THE ALGORITHMIC ADVANTAGE: AI-DRIVEN INSIDER TRADING AND REGULATORY GAPS IN INDIAN REGULATION

Anoushka Sinha, B.A.LL.B., KPMSOL, NMIMS Mumbai

ABSTRACT

With the help of artificial intelligence (AI) and machine learning (ML), the way financial markets operate is being changed significantly, especially in the areas of information handling and decision-making. This paper studies how the use of autonomous trading algorithms has led to such forecasts that they can be mistaken for the effects of Unpublished Price Sensitive Information (UPSI), thus raising a big regulatory question. Insider trading laws like the SEBI (Prohibition of Insider Trading) Regulations, 2015 in India are still based on human-centric ideas of the mind (intent) and things (possession), which are not enough to address the problem of AI-driven trading raised by these complexities. By comparing the Indian law with international best practices, the research uncovers the inadequacies of the Structured Digital Database (SDD) as a compliance tool and the problem of "Black Box" in understanding algorithmic decision-making.

Initially, the study aims at locating elements to underlie the trade of moving away from the proof of intent to focusing on the consequences of trade operations. It draws on the examples of the European Union's MiFID II and the U.S. regulatory approach under FINRA to motivate such a shift. It envisions changes such as the imposition of the examination of trading algorithms as a compulsory function, the growth of the degree of XAI (Explainable AI) transparency, and the engagement of developers in a dialogue so as to make them responsible. The target is to raise a legal framework adaptable to the new era that would ensure that the market remains fair and that investor confidence is retained in the AI-driven finance world.

The intent is to create a modern legal framework that would support market fairness and investor confidence in the AI-empowered financial era.

I. INTRODUCTION: FRAMING THE FROTIER OF MARKET ABUSE

I.A. Statement of problem and thesis

The integrity of global capital markets relies fundamentally on the principle of information parity, ensuring fair price discovery and maintaining investor confidence.[1] In India, this principle is primarily codified through the Securities and Exchange Board of India (SEBI) act 1992, and the SEBI (Prohibition of Insider Trading) Regulations, 2015 (PIT Regulations). However, the rapid increase of sophisticated Artificial intelligence (AI) and Machine Learning (ML) algorithms in high-frequency and propriety trading has introduced a new paradigm of informational asymmetry, granting select entities an "Algorithm Advantage" that challenges the core legal constructs of insider trading.

AI systems are now capable of analyzing vast, real-time datasets to identify complex market pattern that are imperceptible to human traders[2]. This computational superiority enables the autonomous synthesis of predictive market intelligence that is functionally equivalent to unpublished Price Sensitive Information (UPSI). The central argument of this paper is that the current Indian legal framework, rooted in the anthropocentric concepts of intent i.e. (*mens rea)* and human communication/possession of information, is conceptually ill-equipped to police this high-speed, autonomous form of informational exploitation. The deployment of AI/ML strategies, therefore, creates a regulatory void, necessitating a fundamental legislative overhaul. In 2012 Knight Capital Group lost **$440 million in 30 minutes** due to a faulty trading algorithm[3], illustrating how potent and hazardous algorithmic strategies can be. More recently, U.S. firm *Jane Street* was banned and fined for $565 million by Indian regulators in 2025 in allegation that its automated trade manipulated India's Nifty index[4] [5]. These cases while not classical "Insider Trading" underlines how opaque AI strategies can disrupt markets.

I.B. Research Question

This research seeks to address the critical regulatory challenges posed by advanced computational finance:

[1] The Inst. of Company Secs. of India, *A Handbook on SEBI (Prohibition of Insider Trading Regulations), 2015*,(2015), https://www.icsi.edu/portals/2/SEBI%20Insider%20Trading%20Regulations2015.pdf.
[2] T. Lau & X. Wu, *The Algorithmic Advantage: AI-Driven Insider Trading and Regulatory Gaps*, arXiv preprint, 7–8 (2025), *available at* https://arxiv.org/html/2502.08728v2

1. How are autonomous AI/ML models using the computational power in such a way as to create informational advantages that are in effect indistinguishable from UPSI, thus violating the spirit and purpose of market integrity regulations?

2. In which areas of the current Indian law doctrines, especially regarding the ascription of criminal intent (mens rea), the definition of an Insider, and the extent of UPSI, does the algorithmic activity fail that has been autonomously functioning?

3. What precise legislative and technological measures, as a result of the comparison with the well-functioning regulatory frameworks in the European Union (MiFID II) and the United States (SEC/FINRA), would be needed to sufficiently close these regulatory gaps in India?

I.C. Significance of the Study

The Securities and Exchange Board of India (SEBI) has a mandate to prohibit insider traders from profiting while in possession of UPSI and to ensure investor confidence in the mark1. Historically, Indian regulation has evolved through landmark committees from the Thomas committee (1948) to the Justice N.K. Sodhi Committee (2013) leading to substantial amendments and the eventual PIT regulations of 20151. These revisions largely focused on closing loopholes related to human communication, relation access, and physical documents.

However, the current wave of technological advancement represents a systemic risk that cannot be mitigates solely by adjusting human-centric compliance protocols. Global regulatory bodies, including IOSCO, recognize that AI systems present potential risk stemming from malicious uses, data consideration, and concentration effects[6]. As India's market structure becomes increasingly reliant on quantitative and algorithmic strategies, a proactive, exhaustive analysis

[3] Matthew Matthew Heusser, *Software Testing Lessons Learned from Knight Capital Fiasco*, CIO (Aug. 14, 2012), https://www.cio.com/article/286790/software-testing-lessons-learned-from-knight-capital-fiasco.html
[4] Jayshree P. Upadhyay, *Indian court tells markets regulator to respond to Jane Street's appeal, delaying orders*, Reuters (Sept. 9, 2025), https://www.reuters.com/sustainability/boards-policy-regulation/indian-court-tells-markets-regulator-respond-jane-streets-appeal-delaying-orders-2025-09-09/
[5] FTI Consulting, When Algorithmic Trading Meets Allegations of Market Manipulation: The Jane Street – SEBI Case (July 28, 2025) https://www.fticonsulting.com/insights/articles/when-algorithmic-trading-meets-allegations-market manipulation#:~:text=On%20July%203%2C%202025%2C%20India%E2%80%99s,frequency%20trading%20and%20market%20abuse
[6] C. Kuey, *The Promise of Machine Learning in Detecting Insider Trading*, 1 J. Fin. Crime Det. (2025) https://kuey.net/index.php/kuey/article/download/4167/2777/9423

of the resulting regulatory failure points is essential to protect the integrity of the rapid evolving financial infrastructure and secure fair price discovery.[7]

II. THE TECHINCAL FOUNDATION: MECHANISM OF ALGORITHMIC ADVANTAGE

This section establishes the technical necessity of regulatory intervention by analyzing how computational models generate informational asymmetry that is functionally equivalent to illegally obtained UPSI.

II.A. Defining the Technological Shift

Algorithmic trading encompasses a spectrum of strategies, ranging from simple rule-based order routing to complex highly adaptive AI/ML programs. Advanced ML algorithms are mathematical constructions designed to change and evolve in response to the training data they process, allowing them to deliver present results[2]. Unlike traditional, static algorithms, these systems have the ability to learn from historical data and indentify intricate patterns invisible to human observation[2].

This technological shift allows firms to deploy strategies that move beyond mere speed advantages (High-Frequency Trading) into the domain of next generation analytical capabilities. AI's ability to process and analyze data in real time offers a distinct advantage over traditional surveillance methods, enabling algorithms to detect and capitalize on market shifts as they unfold, rather than after the fact[6].

II.B.1. Real time Processing and predictive capabilities

The primary mechanism of the algorithmic advantage lies in the ability of AI/ML models to synthesize disparate streams of nonpublic data, generating highly accurate predictions of stock price movement. By analyzing massive datasets, including high-frequency order book data, firm-specific trading patterns, sentiment analysis (derived from news and social media feeds), and potentially historical insider trading activities, these algorithms can identify key factors that impact prices[2].

[7] Int'l Org. of Sec. Comm'ns, *Artificial Intelligence (AI) in the Financial Sector*, IOSCOPD788, 3–4 (2024), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD788.pdf

This analytical capacity provides a form of computational foresight. The models do not merely react to market data; they predict market trajectory based on AI derived correlations. This capability allows proprietary trading firms and hedge funds to consistently stay ahead of the curve, detecting opportunities and making high-volume trades before human regulators or compliance systems can register the underlying informational flow[6].

II.B.2. Blurring Lines: Insider Trading, Manipulation and Tacit Collusion

The risks posed by autonomous systems extend beyond traditional insider trading definitions. As noted by analysts examining computational finance, AI introduces emerging market abuse risks, including complex forms of market manipulation and the potential for "tacit" collusion among autonomous algorithms[8].

SEBI has acknowledged the serious market impact of quant-driven strategies. Recent regulatory scrutiny, such as investigations into expiry day hiding, indicates that technologically advanced strategies which are financially engineered attract serious consequences if they distort fair price discovery[9]. The regulator's focus on complexity and cross segment trading impacts demonstrates a recognition that abuse mechanisms, are, shifting from simple, human executed from running to intricate, scale driven algorithmic distortion[9].

II.C. The Functional Equivalency of UPSI

The core challenge for Indian law lies in the concept of functional equivalency regulations define UPSI as information related to a company or its securities that is not generally available and which, upon becoming generally available is likely to materially affect the price of the securities[10]. This definition assumes the information as a discrete, identifiable entity (e.g. a merger announcement or financial results)[11]. However, when an algorithm aggregates and processes terabytes of proprietary, real-time market microstructure data; which is technically

---

[8] A. Upadhyaya, Emerging Risks in Computational Finance: Market Manipulation and Tacit Collusion by Autonomous Algorithms, 42 U. Pa. J. Int'l L. 101, 105 (2021), available at https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2035&context=jil.

[9] A. Saxena, *Jane Street and the Expiry Day Trap: Unpacking SEBI's Crackdown on Algorithmic Strategies*, Oxford Bus. L. Blog (2025), *available at* https://blogs.law.ox.ac.uk/oblb/blog-post/2025/07/jane-street-and-expiry-day-trap-unpacking-sebis-crackdown-algorithmic

[10] PwC, *Understanding UPSI and the SEBI PIT Regulations*(2024), https://www.pwc.in/assets/pdfs/services/ras/upsi.pdf

[11] A. Sarkar, *SEBI (PIT) Regulations 2015 and 2024 Amendments: An Analysis of Digital Tracking*, 12 Int'l J. Creative Rsch. Thoughts (2024), https://www.ijcrt.org/papers/IJCRT2509282.pdf

'non-disseminated' and inaccessible to the general public, it generates predictive intelligence that us statistically indistinguishable from processing a conventional piece of UPSI.

The issue is not that the data itself is secret, but that the *computational infrastructure* required to process it is proprietary and grants an insurmountable informational edge. If an AI analyzes complex market dynamics and patterns (invisible to human eyes) to make accurate predictions[2], the informational asymmetry created is functionally identical to the illegal asymmetry to recognize *computational asymmetry* as a distinct and equally harmful form of market abuse. The current framework fails because the market advantage is derived not from possessing a specific secret fact, but from the exclusive ability to synthesize proprietary facts into actionable foresight.

III. THE INADEQUACY OF INDIAN INSIDER TRADING LAWS (SEBI PIT Regulations, 2015)

The Indian legal framework for regulating insider trading is predicated on an anthropocentric model of culpability and information flow. This section critically analyzes why the core definitions and the recent *regular technology* (Advance digital tools like AI/ML) response; the Structured Digital Database (SDD) are inadequate against autonomous AI systems.

III.A. Anthropocentric Foundation

The SEBI PIT Regulations, 2015, are instances where India rely heavily on defining and tracking human activity and intent.

III.A.1. The Definition of 'insider' and 'Possession'

Regulation 2(1)(g) defines an 'insider' as any person who is a connected person or is "in possession of unpublished price sensitive information."[12] This construction presupposes a conscious human actor. Similarly, Section 12A Clause (e) of the SEBI Act, 1992, prohibits a *person* from dealing in securities while in possession of material or non-public information[10].

When an autonomous AI model operates, it possesses predictive certainty, yet it lacks the conscious human mental state required by most liability doctrines. If the AI executes a trade

[12] Securities and Exchange Board of India, *FAQs on SEBI (PIT) Regulations, 2015*, Reg. 2(1)(g) (2015), https://www.sebi.gov.in/sebi_data/faqfiles/apr-2025/1744784643061.pdf.

autonomously based on its synthesized intelligence, the question of who is the "person in possession" of the UPSI becomes a philosophical and legal dilemma. Neither the engineer, who designed the model, nor the operator, who may lack technical control over its tactical decisions, neatly fits the traditional definition of the insider[13].

III.A.2. The Definition of 'UPSI'

UPSI is defined based on the information that is "not generally available"[10]. While this definition covers the data input used by the AI, it fails to account for the transformation of generally available, non-price sensitive data points into highly predictive, price-sensititive intelligence through proprietary computation.

The SEBI framework assumes a static, discrete piece of information that, if revealed, would move the market. The algorithmic advantage relies on dynamic, synthesized intelligence that only becomes market-moving though the algorithm's application, making the resulting informational advantage conceptually distinct from conventional UPSI.

III.B. The Limitations of the Structured Digital Database (SDD)

Due to issues like information leaks through digital channels, SEBI introduced the requirement for listed companies to maintain a Structured Digital Database (SDD) as per Regulation 3(5) of the PIT Regulations.[14]

III.B.1. Mechanism and Purpose

The SDD is a mandatory, non-tamperable digital log designed to chronologically record every communication of UPSI, including details of the Designated Persons and Insiders involved, the sender's and recipient's names, and necessary time-stamps.[14]

This framework was established, in part, to address the challenge of data breaches and insider collaboration exposed through platforms like WhatsApp and Telegram, which SEBI explicitly

[13] V. Sharma, *Accountability by Design: Shared Liability in AI Fraud Under Indian Cyber Law*, Virtuosity Legal (2024),https://virtuositylegal.com/accountability-by-design-shared-liability-in-ai-fraud-under-indian-cyber-law/
[14] A. Tuteja, *SEBI SDD Compliance: Legal Requirements and Penalties*, Legality Simplified (2023), https://www.legalitysimplified.com/sebi-sdd-compliance/; *see also FAQs Structured Digital Database (SDD)*, NSE Circular (Oct. 28, 2022), https://ca2013.com/wp-content/uploads/2022/10/NSE-Circular_28.10.2022_Annexure-II.pdf.

acknowledged as having made insider trading common in India[11]. The goal is to track how confidential market-moving information flows, both internally and externally[14].

III.B.2. Efficacy VS Algorithmic Threats

The SDD framework, while a vital technological tool for traditional compliance, is fundamentally inadequate against AI-driven insider trading. The SDD is designed to police the *relational source* of insider trading: human communication or unlawful procurement.

When an AI system is deployed in a proprietary trading environment, it operates as a closed loop intelligence gatherer. If a Designated Person feeds raw, non-UPSI data into a sophisticated ML model, and the model then autonomously executes a profitable trade based on the generated predictive insight, there is no UPSI "communication," "sharing," or "procurement" to log in the SDD[14].

The critical failure point is that the SDD monitors the ingress and egress points for human information flow, but AI circumvents this by *generating* or *synthesizing* the predictive advantage internally within the proprietary system. The algorithm itself acts as the "insider" possessing the predictive insight, rendering the SDD a necessary, but ultimately insufficient, mechanism for regulating fully autonomous computational abuse. This structural blind spot means that even perfectly compliant SDD logs will fail to capture the existence of an algorithmic informational edge.

SEBI PROVISIONS	OBJECTIVES	EFFICACY AGAINST AI-DRIVEN INSIDER TRADING
Regulation 2(1)(g) (Insider Definition)	Defines based on connection or possession of UPSI (Human-centric).	Fails to assign possession or access when the informational advantage is synthesized autonomously by a non-human system.
Regulation 3(5) (SDD Maintenance)	Track communication and procurement of UPSI via sender/recipient logs.	Ineffective for detecting information *generated* or *synthesized* internally by an

		AI model, which does not constitute communicable UPSI.
SEBI Act Section 12A(e) (Prohibition)	Prohibits dealing while in possession of material non-public information.	Difficult to enforce due to the *Mens Rea* challenge, requiring proof of human knowledge or intent behind the autonomous trade execution.

IV. THE LEGAL ABYSS: CHALLENGES IN ACCOUNTABILITY IN INDIAN JURISPRUDENCE

Indian law prosecution of AI financial crime under Indian law faces severe conceptual barriers rooted in traditional criminal jurisprudence. The two main concepts of *actus reus* (guilty act) and *mens rea* (criminal intent) face conceptual strains when applied to non-anthropocentric systems[15].

IV.A. The Mens Rea Crisis and AI autonomy

The central problem of proving algorithmic market manipulation is the attribution of criminal intent. AI setups follow intricate mathematical functions and established patterns but do not have the human-like cognitive states that are required for mens rea[15].

IV.A.1. The Liability Gap

Conventional criminal law principles have a hard time understanding the concept of the AI's autonomy, hence the problem of a liability gap which is considerable in size.[13]. In the context of AI fraud, the chain of accountability is blurred because the actual execution of the manipulative or abusive trade occurs autonomously after the system is designed[13]. Courts and regulators face immense difficulty applying traditional notions of intent. A developer may not anticipate every possible misuse or unintended consequence of a complex model, and the user

[15] R. Law, *Criminal Accountability for AI: Mens Rea, Actus Reus, and the Challenges of Autonomous Systems*, LIJDL R. (2025), *available at* https://lijdlr.com/2025/04/05/criminal-accountability-for-ai-mens-rea-actus-reus-and-the-challenges-of-autonomous-systems/

operating the system may lack technical control over its moment-to-moment decisions, neatly fits the traditional definition of the insider[13]. For instance, if an algorithm, trained on historical market data, identifies a temporary informational gap and autonomously exploits it for proprietary profit, establishing the required level of human knowledge or willful intent to commit insider trading becomes almost impossible under the current SEBI Act framework.

IV.A.2. Legislative Limitations

Current Indian legislation, including the consolidated provisions for cyber offenses and the Bharatiya Nyaya Sanhita (BNS), 2023, still assumes human actors[1315]. The absence of explicit, AI-specific clauses leaves ambiguity regarding whether autonomous systems fall under the scope of criminal attribution, effectively insulating the human actors and developers from immediate responsibility for the algorithm's actions[15]. This reliance on temporary circulars and guidelines, instead of robust statutory provisions, weakens the liability framework regarding digital crimes[16].

IV.B. The 'Black Box' Problem: Causation and Evidence

Further compounding the mens rea challenge is the "Black Box" problem, which directly hinders the establishment of causation a critical element of actus Reus.

To put it simply, advanced AI algorithms, especially those that use deep learning, are usually very complex and it is hard to figure out their decision-making process[1317]. The absence of transparency causes the accountability to be lessened and the evidentiary value necessary for a criminal prosecution to be weakened[13]. When SEBI is probing a suspicious trade, it has to prove that the trade was carried out as a result of the algorithm having and using UPSI (or its functional equivalent). If the firm utilizing the algorithm cannot explain why the AI decided to initiate the order, determine the timing, or set the price, regulators cannot establish a clear causal link between the informational advantage and the prohibited trading activity[1718].

---

[16] M. Shekhar, *SEBI's Crackdown on Algo Trading: A Step Forward or a Regulatory Puzzle*, RFMLR (2024), https://www.rfmlr.com/post/sebi-s-crackdown-on-algo-trading-a-step-forward-or-a-regulatory-puzzle

[17] Sidley Austin LLP, *Artificial Intelligence in Financial Markets: Systemic Risk and Market Abuse Concerns* (2024), https://www.sidley.com/en/insights/newsupdates/2024/12/artificial-intelligence-in-financial-markets-systemic-risk-and-market-abuse-concerns.

[18] Eur. Sec. & Mkts. Auth., *MiFID II/MiFIR Final Report on Algorithmic Trading*, ESMA70-156-4572, 22–23 (2017),https://www.esma.europa.eu/sites/default/files/library/esma70-156-4572_mifid_ii_final_report_on_algorithmic_trading.pdf.

The opacity means that compliance officers and market operators may not even be able to recognize market abuse solely from the trading patterns and decisions generated by these machine learning models[17]. This evidentiary bottleneck grants sophisticated market actors a practical immunity from detection and prosecution.

IV.C. Redefining Accountability: Shifting focus from intent to Systemic Failure

In view of the impasse encountered in ascribing mens rea to a non-human agent, the law should move away from the concept that a human insider has an internal mental state and concentrate instead on the failures of the system with regard to the design, deployment and control environment of the algorithmic system.

If the AI commits an act of insider trading, the law must identify a culpable human action in the preceding steps. This mandates a legal philosophy where inadequate system validation, insufficient risk controls, and lack of human oversight are defined as the proximate cause of the market abuse. The failure to test the algorithm rigorously prior to production, or the failure to monitor its activity adequately after deployment, must be codified as the breach of duty leading to *actus reus*.

This redefinition requires stronger statutory provisions that impose clear, non-negotiable obligations on developers, deployers, and intermediaries to ensure "accountability by design"[13].

V. COMPARATIVE REGULATORY BENCHMARK AND GLOBAL REGTECH STRATEGIES

International jurisdictions, having navigated the integration of algorithmic trading earlier, offer crucial frameworks for India to address the control and governance challenges inherent in AI systems. The regulatory responses in the EU and the US demonstrate a shift away from intent-based enforcement towards system-based accountability.

V.A. The European Union (MiFID II) 2018: Governance and Definition

The EU's Markets in Financial Instruments Directive II (MiFID II) has established specific guidelines for managing algorithmic risks. MiFID II defines algorithmic trading precisely as trading where a computer algorithm automatically determines individual order parameters; such as whether to initiate the order, the timing, price, or quantity with limited or no human

intervention[18]. This clear delineation sets the state for regulatory oversight.

MiFID II requires that investment firms that use algorithmic trading implement strict organizational measures (as explained in detail in Regulatory Technical Standard 6 or RTS 6) in order to reduce risks arising from algorithmic trading that might include the excessive loading of trading venue systems, the sending of wrong orders, the overreacting to market events as well as the perpetration of market abuse practices[18]. This emphasis on governance mandates measures related to pre-production testing, robust system validation, and periodic self-assessment[18].

Furthermore, the Market Abuse Regulation (MAR) requires operators of trading venues and professionals arranging transactions to report orders that could constitute insider dealing or market manipulation[17]. However, even under this advanced framework, international regulators acknowledge that determining "reasonable suspicion" becomes problematic when complex AI models identify and exploit market patterns that are not immediately recognizable to human observers[17].

V.B. The United States (SEC/FINRA): Systemic Controls and Accountability

The US regulatory environment, managed by the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), centers on rigorous risk management and accountability measures for firms utilizing high-speed strategies.

V.B.1. Risk Management Controls and Supervision

SEC Rule 15c3-5 mandates that brokers or dealers with market access must establish, document, and maintain comprehensive risk management controls[18]. FINRA complements this by issuing extensive guidance on effective supervision and control practices for firms engaging in algorithmic strategies[1920].

This supervision framework includes:

[19] Fin. Indus. Regulatory Auth., *Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies*, Reg. Notice 15-09 (Mar. 26, 2015), *available at* https://www.finra.org/rules-guidance/notices/15-09.

[20] Fin. Indus. Regulatory Auth., *SEC Approves Rule to Require Registration of Associated Persons Involved in the Design, Development or Significant Modification of Algorithmic Trading Strategies*, Reg. Notice 16-21 (June 6, 2016), *available at* https://www.finra.org/rules-guidance/key-topics/algorithmic-trading.

1. **Software Testing and Validation:** Any algorithm-based solution should be subjected to a comprehensive testing procedure before being put into operation so as to meet the regulatory requirements and ensure stability in the market. [20]

2. **Continuous Monitoring:** Companies are required to keep track of the trading activity on a regular basis after the implementation or modification of a strategy based on algorithms. [19][20]

3. **Cross-Disciplinary Oversight:** It is a good practice for a company to have cross-disciplinary committees that bring together staff from compliance, risk, and development departments to comprehensively evaluate and control the risks that arise from complicated algorithmic strategies. [19]

V.B.2. Accountability of Personnel

Crucially, FINRA has established rules that require the registration of associated persons involved in the *design, development, or significant modification* of algorithmic trading strategies (Regulatory Notice 16-21)[20]. This shifts the regulatory focus from the algorithm's autonomous actions to the human experts who architect the system. In the event of registering these developers, the framework conveys the human accountability as clear, recognizable nodes which are the ones responsible for the algorithm's compliance and integrity.

VI. POLICY RECOMMENDATION AND LEGAL ROADMAP FOR INDIA

India needs a holistic approach, which includes a legislative modernization, mandatory technological transparency, and a systemic approach of adopting robust organizational governance standards, to address the in-depth regulatory gaps that have been identified.

VI.A. Legislative Overhaul: Replacing Mens Rea with Strict Liability

The most direct solution to the *mens rea* crisis is the statutory implementation of a **strict liability** regime for defined categories of algorithmic market abuse, including AI-driven insider dealing and manipulation[16].

VI.A.1. Imposing Strict Liability

If SEBI were granted the authority to impose automatic civil fines based solely on the market

outcome—a demonstrable harm or unfair profit resulting from algorithmic activity—it would circumvent the legal burden of proving human intent[16]. This proposal aligns with the strict liability provisions found in certain international anti-fraud rules, such as SEC Rule 10b-5, which simplifies enforcement against entities utilizing opaque, autonomous systems[16]. The focus would shift entirely to the objective consequence of the trade: market integrity distortion or informational exploitation.

VI.A.2. Mandatory Disclosure and Penalities

This strict liability framework should be coupled with a mandate that requires firms to disclose details of their algorithms upon regulatory request. Strong statutory provisions are essential, as relying on temporary circulars is insufficient[16]. Firms unwilling or unable to disclose their algorithms as required would automatically incur substantial fines, forcing transparency and accountability for the market-moving strategies they deploy[16].

VI.B. Mandating Algorithmic Transparency and Auditability

To mitigate the "Black Box" problem, SEBI must mandate features that ensure the traceability and comprehensibility of high-risk algorithms used in capital markets.

VI.B.1. Accountability by Design (AI-XAI)

For all AI/ML models deployed for market-facing functions, SEBI should introduce a requirement for Explainable AI (XAI) features. This "Accountability by Design" philosophy ensures that the underlying logic and data correlations leading to a trade decision can be articulated and audited[13]. While perfect comprehensibility is challenging for deep learning models, mandatory standards for audit-traceable outputs and feature importance mapping would significantly aid compliance and regulatory scrutiny, particularly in establishing causation where complex patterns are exploited[17].

VI.B.2. Compulsory System Audits

Before the deployment of algorithmic models and on a periodic basis thereafter, SEBI should require these models to undergo compulsory, independent third-party audits. Not only must these audits corroborate the regulatory features hardwired in the code, but they must also check the algorithms for strength against taking advantage of informational gaps and verify that their

behavior is non- manipulative.

VI.C. Strengthening Organizational Requirements and Human Accountability

India must adapt the successful governance models utilized in the US and EU to establish clear human accountability nodes within regulated entities.

VI.C.1 Mandatory Governance Frameworks

SEBI must introduce statutory requirements compelling firms utilizing advanced AI to establish cross-disciplinary committees including representatives from risk, compliance, legal, and development teams tasked with the holistic assessment and management of algorithmic risks.^{17} This ensures effective communication and periodic evaluation of compliance tools and supervisory frameworks, adapting them to current market conditions[19].

VI.C.2. System Validation and testing Requirements

Mirroring the FINRA framework, SEBI should mandate statutory standards for rigorous pre-production testing and system validation. This includes continuous monitoring protocols and clear mandates for communication between compliance staff and the personnel responsible for strategy development[20]. The regulatory focus should be on ensuring that the firm's trading activity complies with applicable rules (e.g., FINRA Rule 5210 regarding transaction publication and 2010 regarding high standards of commercial honor)[19].

VI.C.3. Registration of Key Personnel

EBI should require the registration of associated persons involved in the design, development, or significant modification of market-facing algorithms. This measure, similar to FINRA's Regulatory Notice 16-21[20], establishes statutory human accountability for the actions of autonomous systems by holding developers responsible for ensuring compliance and effective risk controls.

VI.D. Statutory Reforms for Cyber and Financial Crime

To resolve the broader legal voids related to AI culpability, amendments must be pursued in wider Indian jurisprudence:

1. **SEBI Act Amendments:** Introduce explicit provisions defining "algorithmic advantage" as a form of non-permissible informational asymmetry and create a specific offense category for market abuse facilitated by autonomous systems.

2. **BNS and IT Act Expansion:** Expand the Bharatiya Nyaya Sanhita and the Information Technology Act, 2000, to explicitly criminalize fraud and market abuse conducted by autonomous AI systems. This would bridge the existing liability gap by defining clear obligations for developers, deployers, and intermediaries in the event of AI-caused harm[1315]. Furthermore, the Consumer Protection Act, 2019, could be leveraged to incorporate AI-specific product liability provisions to enable compensation for victims of AI fraud[13].

VII. CONCLUSION

The rise of AI-driven trading has presented Indian market regulators with an existential challenge to the principle of informational parity. The deployment of Machine Learning models allows for the high-speed synthesis of predictive market intelligence—the Algorithmic Advantage—that is functionally equivalent to Unpublished Price Sensitive Information, thereby circumventing the spirit of the SEBI PIT Regulations, 2015.

The analysis confirms that the current Indian framework is fundamentally constrained by its reliance on anthropocentric concepts. The definitions of "Insider" and "possession of UPSI" strain credibility when applied to autonomous systems, and modern compliance tools like the Structured Digital Database are inherently blind to information synthesized internally by AI. The critical conceptual barrier lies in attributing *mens rea* in the face of the "Black Box" problem, granting practical immunity to firms utilizing the most opaque strategies.

The path forward requires a shift in regulatory philosophy from proving individual human intent to enforcing systemic accountability. By adopting strict liability for adverse market outcomes, mandating robust system governance and pre-production testing (drawing from MiFID II), and establishing human accountability nodes through developer registration and XAI mandates (drawing from FINRA/SEC), India can secure the integrity of its capital markets. Only through such comprehensive legislative evolution, moving beyond anthropocentric paradigms, can SEBI effectively address the distinctive characteristics and unprecedented risks posed by autonomous AI.