REGULATING THE ALGORITHM: ATTRIBUTION OF LIABILITY FOR AI-DRIVEN MARKET MANIPULATION UNDER INDIAN SECURITIES LAW: A DOCTRINAL AND REGULATORY ANALYSIS

Rishab Saraogi, B.Com. LL.B.(H), Amity University, Kolkata

Sulagna Mohanti, B.B.A. LL.B.(H), Amity University, Kolkata

ABSTRACT

"The opacity of an algorithm cannot become the opacity of the law."

Increasing deployment of AI, machine learning, and automated execution algorithms in securities markets poses a challenge to traditional paradigms of regulatory accountability. An algorithm can create, adjust and trade orders at such speed and scale that makes manual intervention by humans simply unfeasible. Nevertheless, the legal ramifications of manipulative trading should not be lost amid the technical intricacies of the system. This paper discusses how liability for AI-enabled algorithmic trading and market manipulation could be ascribed within the framework of Indian securities law. It is claimed that the current regime, consisting of the SEBI Act of 1992, PFUTP regulations of 2003, and the framework for algorithmic trading, would be sufficient to cover the acts committed by means of autonomous systems, without recognizing AI as a legal entity. Instead, the liability for those activities should be distributed among the trader or the beneficial owner, the broker, the developer and the operator of an algorithm, as well as the responsible officials according to their level of involvement and accountability. Possible evidentiary and theoretical challenges, including proving inducement, manipulative intent, attribution, and causation, are discussed. A risk-based approach based on traceability, predeployment testing, real-time controls, and enforcement is proposed.

Keywords: Artificial intelligence; algorithmic trading; market manipulation; SEBI; PFUTP Regulations; attribution; broker liability; securities regulation.

1. INTRODUCTION

Previously, algorithmic trading used to be linked exclusively with large financial institutions and high-frequency trading departments of financial institutions. This is no longer true. Retail traders can employ automated strategies by means of APIs of their brokers, trading platforms or services of third-party software vendors. Artificial intelligence (AI) technology carries this trend forward one more step. An algorithm traditionally follows instructions provided to it by its creator; while a machine learning program changes its behavior depending on the data it receives and may create its own instructions that cannot always be traced and comprehended by its creator. Such technology may enhance efficiency of trading process but also lead to its abuse. For example, artificial intelligence can be used for placing and cancelling orders repeatedly, simulating interest in a stock in order to artificially drive up its price, coordination of trading in several accounts or use of information unavailable to other participants of market.

However, the main issue is not whether an algorithm is capable of becoming a morally blameworthy party. What is important for legal purposes is the ability of the persons and organizations using such technology to become responsible for actions of an algorithm under the relevant provisions of the law. The issues here will be about identifying those who have selected the software in question or controlled it, benefitted from trading conducted using this technology, supervised it or had an actual ability to stop or prevent certain actions from happening. Treating algorithm as the wrongdoer independently would leave open a clear deficiency in the area of accountability as software cannot act as regulated party, bear punishment on itself or respond to directions from SEBI. But at the same time, all persons affiliated with the software cannot be made automatically responsible regardless of their participation.

This paper argues that a responsible approach will consist in assigning liability to a person for his actions that satisfy the legal criteria and separate liability for failure to perform certain functions of broker, software vendor or other regulated entity. The responsibility of each party will be assigned according to the degree of control of the system, awareness of its functioning, ability to avoid negative consequences and benefits from using the technology.

2. THE INDIAN REGULATORY FRAMEWORK

2.1 Statutory foundation and the PFUTP Regulations

The initial reference can be made to the SEBI Act, 1992. Section 11 makes it mandatory for

SEBI to protect investors and regulate and promote the securities market. Further, according to Section 11B, the Board, after conducting an inquiry as per the rules prescribed, can give suitable orders for the protection of investors and promotion of the development of the market. Section 12A makes it illegal to employ any manipulative or deceptive devices, scheme or artifices with regard to securities and any act that constitutes deceit or fraud. Finally, section 15HA prescribes monetary penalties in cases of fraud and unfair trade practices. Notably, these regulations are not conditional upon the use of a particular technology to trade, but rather address the conduct of a transaction and its relation to the securities market.[1]

The SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003 (PFUTP Regulations) provide for details about these prohibitions. Regulation 3 prohibits fraudulent trading, deceptive practices, and devices to defraud. On the other hand, regulation 4 states a number of manipulative, deceptive or fraudulent acts and practices, including those creating fictitious or misleading impression of trading, placing orders without intention to affect them, making orders without intention to transfer the beneficial ownership and price manipulation, among others. Importantly, the definition of 'fraud' in 2(1)(c) of the PFUTP is broadly defined and embraces acts, expressions, omissions, and concealment when the legal criteria are met. While such width provides for easy applicability in the rapidly changing market conditions, it should be noted that it cannot relieve SEBI from establishing the conduct and its relation to the person being proceeded against.[2]

In general, the Supreme Court has tended to prefer an interpretation of law that serves the purpose of keeping the securities market intact. In N Narayanan v Adjudicating Officer, SEBI, it stressed that the corporations are responsible for their actions and obligations are imposed upon its officers to comply with them. Moreover, in SEBI v Kanaiyalal Baldevbhai Patel, it pointed out the wide applicability of the PFUTP fraud definition and decided that front-running by an individual who is not an intermediary can be considered as violation of regulations. It is relevant for AI driven trading as such an individual is not necessarily the one that actually places orders or is officially licensed to trade.[3][4]

Further, in Rakhi Trading Pvt Ltd v SEBI, the Supreme Court took a look at how a coordinated

[1] Securities and Exchange Board of India Act 1992, ss 11, 11B, 12A and 15HA.
[2] Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations 2003, regs 2(1)(c), 3 and 4 (as amended 28 June 2024).
[3] N Narayanan v Adjudicating Officer, Securities and Exchange Board of India (2013) 12 SCC 152.
[4] SEBI v Kanaiyalal Baldevbhai Patel (2017) 15 SCC 1.

and artificial derivative trade can constitute an unfair trade practice. It is imperative to recognise that a trade will not be determined based on the technical execution. The commerciality of the trade and context of the trade must also be taken into consideration. This should also be applied when considering an AI system generating an order pattern.[5]

2.2 Algorithmic-trading controls

From 2012, SEBI started to regulate algorithmic trading through circulars, which have been expanded upon by further directions. These have placed obligations on Stock exchanges and Brokers including order controls, monitoring, capacity and ensuring trades are carried out properly. In February 2025, SEBI issued a further circular to encourage safer retail participation in algorithmic trading. This has put in place requirements to ensure relevant algorithms are approved by the exchange, whilst recognizing the increasing use of APIs and third party algos. It has also recognized the difference between white box strategies (those that are visible and replicable) and black box strategies (those that are less visible). However, SEBI later extended the timeframe to implement this framework, with the new framework now being in place from 1st October 2025.[6][7][8]

This is significant to note as the risk is not solely the responsibility of the investor. The client may receive a strategy from a vendor which they link up to their broker through an API. The broker may then execute the orders for them. The framework puts in place obligations on Brokers and Algo providers. The National Stock Exchange have provided materials in relation to the implementation of the framework and requirements that providers are empaneled by the exchange.[9]

The SEBI (Stock Brokers) Regulations 2026 now form part of the regulatory regime for Stock Brokers. These have included a definition of market abuse, including manipulative, fraudulent and unfair trade practices as set out in the PFUTP Regulations, insider trading framework and

[5] SEBI v Rakhi Trading Pvt Ltd, Civil Appeal No 1969 of 2011 (Supreme Court of India, 8 February 2018).
[6] SEBI, 'Broad Guidelines on Algorithmic Trading' (Circular CIR, MRD, DP,09,2012, 30 March 2012); SEBI, 'Broad Guidelines on Algorithmic Trading' (Circular CIR, MRD, DP,16,2013, 21 May 2013).
[7] SEBI, 'Safer Participation of Retail Investors in Algorithmic Trading' (Circular SEBI, HO, MIRSD, MIRSDPoD, P, CIR,2025,0000013, 4 February 2025).
[8] SEBI, 'Extension of Timeline for Implementation of SEBI Circular dated February 04, 2025 on "Safer Participation of Retail Investors in Algorithmic Trading"' (Circular SEBI, HO, MIRSD, MIRSDPoD, P, CIR,2025,132, 30 September 2025).
[9] National Stock Exchange of India Ltd, 'Implementation Standards for Safer Participation of Retail Investors in Algorithmic Trading' (Circular NSE, INVG,67858, 5 May 2025); NSE, 'Empanelled Algo Providers of the Exchange' (updated 16 October 2026).

section 12A of the SEBI Act.[10] Whilst this has created a stronger framework to supervise those involved in the algorithmic trading, there are still questions to be asked around an AI system that adapts. Just because they are approved, registered doesn't mean they are immune from the PFUTP Regulations. Similarly, just because there was an unexpected outcome there is no assumption that the trade was manipulated.

2.3 The distinction between automation and manipulation

Overall, algorithmic trading is a method of creating and executing orders. It is not illegal to use an algorithm to split large orders into smaller orders, take into account available liquidity or change the timing of execution. This wouldn't be manipulative just because it is automated or uses machine learning. This would depend on if there was any false impression given to the market, if it was misleading, if it was deceptive to others or if it falls under the statutory definitions.

When considering AI, there may be some unusual order patterns due to poor data quality, model drift, feedback loops or an unexpected interaction with another trading system. This could indicate poor supervision or poor risk controls. However, this does not necessarily mean that the client or vendor have committed fraud. SEBI should consider whether the claim is that they have manipulated the market or that the party didn't have the correct systems in place.

3. ATTRIBUTING LIABILITY ACROSS THE AI TRADING CHAIN

3.1 The trader, client and beneficial owner

Typically, the first party to be looked at would be the client, beneficial owner. They may be directly responsible for choosing a manipulative strategy, setting the parameters, giving instructions or knowingly allowing the strategy to be used. The orders being created using software will still create a link back to the client. When looking at multiple accounts, SEBI may look at the funding, control over the accounts, API identifiers, timing, communication and profit sharing to see if there was any coordination.

However, this shouldn't create a strict liability. A retail investor may not understand the source code of the vendor and will rightly trust that the strategy is compliant with the exchange. They

[10] Securities and Exchange Board of India (Stock Brokers) Regulations 2026, reg 2(1) (including the definitions of 'market abuse' and 'fraud').

should only be held responsible if there is evidence to show they adopted, instructed, had knowledge, were reckless or ignored clear warnings. If a client intentionally uses a black box strategy to manipulate prices, they should be held responsible, even though they cannot explain the code. However, if the order was unexpected and the client had no knowledge of it then they should not be considered market manipulators.

3.2 The stock broker and trading member

Brokers play an important role as they are an important gateway into the market. Brokers provide access to trade, operate or link order routing systems, on-board clients and have regulatory obligations relating to managing risk and monitoring. If they allow an unauthorised algorithm, ignore repeated order to trade issues, fail to have the correct controls in place on the API or continue to route orders despite valid warnings they may be subject to regulatory action. Even if they didn't design the algorithm.

Brokers do not simply pass on the orders from their client. The 2025 retail framework expects brokers to be part of the control process for client facing algorithmic trading. This means they should be able to identify the client and strategy, authenticate the API, enforce appropriate order limits, keep records and monitor unusual activity. If required by the rules they should be able to pause or escalate any suspicious trading. Whilst they should not be held substantially liable for everything an independent client, vendor does, they should be held responsible for their own actions.

3.3 The algorithm provider and technology vendor

An algorithm provider may design or train a model, promote the strategy, provide updates and maintain the software. However, they cannot be excluded from the securities laws. If the vendor designed the strategy with the intention to create misleading signals in the market, set it up to take advantage of confidential order flow, hide any known issues or knowingly assist their client with a manipulative strategy then they could be liable. Kanaiyalal notes that simply because they aren't a registered intermediary they aren't excluded from the PFUTP Regulations.[11]

If the model unintentionally creates manipulative trades, then it shouldn't be assumed they are immune. However, they shouldn't be assumed to be manipulators just because their software

[11] SEBI v Kanaiyalal Baldevbhai Patel (2017) 15 SCC 1

was used. If they breached a specific regulation, made misleading claims, hid a material risk or didn't follow the correct approval and change controls then they could be liable. If none of these are evident then the fact that their software was misused by the client shouldn't be enough to hold them liable.

3.4 Directors, compliance officers and other responsible persons

Should the company be held liable or their directors, compliance officers, employees? N Narayanan makes it clear that they cannot always avoid liability by saying it isn't their role to comply. However, just because they have a certain title doesn't mean they are liable.[12] A director shouldn't be penalised just because there was a fault with the AI system. Consider who their role was, what they knew, if they had any warnings, if they had authority to intervene.

Within an AI trading environment, you should identify who approved the model, who set risk limits, who monitored the performance, who had authority to stop it running and who received alerts. If a compliance officer quickly reported any concerns but didn't have the power to change the system then they shouldn't be treated the same as an executive who knowingly bypassed a safeguard. The law should distinguish between genuine lack of oversight and knowingly assisting with market manipulation.

3.5 Exchanges and the regulator

Exchanges are an important gateway into the market. They have obligations to ensure the systems are robust, orders are being monitored and the relevant algorithmic trading framework is in place. They should not be seen as responsible for creating a manipulative strategy for the client but if they didn't have the correct monitoring in place or didn't react to valid indicators then questions may be raised. SEBI must ensure they have a tech savvy, consistent and fair approach to enforcement.

4. PROVING MANIPULATION IN AI-DRIVEN MARKETS

4.1 Intent, effect and circumstantial evidence

AI can make it harder to prove what has happened as the model may not be transparent, adaptive or probabilistic. SEBI may see thousands of orders and cancellations but may not see any

[12] N Narayanan (n 3)

human instructions. This shouldn't cause issues with enforcement. Focus on the elements of the alleged breach and evidence linking the conduct to the person, entity.

Indian securities laws do not require every allegation to be proven as there may be circumstantial evidence which can be considered in the correct civil, administrative proceedings on the balance of probabilities. In SEBI v Kishore R Ajmera, the Supreme Court acknowledged that it may be inferred that there was collusion and the market was manipulated due to the cumulative effect of the circumstances.[13] Kanaiyalal makes it clear that mens rea is not essential to prove every breach under the PFUTP framework.[14] Whilst this doesn't mean that just because there was suspicious trading they were fraudulent, SEBI must identify the relevant provision, establish the ingredients and explain how the evidence supports the finding against the noticee.

Useful evidence may include records of the source code, version of model, training, validation documentation, configuration settings, API credentials, order, cancel logs, timestamps, device, IP details, client, vendor communication, approvals to changes, risk alerts, overrides and records of profit sharing. If there were frequent orders and quick cancellations at certain price points this could support the inference that there was spoofing, layering taking place. However, this may simply be due to legitimate market making or normal execution strategy.

4.2 Model opacity and the duty to preserve evidence

A party shouldn't be able to use the lack of transparency of their model as an excuse if they had obligations to keep records and have explainable controls. This doesn't mean every black box model should be assumed to be manipulative. The records should be proportionate to the risk of the system. Firms should keep records of model versions, material changes, inputs, outputs and any human overrides. This will enable them to recreate what happened to cause the suspicious order.

Model drift may cause issues. A strategy may have been approved as acceptable but as market conditions change, new data comes into the system or other algorithms react to the strategy the results may change. Firms should review their models regularly. If a vendor didn't disclose a significant update or a broker didn't get approval for a material change it may provide a clearer

[13] SEBI v Kishore R Ajmera (2016) 6 SCC 368.
[14] SEBI v Kanaiyalal Baldevbhai Patel (n 4).

reason for regulatory action rather than trying to work out what calculations were taking place internally.

Just because there was a negative impact on investors doesn't necessarily mean there was market manipulation. This could be due to genuine news, lack of liquidity, normal order flow or independent trading systems interacting. SEBI must ensure that they can differentiate between suspicious patterns and actual breaches. Whilst there may be issues with the order book imbalance, price impact and reaction from other traders, this should be considered alongside the commerciality of the strategy and what the person doing the trading was doing.

Rakhi Trading reminds us that just because an order was formally executed doesn't mean it was genuine.[15] This should be considered when looking at orders created by an AI. The regulator should consider if there was a genuine reason to execute the order or if they were placed to create misleading signals. They should also explain how the pattern supports the allegation and why it can be attributed to the client, broker, vendor, officer.

5. GAPS IN THE PRESENT FRAMEWORK

Whilst the current securities framework is broad enough to apply to new technologies, there are still questions to be answered. Whilst the PFUTP Regulations can cover manipulative behaviour using an adaptive system, it is not detailed how liability should be divided between the parties. The model may be designed by one party, implemented by another, provided by a broker and profited by the client.

Secondly, there may be confusion over who is providing the strategy. The vendor may have a lot of influence over how the orders are executed but won't have a contractual relationship with the exchange. The broker may have control over market access but have little insight into how the model works internally. If the regulatory obligations don't take these factors into account, then important risks may not be considered or liability may be applied to those who didn't have much control.

Thirdly, the controls may not be as effective against fast adapting models or those who interact strategically with other systems. Fixed order limits and a one-off approval won't provide controls over model drift, coordination or emergent strategies. Fourthly, there may be an

[15] SEBI v Rakhi Trading Pvt Ltd (n 5).

information gap. The party may have the source code and logs but the regulator will have to try and work out what happened from the exchange data and disclosures. Finally, the law must be applied fairly. Fraud shouldn't be interpreted too broadly.

6. TOWARDS A RISK-BASED ATTRIBUTION FRAMEWORK

A practical approach should be taken to ensure they are held liable for their actions but there should be clear obligations for compliance.

Firstly, SEBI should publish guidance on how liability will be divided between the client, broker, algo provider and exchange. This should make it clear whether they are directly manipulating, knowingly assisting, negligently failing to meet specific regulatory obligations or simply providing technology. Don't assume everyone involved in an algorithmic trade will be jointly liable.

Secondly, consider 5 factors to determine liability: (i) Who had control over the relevant trading logic, access? (ii) What did they know? Were there clear warnings? (iii) Could they reasonably have prevented, stopped the conduct? (iv) Were they involved in or benefiting from the activity? (v) What were their legal, regulatory obligations? This should aid with determining liability but shouldn't override the elements of the provision. If they were directly involved or knowingly assisting then they may be liable under the PFUTP. If there was a failure in controls then this should be treated as a separate breach if there was a specific obligation.

Thirdly, there should be controls in place throughout the lifetime of a high-risk AI. Before going live, firms should document what the strategy is for, test for spoofing, layering and wash trading scenarios, ensure data quality is good and set clear risk limits. Once live they should monitor cancellation patterns, order to trade ratios, unusual coordination between accounts, price impact and unexpected behaviour. Any significant model updates should be reviewed and if required by the rules submitted for new exchange approval. There should also be a clearly defined person with authority to trigger an emergency shutdown.

Fourthly, there should be controls in place to enable them to work out what the system did and why. Firms should keep records of model versions, parameter changes, relevant inputs, outputs, API credentials, order events, alerts, overrides, approvals for the required period of time. The source code and commercially sensitive information doesn't need to be published. SEBI could

utilise secure inspections, independent technical audits or other methods to ensure they can effectively supervise them whilst keeping their legitimate confidentiality interests.

Fifthly, the enforcement should reflect the role and actions of the party. If they have been proven to manipulate then the seriousness, length, scale, benefit, previous actions and level of cooperation may be considered. If the evidence indicates there was a failure in controls but they weren't involved in manipulation then this should be clearly stated. A vendor shouldn't be treated the same if they intentionally created a spoofing strategy compared to if their software was misused by the client without their knowledge. Similarly, a broker shouldn't be able to avoid being investigated if they ignored repeated warnings even though they didn't write the code.

SEBI should continue to develop their technical knowledge and work closely with the stock exchanges. Having a standard format for reporting incidents and securely sharing relevant model information will make investigations more effective. Using regulatory sandboxes and consulting market participants can help create effective standards. The aim shouldn't be to deter legitimate automated trading but to ensure that just because things are fast, complex and commercially confidential it doesn't mean market abuse can't be detected and attributed.

7. CONCLUSION

The modern nature of market abuse using AI based algorithmic trading highlights the issue that the individual carrying out the manipulative act might not actually be the one placing the order. However, Indian securities law has provisions to combat this situation. Section 12A and section 15HA of the SEBI Act, and regulation 3 and regulation 4 of the PFUTP Regulations can be used to address situations of manipulative transactions carried out using automated trading systems. The decisions of the Supreme Court in N Narayanan, Kanaiyalal, Kishore R Ajmera and Rakhi Trading support taking a substantive approach to these situations.

The issue here is determining who should be held accountable. Whilst AI should not be used as a legal loophole, everyone involved with the AI should not automatically be held liable. Instead, liability should be determined by looking at the evidence that they were involved in. This means considering if they were involved in the transaction, had control, knew about it, benefited from it and what specific obligations they have. For example, whether they were a client, had a gatekeeper role as a broker, had influence over the model as a vendor, or had

supervisory powers as an officer.

Having a risk-based approach to testing models, monitoring, change management, having good audit trails and proportionate enforcement will help ensure that the law can keep up with adaptive trading. Ultimately, whilst AI might change how market manipulation is done, the law should still be able to determine who is responsible for the actions.

REFERENCES

Legislation and Regulations

Securities and Exchange Board of India Act 1992.

Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations 2003.

Securities and Exchange Board of India (Stock Brokers) Regulations 2026.

Cases

N Narayanan v Adjudicating Officer, Securities and Exchange Board of India (2013) 12 SCC 152.

SEBI v Kishore R Ajmera (2016) 6 SCC 368.

SEBI v Kanaiyalal Baldevbhai Patel (2017) 15 SCC 1.

SEBI v Rakhi Trading Pvt Ltd, Civil Appeal No 1969 of 2011 (Supreme Court of India, 8 February 2018).

Regulatory Materials

SEBI, 'Broad Guidelines on Algorithmic Trading' (Circular CIR, MRD, DP,09,2012, 30 March 2012).

SEBI, 'Safer Participation of Retail Investors in Algorithmic Trading' (Circular SEBI, HO, MIRSD, MIRSD-PoD, P, CIR,2025,0000013, 4 February 2025).

SEBI, 'Extension of Timeline for Implementation of SEBI Circular dated February 04, 2025' (Circular SEBI, HO, MIRSD, MIRSD-PoD, P, CIR,2025,132, 30 September 2025).

National Stock Exchange of India Ltd, 'Implementation Standards for Safer Participation of Retail Investors in Algorithmic Trading' (Circular NSE, INVG,67858, 5 May 2025).