REGULATING AI IN INDIAN STOCK TRADING: ENSURING ACCOUNTABILITY, TRANSPARENCY, AND INVESTOR PROTECTION

Amrth Narayan, School of Law, SASTRA University

Laavanyaa Ramesh, School of Law, SASTRA University

ABSTRACT

The rapid integration of artificial intelligence (AI) into India's stock trading ecosystem has revolutionised the speed, efficiency, and complexity of financial transactions. AI-powered algorithmic trading systems now autonomously execute buy and sell orders using real-time market data, technical indicators, and predictive analytics, greatly reducing the necessity for constant human oversight during market fluctuations. While these advancements expand market access and encourage data-driven investments, they also introduce significant legal and regulatory challenges concerning accountability, transparency, and investor protection.

A central issue lies in regulating AI trading model providers. In India, there is currently no dedicated legal framework specifically governing these entities. SEBI's June 20, 2025, consultation proposes principles for responsible AI/ML use by market infrastructure institutions, intermediaries, and mutual funds. SEBI's February 3, 2025, Circular on retail algorithmic trading, now effective October 1, 2025, begins operational controls through empanelment, strategy approvals, and unique algo IDs. In contrast, global jurisdictions such as the European Union and the United States have begun to implement stringent measures, including mandatory audits, licensing, algorithmic transparency, and advanced cybersecurity standards for AI-driven financial services. This regulatory gap in India creates ambiguity in assigning liability for software errors, market manipulation, or cyber breaches, which is further complicated by the "black box" nature of advanced AI models.

Additionally, while automated trading reduces the need for manual intervention, it exposes investors to risks like market volatility, technical glitches, and data miscalculations, potentially resulting in considerable losses. This paper critically examines the existing regulatory framework in India, compares it with global best practices, and promotes the establishment of stringent guidelines to guarantee accountability, operational transparency,

and effective investor protection. Strengthening India's regulatory framework is essential for promoting innovation while protecting investors in an increasingly automated stock trading environment.

1. INTRODUCTION

1.1. Background

Indian financial markets have quickly evolved from manual execution to automated systems driven by technology. A key component of this shift is algorithmic trading, where computer programs execute trades based on predefined instructions. The Securities and Exchange Board of India (SEBI) permitted this practice in 2008, driving exponential growth.[1] Today, algorithmic trades dominate the market, accounting for a majority of transactions in both equity and derivative segments.

This technological advancement has now progressed further with the integration of Artificial Intelligence (AI). Unlike traditional algorithms, AI-based systems can learn from market data, identify complex patterns, and make autonomous predictive decisions. This evolution from rulebased execution to adaptive AI represents a critical defining point, introducing new levels of speed and efficiency. However, the autonomy and complexity of these AI systems also present novel and urgent challenges for India's existing legal and regulatory frameworks.

1.2 Problem Statement

The rapid integration of artificial intelligence (AI) into stock trading has transformed the speed and complexity of financial markets. In India, while algorithmic trading is well-regulated, existing laws do not adequately address the unique challenges posed by AI-driven autonomous systems. These systems operate with limited human oversight and often involve opaque decision-making processes, creating difficulties in assigning legal liability, ensuring transparency, and protecting investors. Besides, the lack of tailored regulation for AI raises concerns about market manipulation, cybersecurity risks, and data governance. This research seeks to critically analyse these regulatory gaps within India's legal framework, focusing on cyber law and securities regulation, to identify challenges in governing AI in stock exchanges.

[1] Securities and Exchange Board of India, Algorithmic Trading in India: Rules and Regulations, SEBI circulars (2008)

1.3 Research Gap

India currently lacks a dedicated, thorough legal framework specifically regulating AI in stock trading and financial markets. Existing regulations primarily address traditional market conduct and generic IT provisions. They refuse to focus on the unique challenges posed by AI autonomy, interpretation, and data governance. There is insufficient clarity on legal liability and accountability for AI-driven trading decisions under the Indian cyber laws and securities regulations. The enforcement mechanisms in India are weaker compared to its global counterparts, lacking specialised expertise and state-of-the-art governmental technologies to monitor complex algorithmic and AI activities. There is minimal scholarly exploration examining the legal, security, and systemic risks tied to AI in Indian financial contexts.

International risk-based regulatory models such as the EU AI Act contrast sharply with India's principle-based, technology-neutral approach, highlighting a regulatory void India must urgently address.

1.4 Study Significance

This study is significant because it addresses the pressing need for legal clarity and reform amidst the rapid adoption of AI in Indian financial markets. Grounding the analysis in cyber laws and securities regulations, it informs regulators, academics, and market participants about the risks and responsibilities arising from AI-driven trading. The findings can guide the development of tailored regulatory frameworks that balance innovation with investor protection and market integrity.

Another aspect to be observed is that, by comparing India's regulatory approach with international models, particularly the EU and the U.S., the study contributes to the global dialogue on AI governance and supports India's emergence as a responsible AI-finance hub.

1.5 Research Questions

1. How does the existing Indian cyber law framework apply to AI-driven trading, and where are its deficiencies?

2. How are liabilities determined and enforced in cases of opaque or automated decisionmaking by AI systems in Indian stock markets?

3. How do international regulatory models for AI in financial markets compare to India's approach?

1.6 Research Objectives

1. To critically analyse the IT Act, 2000, SEBI regulations, including Cybersecurity and Cyber Resilience Framework (CSCRF) and the Digital Personal Data Protection Act, 2023, in the context of AI trading.

2. To identify the legal risks and challenges posed by AI autonomy, lack of transparency, and accountability issues in stock trading.

3. To analyse international regulatory approaches to AI trading for insights applicable to the Indian context.

2. THE TECHNOLOGICAL AND REGULATORY LANDSCAPE

2.1 LITERATURE REVIEW

Several important studies and institutional reports have examined the impact of artificial intelligence on financial trading and market regulation. This section reviews five key scholarly contributions that deepen the understanding of AI-driven algorithmic trading, its effects on market behaviour, and the regulatory challenges in India and global markets.

1. Legal Implications of Algorithmic Trading: Safeguarding Fairness and Transparency in Financial Markets

This paper examines the legal implications of algorithmic trading, focusing on market manipulation risks, fairness and transparency challenges, and regulatory responses including MiFID II and Indian exchanges surveillance mechanisms, while analyzing case studies such as the 2010–2012 Indian flash crashes and the Knight Capital glitch to recommend enhanced transparency requirements, cross-border enforcement, and adaptive regulatory frameworks that balance innovation with market integrity. However, the paper's literature review relies heavily on generalized discussions of algorithmic strategies and manipulation techniques without critically engaging with AI-specific governance challenges, such as the black-box opacity of machine learning models, explainability requirements (XAI) for compliance audits, model risk

management frameworks, or liability attribution when autonomous AI systems (rather than rule-based algorithms) generate manipulative outcomes. Additionally, it does not synthesize Indian enforcement jurisprudence (SEBI adjudication orders, SC case law on algorithmic conduct), sectoral regulatory circulars, or comparative AI governance standards (EU AI Act risk tiers, algorithmic accountability regimes), leaving a jurisdictional and doctrinal gap.

2. ***Algorithmic Trading - Changing The Paradigm of Stock Trading in The Indian Capital Market***

The authors explore how algorithmic trading has transformed Indian capital markets by automating stock trades with sophisticated software. They analyse trading trends and SEBI's regulatory role. While acknowledging benefits like faster trade execution, they call attention to mixed evidence on impacts on liquidity and turnover. The paper advocates for further research to evaluate algorithmic trading's broader influence and to fine-tune regulatory frameworks. The study relies exclusively on secondary data sources and does not capture real-time technological advancements, limiting its ability to assess emerging AI-driven risks, autonomous decision-making patterns, and their implications for legal accountability frameworks in Indian capital markets.

3. ***The Rise of Algorithmic Trading In India: Regulatory Challenges, Institutional Response, And The Road Ahead***

This study discusses the growth of algorithmic trading in India, emphasising the role of regulations in shaping its adoption. It explains how improved technology and SEBI's guidelines have enabled market access for institutional and retail investors. Key challenges include maintaining transparency and investor protection. The authors recommend stronger regulatory measures and encourage balancing innovation with safeguards for market integrity. The existing literature focuses on broader algorithmic trading impacts on market efficiency and volatility without deeper exploration of how India's regulatory policies specifically influence AI-driven trading adoption, transparency requirements, and investor protection mechanisms, which forms the core objective of this research

4. ***Legal Challenges of Artificial Intelligence in India's Cyber Law Framework: Examining Data Privacy and Algorithmic Accountability Via a Comparative Global Perspective***

This paper examines AI's legal challenges in India's cyber law framework, focusing on algorithmic accountability and data privacy through comparative analysis of the EU AI Act and U.S. Algorithmic Accountability Act, and identify how the Information Technology Act, 2000 lacks AI-specific provisions for transparency, bias mitigation, and liability attribution, while proposing risk-based regulation, algorithmic audits, and interpretation of Section 43A to address autonomous decision-making harms. However, their literature review does not address the financial markets domain, specifically how AI-driven algorithmic trading in stock exchanges creates unique regulatory challenges around market manipulation, systemic risk amplification through highfrequency autonomous trading, and investor protection gaps when opaque machine learning models execute trades without human oversight.

5. Liability for Harm Caused by AI: Examining the Legal Responsibility for the Actions of Autonomous Systems

This paper surveys liability for harm caused by AI across tort, product, and criminal law, highlight challenges of intention, negligence, causation, and attribution in autonomous systems, discuss strict liability as a potential response, examine algorithmic bias implications, and illustrate issues through case studies such as Uber AV, COMPAS, Cambridge Analytica, and Tesla Autopilot while recommending clearer legal frameworks, standards, audits, transparency, and even liability funds to keep pace with AI adoption. The key limitation is that this literature review is general-purpose and not sector-specific: it does not engage with AI-driven algorithmic trading's market-integrity risks, explainability and auditability of trading models, SEBI's securities law enforcement and evidentiary standards, or model-risk controls in financial markets.

Overall, the global literature emphasises the importance of clear and adaptive regulation, crossborder cooperation, and ongoing monitoring of AI's impact on financial market stability, while safeguarding consumer interests.

2.2 METHODOLOGY

This research adopts a doctrinal legal methodology, focusing primarily on the analysis of the statutes, the regulatory guidelines, the judicial decisions, and the scholarly literature relevant to AI and algorithmic trading within the Indian cyber law framework. The study involves a critical examination of the existing laws, such as the Information Technology Act, 2000; the

Securities and Exchange Board of India (SEBI) regulations; and the Digital Personal Data Protection Act, 2023 (DPDPA), along with a comparative analysis of international legal instruments like the European Union's AI Act and the regulatory approaches of the United States. Secondary sources, including academic articles, policy reports, and industry publications, supplement this doctrinal research by providing insight into emerging legal challenges and regulatory trends. The objective is to identify gaps in the current legal framework and propose recommendations for effective governance of AI in India's financial markets.

2.3. Jurisprudence of Artificial Intelligence (AI) in Stock Market Regulation

Definition and Nature of AI in Law

Reaching a consensus on the legal meaning of AI is complex. The concept evolves continuously with technology. No universal legal definition exists, and jurisdictions interpret AI differently to suit their legal environments. The European Union defines AI as a machine-based system that operates with varying levels of autonomy and adaptability after deployment. It infers from inputs to generate outputs such as predictions, content, recommendations, or decisions that influence physical or virtual environments. The key characteristics are autonomy, adaptability, purposeful inference, and the capacity to affect human or institutional behaviour. Within financial markets, this translates into AI systems that make trading decisions, detect trends, and execute transactions without direct human oversight.

Legal Personality and Rights-Duty Framework

The jurisprudence of AI questions whether an autonomous system can be regarded as a legal person capable of holding rights and duties. According to Salmond, a legal person is any being to whom the law attributes rights and duties, whether human or not. Indian jurisprudence continues to reject independent legal personality for AI, treating it as a property or tool. AI cannot possess ownership, rights, or duties in its own name because it lacks consciousness and intent. In stock trading, this means that AI cannot own assets, enter contracts, or be sued independently. The responsibility for its actions rests with the human or juristic persons deploying it—developers, brokers, or trading platforms. The legal system, therefore, applies the principle of agency and vicarious liability, recognising AI as an instrument under human control rather than an autonomous rights-bearing entity.

Possession, Ownership, and Liability

In law, possession denotes control, and ownership denotes the ultimate right to enjoy or dispose of a thing. AI systems and trading algorithms are owned by the companies or individuals who develop or operate them. The AI itself has no possessory or proprietary claim over data or profits it generates. Any wrongful gain or harm caused by AI in trading is attributed to its owner or operator. This is consistent with the jurisprudential view that liability arises from control and benefit, not from consciousness. Applying this principle, SEBI's 2025 circulars hold brokers and intermediaries liable for the functioning of algorithms approved for trading. The doctrine of strict liability may be used where harm results from autonomous systems, placing responsibility on those best positioned to prevent risk. This approach aligns with Hart's positivism and utilitarian theory, where accountability serves public welfare rather than moral blame.

Challenges in Applying Jurisprudence to AI

Incorporating AI into financial regulation introduces philosophical and operational challenges. AI models act without human intent, making it difficult to assign mens rea, foreseeability, or negligence. Traditional legal principles based on human reasoning struggle to accommodate machine autonomy. Bias in data, the opacity of decision-making, and unpredictable outcomes complicate enforcement. These challenges mirror those seen in judicial applications of AI, where reliance on opaque systems risks injustice. In stock markets, similar risks arise when AI misinterprets signals or triggers manipulative trades without intent. Regulators must therefore ensure algorithmic transparency, data accountability, and human oversight to preserve fairness and investor confidence.

The Future Jurisprudence of AI in India's Financial Markets

The future of AI regulation in India's stock market depends on evolving the jurisprudence of accountability. Instead of recognising AI as a separate legal person, the law should strengthen doctrines that assign responsibility across the chain of control—from developers to traders. Legal reforms must clarify the status of AI-generated data, ownership of decisions, and liability for algorithmic errors. India's approach must remain human-centric, ensuring that technological autonomy does not dilute fiduciary duties or investor protection. As SEBI, RBI, and the legislature explore risk-based governance frameworks, jurisprudence must adapt to

integrate AI within the principles of justice, reasonableness, and proportional liability.

2.4. CORE TECHNOLOGICAL CONCEPTS IN MODERN AUTOMATED TRADING

To analyse the legal implications of AI in stock trading, it is essential to understand the core technologies that differentiate modern systems from their predecessors. The legal challenges arise not from automation itself, but from the autonomy and complexity inherent in these new forms of AI. The sections that follow explain the key concepts that underpin this technological transition.

2.4.1 Machine Learning: The Engine of Adaptive Trading

AI-driven trading is based on machine learning (ML), a subset of artificial intelligence. Unlike traditional algorithms, which are explicitly coded with a fixed set of rules, ML models are intended to learn from data. In the context of financial markets, an ML system receives massive amounts of historical and real-time data, such as price changes, trade volumes, economic reports, and news. The machine learning model identifies patterns and correlations within this data to build a predictive framework. This learning process allows the system to change its trading tactics over time without requiring direct human reprogramming, which distinguishes it from traditional algorithmic trading. A frequent use is to train a model to detect market conditions that have historically preceded a rise or fall in stock price.

2.4.2 Neural Networks: Simulating Decision-Making

A more advanced form of machine learning is achieved through neural networks, particularly deep learning models. These are complex computational systems inspired by the structure of the human brain. A neural network consists of layers of interconnected nodes, or "neurones", that process information collectively. In trading, each layer might analyse a different level of abstraction, such as raw price data, technical indicators, or broader market trends. By processing information through these multiple layers, deep learning models can uncover highly sophisticated and nonobvious patterns that would be impossible for a human analyst to detect. This capability allows them to make highly nuanced trading decisions, but it also contributes significantly to their complexity and opacity.

2.4.3 The "Black Box" Problem: A Crisis of Transparency

The sophistication of deep learning and other advanced ML models raises a key legal and

regulatory issue known as the "black box" problem. A black box model is a system whose internal workings are so sophisticated that its human architects cannot completely explain how it arrived at a particular conclusion. While the model's predictive accuracy may be high, the decision-making process is opaque.[2] For regulators and legal professionals, this opacity is extremely problematic. When the system causes a large market event, it is almost impossible to audit a trading decision, verify whether it was the product of a fault or manipulation, or assign culpability. This lack of transparency directly conflicts with legal principles of accountability and due process.

2.4.4 Explainable AI (XAI): The Pursuit of Transparency

In response to the black box dilemma, the field of Explainable AI (XAI) arose.[3] XAI refers to a range of methodologies and technologies for making AI models' decisions intelligible to humans.

An XAI system seeks to provide a clear justification for its outcomes. Instead of merely executing a "sell" order, an explainable trading model may optionally generate a report saying that its decision was influenced by a mix of negative sentiment detected in news stories and a specific bearish technical pattern. XAI is crucial in terms of legal implications. It provides the openness required for regulatory monitoring, internal audits, and fair dispute resolution, potentially addressing the accountability dilemma caused by opaque AI systems.

2.5 The Existing Regulatory Framework in India

SEBI's Role in Algorithmic Trading Regulation

The Securities and Exchange Board of India (SEBI) is the primary regulator for algorithmic trading in Indian securities markets. SEBI has published a number of circulars and guidelines, the most recent in 2025, to address the dangers connected with automated trading strategies.[4] These regulations dictate that all algorithmic methods be approved by stock exchanges before deployment, that each algorithm have a unique identification code, and that brokers be responsible for monitoring and supervising customer algorithms. Brokers must also use real-

[2] Trustpath.ai, The AI Black Box Problem in Finance
[3] Finbox.in, AI in Finance – Can We Resolve the Black Box Problem,2025
[4] Securities and Exchange Board of India, Safer Participation of Retail Investors in Algorithmic Trading, Circular No. SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/0000013 (Feb. 4, 2025),

time surveillance and emergency measures to avoid market manipulation and technical difficulties. SEBI's strategies distinguish between transparent "white box" algorithms and proprietary "black box" models, with the latter receiving further scrutiny. While these steps improve market safety and investor protection, SEBI's primary focus remains on market risk and operational integrity, rather than the underlying technology's legal or cyber implications.

Cybersecurity and Cyber Resilience Framework

The SEBI Cybersecurity and Cyber Resilience Framework (CSCRF), introduced in August 2024, establishes a unified, risk-based cybersecurity regime for all market participants. It replaces earlier circulars and aligns with CERT-In's CCMP and the IT Act, 2000, to strengthen market resilience. The framework classifies regulated entities into five tiers based on systemic importance, mandating stronger measures like 24x7 SOCs for large players and shared Market-SOCs for smaller ones. It enforces incident reporting, third-party risk management (including SBOMs), and encryption and VAPT audits, ensuring the cybersecurity of algorithmic trading systems and overall market integrity.

Information Technology Act, 2000

The Information Technology Act of 2000 is the foundation of India's cyber law framework. It legally recognises electronic records and digital signatures, making electronic commerce and record-keeping easier. The Act also handles offences such as hacking, unauthorised access, and data theft, all of which are important to trading platform security and the safeguarding of sensitive financial information. Sections 43 (penalties for computer system damage), 66 (computer-related offences), and 72 (breach of secrecy and privacy) are among the most important sections. While the Act creates a framework for pursuing cybercrimes, it does not address the specific hazards posed by autonomous AI trading systems or the intricacies of algorithmic decision-making.

Digital Personal Data Protection Act, 2023 (DPDPA)

The Digital Personal Data Protection Act, 2023, is India's most recent legislation controlling the collection, processing, and protection of personal data. Its importance to AI trading stems from the usage of vast data sets, typically containing sensitive personal information, to train and run trading algorithms. The Act requires data fiduciaries to guarantee purpose limitation,

data minimisation, and adequate security protections. It also gives individuals control over their personal data, such as the ability to view, modify, and delete information. Compliance with DPDPA is critical for AI trading platforms when dealing with client data, market information, or any dataset that may be related to identifiable individuals. However, the Act's applicability to anonymised or aggregated data used in AI model training remains a source of legal ambiguity.

2.6 The Core Legal Challenges in the Existing Regulatory Framework in India

2.6.1 The Critical Issue of Legal Liability and Accountability in Indian Cyber Law

The increasing application of artificial intelligence in financial trading has highlighted substantial shortcomings in India's legal system, notably in terms of liability and accountability. At the heart of this quandary is the lack of mens rea, or a "guilty mind", in AI systems. Indian criminal law, as codified in the Bharatiya Nyaya Sanhita (BNS) and the Information Technology Act of 2000, bases criminal culpability on the presence of intent or knowledge. AI is fundamentally incompatible with existing criminal and civil culpability laws since it lacks awareness and the ability to establish intent by design.[5]

The Knight Capital Group scandal in the United States in 2012, in which an autonomous trading algorithm generated $440 million in losses in 45 minutes owing to a software bug, exemplifies the magnitude of harm that AI systems may wreak without malicious human intent.[6] While this was not pursued as a criminal case, it emphasised the difficulty of attributing blame when harm is caused by autonomous machine judgements rather than human actions.

In India, the Information Technology Act of 2000 governs offences such as unauthorised access (Section 43), hacking (Section 66), and cheating by impersonation using computer resources (Section 66D). However, these regulations assume that a human actor or legal person can be recognised and penalised. When an AI system acts independently, the chain of accountability gets muddled. Developers, operators, and end users may all claim that the guilt rests elsewhere, particularly when the AI's behaviours are the product of complicated, adaptive learning rather than direct programming.

[5] Lakshmikumaran & Sridharan, Acts and Laws to Keep in Mind Before Implementing AI.
[6] Karen Weise & Suzanne Craig, Knight Capital and the $440 Million Algorithmic Trading Fiasco, N.Y. Times

This distribution of accountability is especially troublesome in high-risk industries such as financial trading. Indian law has yet to determine whether AI should be classified as a product or a service in terms of liability. The Consumer Protection Act of 2019 defines product liability broadly but does not specifically cover digital or autonomous systems.[7] As a result, victims of AIrelated injury may have difficulty establishing a clear cause of action, particularly if the harm is intangible, such as financial loss or data breach.

The unpredictability of AI action hampers the determination of intent or knowledge. Indian courts would encounter substantial difficulties in implementing charges such as culpable murder or negligence, which require foreseeability and a direct causal relationship. The law's emphasis on human agency and foreseeability makes it unsuitable for dealing with autonomous AI, which may behave outside of the intentions or expectations of any human stakeholder.

To address these concerns, legal academics and policymakers have offered a number of different models. One option is strict responsibility, in which the entity best positioned to control and mitigate risk, often the creator or operator, is held liable for any harm produced by AI, regardless of purpose. Another is vicarious liability, which assigns accountability to companies that use AI, comparable to employer liability for employee activities. A hybrid paradigm, in which developers, operators, and users share culpability based on their responsibilities and levels of control, may also be explored.

In essence, the present Indian legislative framework, which includes the IT Act and the Consumer Protection Act, fails to appropriately handle the particular issues brought by autonomous AI in trade. The absence of mens rea, the dispersal of accountability, and the limitations of existing liability models underscore the urgent need for legal reform. As AI systems become more prevalent in critical sectors, Indian law must evolve to ensure accountability, protect consumers, and maintain trust in digital markets.

2.6.2 AI-Driven Market Manipulation and Cybercrime

The integration of artificial intelligence into financial markets has created new and complex avenues for market manipulation and cybercrime. AI-generated deepfakes, coordinated "swarm" trading, and autonomous trading bots now have the capacity to manipulate market sentiment, amplify rumours, and distort prices at a scale and speed previously unimaginable.

[7] Consumer Protection Act, No. 35 of 2019

These systems can act without direct human input, reacting to real-time data, testing regulatory boundaries, and even learning to exploit market inefficiencies.

New Threat Vectors: From Deepfakes to Swarm Trading

AI-driven manipulation is no longer limited to traditional pump-and-dump schemes. Today, sophisticated algorithms can generate and disseminate misleading information through social media, video platforms, and news aggregators. For example, deepfake technology can be used to create convincing but false statements from company executives, triggering artificial price movements. Swarm trading, where multiple AI agents coordinate to execute trades that create the illusion of genuine market activity, can further distort prices and volumes without any explicit human conspiracy.

The Sadhna Broadcast Case: A Modern Manipulation Scheme

A recent and prominent example is the Sadhna Broadcast Limited case, investigated by SEBI in 2022-2023. In this case, a group of individuals and entities orchestrated a two-phase scheme to manipulate the price of Sadhna Broadcast shares. In the first phase, connected and promoter-linked entities engaged in collusive trading among themselves, gradually inflating the share price through small-volume transactions that had an outsized effect due to low liquidity. In the second phase, misleading and promotional videos were disseminated across YouTube channels such as Moneywise, The Advisor, and Profit Yatra. These videos presented Sadhna Broadcast as a highly promising investment, drawing in retail investors and amplifying the artificial market activity. SEBI's investigation revealed that the scheme was carefully structured, with information intermediaries and facilitators playing key roles in executing manipulative trades and spreading false narratives. The regulator ultimately banned 59 individuals and entities from the securities market for periods ranging from one to five years, imposed monetary penalties, and ordered the disgorgement of unlawful gains totalling over ₹58 crore.[8] The Sadhna Broadcast case illustrates how digital platforms and coordinated online campaigns can be weaponised to manipulate markets, often with the aid of algorithmic tools.

The Jane Street Group Case: Algorithmic Index Manipulation

The Jane Street Group case, which came to notice in 2025, further illustrates the evolving nature

[8] SEBI Final Order in the matter of Sadhna Broadcast Limited, MSEI Circular 17258 (May 30, 2025)

of market manipulation in the age of AI and high-frequency trading. SEBI's interim order accused Jane Street, a global quantitative trading firm, of orchestrating a complex strategy to manipulate the Bank Nifty index during expiry-day trading.[9] According to SEBI, Jane Street engaged in "intraday index manipulation" by aggressively buying large quantities of Bank Nifty constituent stocks in the cash market, temporarily pushing up the index, and then unwinding these positions while holding significant short bets in index options. This strategy allegedly allowed Jane Street to profit from the artificial movement in the index, at the expense of other market participants. SEBI found that Jane Street's trading activity accounted for a substantial share of market volume during the relevant periods, suggesting that the firm was not merely participating in the market but actively directing it. The regulator directed Jane Street to deposit ₹4,843 crore, representing alleged unlawful gains, into an escrow account and temporarily barred the firm from trading in Indian markets. Jane Street complied with the order but has contested the findings, arguing that its actions constituted legitimate index arbitrage rather than manipulation. The case remains under adjudication, with broader implications for how Indian law distinguishes between aggressive trading strategies and unlawful market manipulation.

Legal Challenges: The Limits of Current Law

Despite SEBI's decisive actions, both the Sadhna Broadcast and Jane Street cases highlight the limitations of existing legal frameworks. The SEBI Act, 1992, and the SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003, are grounded in the assumption of human intent and direct manipulation. They prohibit the use of manipulative or deceptive devices and the dissemination of false or misleading information likely to influence investors.

However, AI-driven manipulation often blurs the line between lawful data-driven trading and unlawful distortion.[10] For instance, an AI agent may autonomously detect a surge in retail interest and execute trades ahead of others, or another AI may circulate selective but accurate headlines to stimulate market activity. In such cases, there may be no direct falsehood or conspiracy, yet the result is a distorted market and profit for the operator.

[9] SEBI, Interim Order in the Matter of Index Manipulation by Jane Street Group, WTM/AB/EFD-1/DRA-3/202595040

[10] S. Paliwal & M. Shinghal, SEBI's Order on Spoofing – A Way Forward, IndiaCorpLaw

The opacity of "black box" AI models further complicates enforcement. These systems often lack transparency, making it difficult for regulators to trace decision pathways or establish a clear audit trail. Unlike traditional schemes, where emails or chat logs might reveal intent, AI-driven manipulation can occur silently, with multiple autonomous agents acting in concert without explicit coordination. This silent conspiracy of AI models is largely undetectable under current surveillance tools.

Existing Indian laws, including the Information Technology Act, 2000, and the SEBI Act, are not fully equipped to address these challenges. Both statutes rely on the concept of human intent and knowledge, which is often absent in AI-driven schemes. The legal definitions of fraud and manipulation require proof of intent, knowledge, or wilful conduct, which are difficult to establish when actions are taken by autonomous systems. As a result, sophisticated coordinated digital abuses can evade prosecution, and enforcement remains reactive and fragmented.

2.7 A Comparative Perspective

2.7.1 The European Union's AI Act

The European Union's Artificial Intelligence Act (EU AI Act), adopted in June 2024, represents a landmark in global AI regulation. The Act introduces a risk-based approach, classifying AI systems into different tiers: minimal risk, limited risk, high risk, and prohibited practices, based on their potential impact on individuals and society. This framework is designed to ensure that regulatory requirements are proportionate to the risks posed by specific AI applications, rather than applying a one-size-fits-all model.

Risk Tiers Under the EU AI Act:

Minimal Risk: Most AI systems fall into this category and are largely unregulated, except for basic transparency requirements.

Limited Risk: These systems must meet certain transparency obligations, such as informing users they are interacting with AI.

High Risk: AI systems used in critical sectors (including finance, healthcare, and law enforcement) are subject to stringent requirements. These include mandatory risk management,

data governance, technical documentation, transparency, and human oversight. Providers of highrisk AI must ensure their systems are robust, auditable, and explainable.

Prohibited Practices: Certain AI uses, such as social scoring or manipulative biometric identification, are banned outright due to their unacceptable risk to fundamental rights.

Application of the EU AI Act in Financial Markets

The EU AI Act, effective from August 2024 and fully enforceable by August 2026, establishes a harmonised regulatory framework for AI systems across all sectors, including financial services. The Act classifies AI systems by risk level, with "high-risk" systems subject to the most stringent requirements. In the financial sector, high-risk AI includes systems used for creditworthiness assessments, algorithmic trading, market surveillance, and risk management.[11]

Key obligations for high-risk AI systems in finance include:

Risk Management and Governance: Financial institutions must implement comprehensive risk management frameworks for AI systems, including ongoing monitoring, documentation, and mitigation of risks to market integrity, consumer protection, and financial stability.

Transparency and Explainability: Providers must ensure that high-risk AI systems are transparent and explainable. This includes maintaining technical documentation, enabling audit trails, and providing regulators with access to decision-making processes.

Data Governance: The Act mandates strict standards for data quality, security, and privacy. AI models must be trained on accurate, representative, and unbiased data, with robust safeguards against data breaches and misuse.

Human Oversight: High-risk AI systems must be subject to meaningful human oversight. Financial institutions are required to ensure that human experts can monitor, interpret, and intervene in AI-driven processes, especially in trading and risk management.

Market Surveillance and Enforcement: National financial supervisory authorities, such as the European Securities and Markets Authority (ESMA), are empowered to enforce the AI

[11] European Commission, AI Act, Shaping Europe's Digital Future

Act's provisions. These authorities can conduct ex-post market surveillance, require corrective actions, and withdraw non-compliant AI systems from the market.

Coordination with Sectoral Regulation: The AI Act operates alongside existing EU financial services laws, such as MiFID II and the Digital Operational Resilience Act. Financial institutions must comply with both sector-specific and AI-specific requirements, ensuring a layered approach to governance and supervision.

The EU AI Act's risk-based approach is designed to address the unique challenges posed by AI in financial markets, including opacity, autonomy, and the potential for market manipulation. By imposing tailored obligations on high-risk systems, the Act seeks to safeguard market integrity, consumer rights, and systemic stability.

In contrast, India's regulatory framework for AI and algorithmic trading remains fragmented and technology-neutral. The Securities and Exchange Board of India (SEBI) regulates algorithmic trading primarily through circulars and guidelines focused on market conduct, risk management, and operational integrity. These rules require brokers to obtain approval for trading algorithms, implement surveillance mechanisms, and maintain emergency controls. However, they do not impose specific requirements for transparency, explainability, or data governance in AI systems.

2.7.2 The United States' Sector-Specific Approach

In the United States, the regulation of artificial intelligence in financial markets is handled by existing sectoral regulators, such as the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), and Financial Industry Regulatory Authority (FINRA). Each agency develops its own rules and guidance for the use of AI within its jurisdiction, focusing on issues like market integrity, investor protection, and risk management.

There is no single, comprehensive federal law governing AI across all sectors. Instead, oversight is fragmented, with each regulator addressing AI risks as they arise within their specific domain.

AI is now widely used on Wall Street for high-frequency trading, risk analysis, and automated decision-making. These systems can process vast amounts of data, react to market events in

real time, and execute trades at speeds far beyond human capability. While this has increased efficiency and accuracy, it has also introduced new risks. The speed and autonomy of AI-driven trading can amplify market volatility, potentially triggering rapid, large-scale sell-offs that human traders would be unable to stop. Experts warn that a future market crash could be triggered not by human error, but by the recursive, self-reinforcing actions of AI systems acting in concert.

U.S. regulators have responded by emphasising the need for robust risk management, transparency, and human oversight. The SEC, for example, has prioritised AI in its regulatory agenda, focusing on the reliability of automated models and the accuracy of disclosures. However, there are no uniform standards for explainability, data governance, or liability for AI-driven errors. Most AI platforms place responsibility for any harm on the user, and professional liability coverage for AI-related losses remains uncertain.

In contrast, the European Union's AI Act adopts a horizontal approach, applying a single set of rules to all sectors, including finance. The EU classifies AI systems by risk and imposes strict requirements for high-risk applications, such as algorithmic trading and credit scoring. These include mandatory risk management, transparency, data quality, and human oversight, enforced by national and EU-level supervisory authorities.

3. Suggestions and Future Directions

To effectively regulate AI in Indian stock trading, there must be a dedicated legal framework that explicitly addresses the unique challenges posed by AI-driven trading systems. This framework should emphasise algorithmic transparency, requiring AI models to be explainable and their decision-making processes clear to regulators and market participants. Such transparency will mitigate the issues related to the "black box" nature of advanced AI, allowing for better auditability and accountability. Legal liability also needs reconsideration in light of AI autonomy.

A strict liability or hybrid accountability model should be adopted, assigning responsibility to developers, operators, and platform providers. This approach will close gaps in current laws that struggle to attribute fault when autonomous AI systems cause financial harm without clear human intent. Establishing mandatory registration and unique identifiers for trading algorithms can enhance traceability and oversight.

India should align its regulatory standards with international frameworks like the EU AI Act and encourage regulatory sandboxes that support AI innovation under controlled conditions. Finally, the regulatory ecosystem must remain adaptive, periodically updating to keep pace with rapid technological developments and emerging AI-driven market risks, ensuring sustained investor confidence and market integrity.

4. Conclusion

SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF) marks a vital advancement in securing India's capital markets by reinforcing robust cybersecurity controls, continuous threat monitoring, and structured incident response. However, the framework's emphasis remains largely technical and operational, leaving critical legal challenges of autonomous AI-driven trading unaddressed. Unlike the EU's AI Act, SEBI's CSCRF does not enforce explicit mandates on AI explainability, algorithmic transparency, or governance of AI model training, which perpetuates the "black box" problem, where AI decision-making remains opaque to regulators and market participants.

Moreover, the framework assigns broad cybersecurity responsibility but lacks a detailed legal structure to attribute liability when autonomous AI causes financial harm without identifiable human error. This gap stems from the challenge of applying traditional mens rea principles to nonsentient AI systems, creating significant uncertainty in investor protection and accountability postAI-induced market events.

Though CSCRF incorporates a tiered approach and Market-SOCs to assist smaller entities, resource constraints and the fast-paced evolution of AI threats pose ongoing implementation challenges. Ultimately, while SEBI has fortified India's market defenses against known cyber risks, a comprehensive legal and governance architecture specifically tailored to AI's distinct risks is still pending. Future regulatory efforts must evolve beyond infrastructure security to proactively govern the intelligent systems that drive today's automated trading landscape, ensuring transparency, accountability, and investor confidence in the AI era.

References

1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
2. https://www.sebi.gov.in/legal/circulars/sep-2008/circular-on-algorithm-trading-in-indiarules-and-regulations_31684.html
3. https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resiliencеframework-for-sebi-regulated-entities_67536.html
4. https://www.sebi.gov.in/legal/circulars/feb-2025/safer-participation-of-retail-investors-inalgorithmic-trading_69125.html
5. https://www.indiacode.nic.in/showdata?actid=AC_CEN_5_30_00015_199201_1517807324187
6. https://www.sebi.gov.in/orders/jul-2025/sadhna-broadcast-limited-finalorder_67898.html
7. https://www.sebi.gov.in/orders/oct-2025/jane-street-interim-order_68421.html
8. https://www.sebi.gov.in/orders/mar-2023/sadhna-broadcast-youtube-recommendationsinterim-order_45831.html
9. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
10. https://finbox.in/ai-in-finance-black-box-problem
11. https://indiacorplaw.in/2025/10/sebi-ai-ml-governance-framework.html
12. https://lakshmisri.com/insights/acts-and-laws-to-keep-in-mind-before-implementing-ai/
13. https://trustpath.ai/ai-black-box-problem-finance