under the EU Artificial Intelligence Act. Article 50 establishes transparency obligations concerning certain AI-generated or manipulated content, including requirements designed to inform users where content has been artificially generated or manipulated.[29] The European

[24] Ministry of Electronics and Information Technology, Government of India, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, updated pursuant to the February 2026 amendments relating to synthetically generated information, available at: MeitY – IT Rules, 2021 (accessed 4 August 2026).

[25] Ministry of Electronics and Information Technology, Government of India, *Frequently Asked Questions – Amendments to IT Rules, 2021 relating to Synthetically Generated Information*, explaining the statutory definition of "synthetically generated information" and "audio, visual or audio-visual information", available at: MeitY – SGI Amendment FAQs (accessed 4 August 2026).

[26] Ministry of Electronics and Information Technology, Government of India, *Explanatory Note: Draft Amendments to IT Rules, 2021 relating to Synthetically Generated Information*, identifying labelling, visibility, metadata embedding and technical verification as important regulatory measures, available at: MeitY – SGI Explanatory Note (accessed 4 August 2026).

[27] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, Supreme Court of India, recognising privacy as a fundamental right protected under Articles 14, 19 and 21 of the Constitution, available at: Puttaswamy Judgment – Privacy Rights (accessed 5 August 2026).

[28] U.S. Securities and Exchange Commission, *Beware of Fraudsters Impersonating Investment Professionals and Firms*, supra note 2, explaining that technological advances including AI have increased the sophistication of impersonation schemes involving investment professionals and firms, available at: Investor.gov – Impersonation Schemes (accessed 5 August 2026).

[29] Regulation (EU) 2024/1689, *Artificial Intelligence Act*, art. 50, concerning transparency obligations for providers and deployers of certain AI systems and AI-generated or manipulated content, available at: European Union – Artificial Intelligence Act (accessed 5 August 2026).

approach illustrates a preventive model based upon transparency and identification. India's emerging SGI regime similarly moves towards labelling and technical identification, although its implementation must be evaluated in terms of proportionality, enforceability and its interaction with existing intermediary obligations.

The comparative analysis demonstrates that no single legal provision can comprehensively address deepfake-enabled corporate and securities fraud. Securities regulators are concerned primarily with market integrity and investor protection; corporate law focuses on directors, companies and fraudulent corporate conduct; cyber law addresses unauthorised computer-related activity and personation; data-protection law addresses the misuse of personal information; and intermediary regulation addresses dissemination and platform responsibilities. Deepfake incidents frequently cross all these categories simultaneously.

5. Assessment of Legal Adequacy and Emerging Regulatory Requirements

The analysis establishes that India's existing legal framework is capable of addressing a significant portion of deepfake-enabled fraud, but its effectiveness depends upon coordinated interpretation and enforcement. The PFUTP Regulations are sufficiently broad to potentially encompass fabricated information deliberately disseminated to deceive investors or influence securities prices. The Companies Act provides mechanisms for addressing corporate fraud and fraudulent inducement. The Information Technology Act provides offences relating to identity theft and cheating by personation, while the amended IT Rules introduce a more direct regulatory response to synthetic content.

However, three principal gaps remain. First, attribution remains difficult because the apparent speaker in a deepfake may be entirely innocent. Secondly, evidentiary standards and forensic capacity must evolve to establish authenticity and provenance. Thirdly, regulatory responsibilities remain distributed among several institutions. A deepfake securities attack may therefore require simultaneous action by SEBI, stock exchanges, cybercrime authorities, companies, intermediaries and technology platforms.

The jurisprudence in *Rakhi Trading* demonstrates that securities law can respond to technologically sophisticated manipulation when the underlying conduct compromises market integrity.[30] The lesson for deepfakes is that regulators should adopt a substance-oriented approach. The central inquiry should be whether the synthetic communication was deliberately created or disseminated to deceive, whether it was material to investors, whether it affected market behaviour and whether the responsible persons traded or obtained an advantage from the resulting distortion.

The study consequently finds that deepfake regulation should not be limited to criminalisation. Preventive corporate governance is equally important. Listed companies should maintain authenticated channels for corporate announcements, introduce independent verification for sensitive communications and establish rapid-response mechanisms for false AI-generated statements. Financial institutions and investment intermediaries should implement multi-channel authentication for high-value instructions. Stock exchanges should strengthen mechanisms for rapid verification of suspicious announcements. Regulators should develop specialised AI-forensics capacity, while platforms should maintain mechanisms for detecting, labelling and rapidly responding to synthetic financial content.

Overall, deepfakes represent a qualitative change in the nature of corporate and securities fraud. The technology does not necessarily create entirely new legal wrongs; rather, it enables existing wrongs to be committed with greater realism, speed, scale and anonymity. The principal legal challenge is therefore to ensure that established concepts of fraud, deception, manipulation, attribution and evidence remain effective when digital content can no longer be presumed authentic merely because it appears or sounds genuine. The preservation of investor confidence ultimately requires an integrated framework combining substantive securities regulation, corporate accountability, cybercrime enforcement, data protection, platform responsibility, technological authentication and investor awareness.

FINDINGS AND DISCUSSION

The study finds that deepfake technology has emerged as a significant enabler of corporate fraud, securities-market manipulation and cyber-enabled financial deception. The analysis demonstrates that AI-generated audio, video and images can impersonate corporate executives, investment professionals and other trusted individuals, thereby creating false information capable of influencing investor decisions and securities prices. The first research objective is therefore

[30] *SEBI v. Rakhi Trading Pvt. Ltd.*, (2018) 13 SCC 753, supra note 5. The Court emphasised that securities-market regulation must respond to ingenious forms of manipulation and that SEBI must develop principles capable of maintaining free and fair trading as market practices evolve (accessed 5 August 2026).

substantially established, as deepfakes can be used to facilitate fraudulent corporate announcements, investment scams, executive impersonation and market manipulation.

The findings further indicate that India's existing legal framework provides several mechanisms for addressing these emerging risks. The SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003, particularly Regulations 3 and 4, can potentially address deepfake-based dissemination of false or misleading information intended to manipulate securities markets. The Companies Act, 2013, especially Sections 36, 447 and 448, provides additional safeguards against fraudulent inducement, corporate fraud and materially false statements. Similarly, Sections 66C and 66D of the Information Technology Act, 2000 may apply to identity theft and cheating by personation through digital means.

However, the findings reveal significant regulatory and enforcement challenges. Attribution of responsibility is difficult because the individual depicted in a deepfake may be entirely innocent. Establishing authenticity, provenance and authorship also requires advanced digital-forensic capabilities. The study further finds that fragmented institutional responsibilities among corporate regulators, securities authorities, cybercrime agencies and digital intermediaries may delay effective responses. Therefore, a coordinated regulatory framework incorporating AI detection, authenticated corporate communications, stronger cybersecurity controls, digital evidence standards, intermediary accountability and investor awareness is necessary to preserve corporate transparency, investor protection and securities-market integrity.

The analysis demonstrates that Objective 1 is substantially established because deepfakes can facilitate executive impersonation, false corporate announcements, fraudulent investment solicitation and artificial securities-market movements. Objective 2 is also established: although the Companies Act, SEBI regulations, Information Technology Act and amended IT Rules provide significant legal tools, important challenges remain concerning attribution, AI-generated evidence, provenance, cross-platform dissemination, intermediary responsibility and rapid regulatory response. The emerging Indian framework therefore requires coordinated enforcement rather than reliance upon a single statute.

CONCLUSION

Deepfakes represent an emerging and technologically sophisticated threat to corporate governance, securities-market integrity and cyber-law enforcement. The study concludes that AI-generated audio, video and images can facilitate executive impersonation, fraudulent corporate communications, investment deception and securities-market manipulation by creating highly convincing but false information. India's existing framework, including the Companies Act, 2013, SEBI's PFUTP Regulations, the Information Technology Act, 2000 and the evolving regulatory framework concerning synthetically generated information, provides important legal mechanisms for addressing these risks. However, significant challenges remain regarding attribution, authentication, digital evidence, cross-platform dissemination and coordinated enforcement. The analysis demonstrates that conventional approaches to fraud and cybersecurity cannot independently address the speed, scale and sophistication of deepfake-enabled misconduct. A comprehensive response therefore requires stronger corporate verification systems, advanced AI-forensic capabilities, rapid regulatory intervention, intermediary cooperation and enhanced investor awareness. Ultimately, maintaining confidence in India's digital corporate and securities ecosystem requires the law to evolve alongside AI technology while balancing innovation, accountability, privacy and freedom of expression.

SUGGESTIONS

1. **Strengthen SEBI regulations** by expressly addressing AI-generated misinformation and deepfake-enabled securities-market manipulation.

2. **Establish corporate authentication protocols** requiring independent verification of sensitive communications issued by directors and senior executives.

3. **Develop AI-forensic capabilities** within SEBI, cybercrime authorities and law-enforcement agencies to detect, authenticate and trace deepfake content.

4. **Enhance intermediary accountability** by requiring prompt identification, labelling and removal of demonstrably fraudulent synthetic financial content.

5. **Strengthen digital evidence standards** to establish the origin, authenticity, manipulation and dissemination history of AI-generated material.

6. **Promote investor awareness** through regular SEBI campaigns concerning deepfake investment scams and fabricated corporate announcements.

7. **Encourage corporate cybersecurity training** for employees, directors and financial officers to reduce risks of AI-enabled impersonation and fraudulent transactions.

8. **Promote international cooperation** for investigating cross-border deepfake fraud, identifying perpetrators and preserving digital evidence.

FUTURE SCOPE

Future research may examine the effectiveness of India's evolving synthetic-media regulations, emerging judicial approaches to deepfake evidence, and comparative international frameworks. Empirical studies could assess investor awareness and corporate preparedness. Further research may also explore AI-forensic technologies, blockchain-based content authentication, intermediary liability and cross-border enforcement of deepfake-enabled securities fraud.

REFERENCES

1. Securities and Exchange Commission, North American Securities Administrators Association & Financial Industry Regulatory Authority, *Artificial Intelligence (AI) and Investment Fraud: Investor Alert* (25 January 2024), explaining that AI-generated audio, images and videos can be used to impersonate company executives and disseminate false information for securities-price manipulation, available at: SEC Investor Alert on Artificial Intelligence and Investment Fraud (accessed 2 August 2026).
2. Ibid., noting that fraudsters may employ AI-generated audio and video to impersonate corporate executives and spread false information capable of influencing securities prices (accessed 2 August 2026).
3. Securities and Exchange Board of India, *SEBI Investor Education – DeepFake and Financial Fraud*, SEBI Investor, available at: SEBI Investor Education Resources on Deepfake Financial Fraud (accessed 3 August 2026).
4. Securities and Exchange Board of India, *Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003*, regs. 3–4, available at: SEBI PFUTP Regulations, 2003 (accessed 3 August 2026).
5. Securities and Exchange Board of India, *Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003*, last amended 5 December 2025, available at: SEBI PFUTP Regulations – Latest Amended Version (accessed 4 August 2026).
6. The Companies Act, 2013, No. 18 of 2013, § 447, India Code, defining fraud in relation to the affairs of a company and prescribing punishment for fraud, available at: India Code – Section 447, Companies Act, 2013 (accessed 4 August 2026).
7. The Companies Act, 2013, No. 18 of 2013, § 448, concerning liability for knowingly making materially false statements or omitting material facts in documents required under the Act, available at: India Code – Section 448, Companies Act, 2013 (accessed 4 August 2026).
8. The Companies Act, 2013, No. 18 of 2013, § 36, concerning fraudulent inducement of persons to invest money through false, deceptive or misleading statements or concealment of material facts, available at: The Companies Act, 2013 – Official Text (accessed 5 August 2026).
9. The Information Technology Act, 2000, No. 21 of 2000, §§ 66C–66D, India Code; section 66C concerns identity theft and section 66D concerns cheating by personation through a communication device or computer resource, available at: India Code – Information Technology Act, 2000 (accessed 5 August 2026).
10. Ministry of Electronics and Information Technology, Government of India, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, as amended, including provisions concerning synthetically generated information, available at: MeitY – Information Technology Rules, 2021 (accessed 5 August 2026).
11. The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Ministry of Electronics and Information Technology, Government of India, available at: Digital Personal Data Protection Act, 2023 – Official Text (accessed 5 August 2026).
12. Securities and Exchange Board of India, *SEBI Investor Education Resources*, addressing deepfake videos, fake stock tips and digitally enabled investment fraud, available at: SEBI Investor Education Portal (accessed 5 August 2026).
13. U.S. Securities and Exchange Commission, North American Securities Administrators Association & Financial Industry Regulatory Authority, *Artificial Intelligence (AI) and Investment Fraud: Investor Alert*, noting that fraudsters may use AI-generated audio and video to impersonate corporate executives and manipulate stock prices, available at: Investor.gov – Artificial Intelligence and Investment Fraud (accessed 2 August 2026).

14. Ibid.; see also U.S. Securities and Exchange Commission, *Beware of Fraudsters Impersonating Investment Professionals and Firms – Investor Alert*, 11 December 2024, available at: Investor.gov – Investment Professional Impersonation Alert (accessed 2 August 2026).
15. Securities and Exchange Board of India, *SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003*, regs. 3–4, available at: SEBI – PFUTP Regulations, 2003 (accessed 2 August 2026).
16. Ibid., reg. 2(1)(c), defining "fraud" to include knowing misrepresentation, concealment of material facts, false statements and misinformation affecting the market price of securities (accessed 2 August 2026).
17. *Securities and Exchange Board of India v. Rakhi Trading Pvt. Ltd.*, (2018) 13 SCC 753, Supreme Court of India, available at: SEBI v Rakhi Trading – Supreme Court Judgment (accessed 3 August 2026).
18. Ibid. The Supreme Court held that non-genuine and synchronised transactions capable of creating artificial market activity may constitute manipulative and deceptive devices notwithstanding their execution through an apparently anonymous screen-based trading system (accessed 3 August 2026).
19. *SEBI v. Kanaiyalal Baldev Patel*, SEBI Special Case No. 1592 of 2021, Judgment dated 23 April 2024, SEBI Special Court, Mumbai; the accused was convicted under section 24(2) of the SEBI Act and sentenced to three years' simple imprisonment with a fine of ₹10 lakh, available at: SEBI – Judgment in Kanaiyalal Baldev Patel (accessed 3 August 2026).
20. The Companies Act, 2013, No. 18 of 2013, § 447, *Punishment for Fraud*, India Code, available at: India Code – Section 447, Companies Act 2013 (accessed 3 August 2026).
21. The Companies Act, 2013, § 448, relating to punishment for false statements, available through India Code, available at: India Code – Companies Act, 2013 (accessed 3 August 2026).
22. *Arup deepfake fraud case*, involving the use of AI-generated representations of corporate executives during a video conference and the transfer of approximately US$25 million from the company's Hong Kong office, reported by the *Financial Times*, available at: Financial Times – Arup Deepfake Fraud Case (accessed 4 August 2026).
23. The Information Technology Act, 2000, No. 21 of 2000, §§ 66C–66D, India Code, concerning identity theft and cheating by personation using a communication device or computer resource, available at: India Code – Information Technology Act, 2000 (accessed 4 August 2026).
24. Ministry of Electronics and Information Technology, Government of India, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, updated pursuant to the February 2026 amendments relating to synthetically generated information, available at: MeitY – IT Rules, 2021 (accessed 4 August 2026).
25. Ministry of Electronics and Information Technology, Government of India, *Frequently Asked Questions – Amendments to IT Rules, 2021 relating to Synthetically Generated Information*, explaining the statutory definition of "synthetically generated information" and "audio, visual or audio-visual information", available at: MeitY – SGI Amendment FAQs (accessed 4 August 2026).
26. Ministry of Electronics and Information Technology, Government of India, *Explanatory Note: Draft Amendments to IT Rules, 2021 relating to Synthetically Generated Information*, identifying labelling, visibility, metadata embedding and technical verification as important regulatory measures, available at: MeitY – SGI Explanatory Note (accessed 4 August 2026).
27. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, Supreme Court of India, recognising privacy as a fundamental right protected under Articles 14, 19 and 21 of the Constitution, available at: Puttaswamy Judgment – Privacy Rights (accessed 5 August 2026).
28. U.S. Securities and Exchange Commission, *Beware of Fraudsters Impersonating Investment Professionals and Firms*, supra note 2, explaining that technological advances including AI have increased the sophistication of impersonation schemes involving investment professionals and firms, available at: Investor.gov – Impersonation Schemes (accessed 5 August 2026).
29. Regulation (EU) 2024/1689, *Artificial Intelligence Act*, art. 50, concerning transparency obligations for providers and deployers of certain AI systems and AI-generated or manipulated content, available at: European Union – Artificial Intelligence Act (accessed 5 August 2026).
30. *SEBI v. Rakhi Trading Pvt. Ltd.*, (2018) 13 SCC 753, supra note 5. The Court emphasised that securities-market regulation must respond to ingenious forms of manipulation and that SEBI must develop principles capable of maintaining free and fair trading as market practices evolve (accessed 5 August 2026).