# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

**ISSN: 2582-6433**

# DISCLAIMER

**ISSN: 2582-6433**

# ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

# *PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT*

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

# THE REGULATORY OVERSIGHT OF ARTIFICIAL INTELLIGENCE IN CAPITAL MARKETS: A CRITICAL STUDY OF THE SEBI 2026 FRAMEWORK AND THE EVOLUTION OF ALGORITHMIC TRADING INTEGRITY

AUTHORED BY - SHRADDHA UPADHYAY
LLM (Corporate Law),
GD Goenka University

## Abstract

The structural evolution of the Indian capital markets has entered a definitive era of systemic transformation, characterized by the transition from human-intermediated oversight to the direct supervision of complex technical systems. As of April 1, 2026, the Securities and Exchange Board of India (SEBI) has implemented a comprehensive regulatory framework that mandates the pre-approval of all algorithmic trading strategies, with a specific emphasis on those driven by artificial intelligence (AI) and machine learning (ML). This regulatory shift represents the culmination of a decade-long reckoning with the risks of technological disruption, addressing a landscape where automated systems now account for more than 50% of the turnover in domestic equity markets. The 2026 mandate is not merely an operational update but a profound redirection of securities law, aiming to resolve persistent ambiguities in liability, enhance the transparency of "black box" logic, and create a robust audit trail for every automated decision.

## The Genesis of the 2026 Regulatory Reckoning

The journey toward the 2026 framework began in 2008 with the introduction of Direct Market Access (DMA) for institutional investors, yet the subsequent decade revealed significant gaps in enforcement as technology outpaced traditional rules. Between 2019 and 2024, the proliferation of broker APIs and cloud-based deployment tools democratized high-frequency trading (HFT), bringing complex automation to the retail segment. This era was marked by the rise of unregistered vendors operating via Telegram and social media, who distributed algorithmic strategies under the guise of "educational tools" while making unverifiable claims of guaranteed returns. SEBI’s data from the 2025 fiscal year underscored the urgency of

ISSN: 2582-6433

intervention, noting that individual retail net losses in the futures and options (F&O) segment had widened to ₹1.05 lakh crore, with over 90% of such traders losing money.

| Milestone Date | Regulatory Development | Primary Objective |
|---|---|---|
| April 3, 2008 | Introduction of DMA | Standardizing institutional algo access |
| March 30, 2012 | 2012 Circular (Risk Controls) | Mandating broker routing and prior exchange permission |
| August 5, 2016 | Discussion Paper on Fairness | Addressing the NSE co-location controversy |
| February 4, 2025 | Master Retail Algo Circular | Formalizing the 2026 compliance architecture |
| January 5, 2026 | Milestone for API Access | Barring non-compliant brokers from new client onboarding |
| April 1, 2026 | Full Mandatory Enforcement | Implementation of unique Algo-IDs and strategy registration |

The 2026 framework seeks to eliminate the "grey market" ecosystem by establishing a regulated playing field where every line of code executing a trade is auditable and every participant occupies a defined legal role. The regulator's philosophy has evolved from supervising institutions to supervising systems, recognizing that in a high-speed environment, the metadata of a decision is often more valuable than the decision itself.

**Procedural Mandates: Strategy Registration and Unique Identifiers**

The cornerstone of the SEBI 2026 mandate is the requirement for the pre-approval of algorithmic strategies by the stock exchanges. This process requires brokers to ensure that each algorithm is tested, certified, and approved before it enters the live market, a measure intended to reduce the frequency of erroneous or manipulative orders. The registration process involves deep documentation of the strategy's logic, back-testing against historical data, and evidence of robust risk management guardrails.

Once a strategy is registered, it is assigned a unique, exchange-provided Algo-ID. This ID serves as a digital license plate, allowing regulators to trace any market anomaly or flash crash back to the specific code and account responsible for the order flow. To prevent the over-regulation of minor personal scripts, SEBI has implemented a tiered threshold based on order

ISSN: 2582-6433

frequency.

| Activity Type | Threshold Metric | Regulatory Status |
|---|---|---|
| Regular API User | Below 10 Orders Per Second (OPS) | Exempt from formal strategy registration; uses Generic IDs |
| High-Frequency Trading | Above 10 Orders Per Second (OPS) | Mandatory individual strategy registration and unique ID |
| Low-Latency Arbitrage | Above 10 OPS per Segment | Subjected to rigorous testing and RA certification |

The 10 OPS threshold allows the majority of retail traders to continue using simple automation, such as moving average crossovers or systematic investment plan (SIP) equity scripts, without the burden of full registration. However, any strategy that exceeds this limit is classified as algorithmic, triggering mandatory disclosure and oversight. Furthermore, self-built algorithms remain restricted to personal and immediate family use; any attempt to distribute or sell these tools requires formal exchange empanelment.

**The Transparency Bifurcation: White Box versus Black Box Logic**

The 2026 framework introduces a critical distinction between "White Box" and "Black Box" algorithms, which determines the degree of regulatory scrutiny and the specific licensing requirements for the provider. White box algorithms are defined as transparent, rule-based systems where the logic is visible and can be independently replicated by the user or the regulator. These systems, typically including simple execution tools such as Volume Weighted Average Price (VWAP) or Time Weighted Average Price (TWAP), are subject to a more straightforward approval process.

In contrast, black box algorithms involve proprietary or AI-driven logic where the internal decision-making process is hidden. Because these models learn dynamically from market data and may produce unpredictable outputs, they represent a significant risk to market integrity. To mitigate this, SEBI mandates that providers of black box strategies must be registered as Research Analysts (RA). This requirement imposes a fiduciary duty on the provider, forcing them to maintain detailed research reports for every algorithm and to confirm to the exchanges that the performance metrics and risks have been documented.

The mandate for RA registration for black box providers is designed to ensure that innovation does not come at the cost of transparency. Any material modification to the logic of a black

ISSN: 2582-6433

box algorithm is treated as a new strategy, requiring re-registration and a new approval cycle. This prevents "parameter-fitting" or the injection of new, unverified logic into previously approved models. For the retail investor, this marks a shift from a "plug-and-play" mentality to an "understand-and-deploy" paradigm, as they can no longer legally subscribe to opaque strategies without verifying the provider's regulatory credentials.

**Liability Frameworks: The Broker-Principal Model and Kill Switches**

The resolution of the "attribution problem"—the question of responsibility when an algorithm causes harm—is the primary innovation of the 2026 liability framework. Prior to this period, brokers often claimed they were merely providing the infrastructure for third-party scripts, while vendors argued they were purely technology providers, leaving a void in accountability for flash crashes. The 2026 framework resolves this by establishing a clear principal-agent relationship: the broker is the principal and the algo provider is the agent. Consequently, the broker is legally responsible for every order generated by an algorithm running on their platform.

| Entity | Role under 2026 Framework | Statutory Responsibility |
|---|---|---|
| Stockbroker | Principal | Approval of strategies; maintenance of audit trails; grievance redressal |
| Algo Provider | Agent | Documentation of code; compliance with RA norms for black box models |
| Exchange | Supervisor | Implementation of "Kill Switches"; SOPs for emergency deactivation |

This architecture requires brokers to implement real-time monitoring tools and "kill switches" that can immediately disable malfunctioning algorithms to prevent systemic disruptions. While the kill switch is a vital safety mechanism, its implementation raises legal concerns regarding arbitrary deactivation. If a kill switch is activated during a period of market stress without an adequate SOP, it could lead to unfair disadvantages for retail investors or trigger runaway execution loops if interconnected systems react to the sudden withdrawal of liquidity.

Furthermore, the updated Technical Glitch Framework, effective January 9, 2026, has shifted the penalty structure to be more rationalized and risk-based. Penalties are now calculated based on the broker's size, the number of affected clients, and whether a secondary trading mode remained functional during the outage. This framework exempts smaller brokers with fewer

ISSN: 2582-6433

than 10,000 clients from the most expensive disaster recovery mandates, while ensuring that the infrastructure supporting millions of retail users is held to institutional standards of resilience.

**Algorithmic Manipulation and High-Frequency Forensics: The Jane Street Case**

The July 2025 enforcement action against Jane Street Group serves as a landmark case study for the 2026 framework's emphasis on "process integrity" over simple economic rationale. SEBI's 105-page interim order detailed a coordinated strategy that allegedly distorted the Bank Nifty index across 18 derivative expiry days between 2023 and 2025. The investigation utilized high-frequency forensics to uncover a recurring pattern known as the "Two-Patch Playbook".

In Patch I (the morning session), Jane Street aggressively purchased bank Nifty component stocks and futures, often representing more than 20% of the market-wide traded value in scrips such as Kotak Bank and Axis Bank. These orders were consistently placed above the last traded price (LTP), artificially inflating the index level. Simultaneously, the firm built massive short positions in liquid index options, establishing a net bearish delta that would benefit from a subsequent decline in the index. In Patch II (the afternoon session), the firm reversed its earlier activity, unleashing aggressive sell orders that coincided with options expiry to depress the settlement price and earn outsized profits on its derivatives positions.

| **Phase** | **Algorithmic Mechanism** | **Index Impact** | **Derivatives Result** |
|---|---|---|---|
| Patch I | Aggressive Buy Orders > LTP | Support/Inflation | Building Short Gamma/Delta |
| Patch II | Reversing long positions | Depressing Settlement | Realizing Gains on Puts/Short Calls |

SEBI concluded that this was a "deliberately devised device" to interfere with market discovery, impounding unlawful gains of approximately ₹4,843 crore. The case has profound implications for algorithmic liability, as it signals that intent can be inferred from the scale and timing of automated trade patterns, even in the absence of a "smoking gun" email or human instruction. For institutional participants, the JS case necessitates a recalibration of quant models that assume stable, unmanipulated settlement mechanisms, particularly around unpredictable expiry-day volatility.

ISSN: 2582-6433

**Explainable AI (XAI) and the Standards for Financial Audits**

The rapid adoption of generative AI and automated decision-making has triggered a global shift toward mandatory "Explainable AI" (XAI) standards. In 2026, XAI is no longer a peripheral feature but a binding compliance requirement for financial institutions. SEBI's 2026 regulations require AI models used for market analysis or advisory services to be transparent and ethical, mandating clear documentation of how models make individual trading decisions. A key development in 2026 is the implementation of "Reasoning Logs" for AI agents. Before an AI system outputs a recommendation or executes a trade, it must generate a step-by-step metadata log of the data joins and business filters applied. This prevents "Vibe Coding"—the early-2026 phenomenon where AI agents "guessed" business logic rather than following deterministic rules. The Bank for International Settlements (BIS) has supported this shift, recommending impact-based standards where models used for critical business areas, such as underwriting or capital requirement determination, are subject to higher scrutiny and the mandatory use of XAI techniques.

| Governance Factor | 2026 Mandate | Implementation Mechanism |
|---|---|---|
| Transparency | Elimination of Black-Box Omissions | Metadata reasoning logs and model cards |
| Integrity | Preventing Strategy Drift | Mandatory re-registration for version updates |
| Fiduciary Duty | AI Advice Accountability | Investment Advisor solely responsible for AI outputs |
| Data Security | Privacy-by-Design | VAPT and NIST Privacy Framework 2026 update |

The SEC in the United States has also intensified its focus on "AI-washing"—the misrepresentation of AI capabilities by firms seeking to project an image of technological sophistication. The SEC's 2026 examination priorities emphasize that leadership must understand what their AI systems do and the material risks they pose, treating AI as part of a firm's core operations rather than an external tool. This aligns with SEBI's view that using AI does not reduce responsibility but rather increases the burden of oversight.

**Digital Securities and Fractional Ownership under the SCRA**

The tokenization of real-world assets (RWAs)—representing rights to tangible property such

ISSN: 2582-6433

as real estate, infrastructure, and gold as blockchain-based digital tokens—represents a significant frontier for the Indian capital market. While technologically sound, the concept faces major legal challenges under the Securities Contracts (Regulation) Act, 1956 (SCRA). The primary hurdle is the broad and inclusive definition of "securities" in Section 2(h) of the SCRA.

Tokens that represent fractional investment in a project, where income is managed by a central entity and investors lack day-to-day control, are likely to be classified as units in a Collective Investment Scheme (CIS). Judicial interpretation in India, notably the *PGF Ltd. v. Union of India* and *Osian's Art Fund* cases, establishes that SEBI prioritizes "substance over form," treating any pooled-yield product as a security regardless of its digital label.

| **Token Type** | **Financial Equivalent** | **Regulatory Pathway** |
|---|---|---|
| Real Estate Token | REIT Unit | Small and Medium REIT (SM-REIT) Framework |
| Private Credit Token | AIF Unit | Category II/III Alternative Investment Fund |
| Infrastructure Token | InvIT Unit | Infrastructure Investment Trust (InvIT) Regulations |
| Virtual Digital Asset | Property | VDA Tax Regime and PMLA Reporting |

A fundamental conflict exists between the Registration Act, 1

| **Liability Theory** | **Basis for Accountability** | **Application to AI Trading** |
|---|---|---|
| Vicarious Liability | Principal responsible for agent's acts | Broker held liable for empanelled vendor's code |
| Strict Liability | Liability regardless of fault | Holds firms responsible for high-risk systemic shocks |
| Product Liability | Manufacturing/Design defect | Applicable if the algorithm's base code is fundamentally flawed |
| Active Diligence | Affimative duty of care | Directors liable for failing to oversee technical risk |

908, and blockchain technology: in India, land titles are not conclusive evidence but are presumed true unless challenged, and transfers of immovable property must be physically registered and stamped. To legally align tokens with property rights, issuers often utilize an

ISSN: 2582-6433

SPV-based structure, where the property is owned by a body corporate and the tokens represent equity in that entity, thereby bringing the transaction under the SCRA's established oversight. The Asset Tokenisation (Regulation) Bill 2026, introduced as a Private Member's Bill in March 2026, seeks to provide the missing statutory framework. The Bill recognizes asset tokens as valid digital representations of rights and economic benefits while clarifying that the issuance of a token does not, by itself, transfer ownership of the underlying physical asset. It proposes a coordinated multi-regulator model where SEBI remains the principal authority for tokens involving securities, while the RBI oversees tokens integrated with payment systems or stablecoins.

**Liability for Autonomous Machines: Flash Crashes and Systemic Risk**

The occurrence of "flash crashes"—sudden price dislocations triggered by algorithmic interaction—poses a profound challenge to established liability regimes based on human intent (scienter). Automated markets are characterized by tight coupling, where a minor error, such as a coding bug or server malfunction, can trigger a series of rapid trades that disrupt the entire market. In February 2026, the failure of the AI-powered bot "Lobstar Wilde," which emptied its treasury in seconds due to a decimal-point programming error, demonstrated how autonomous agents can cause irreversible financial damage.

Legal theorists argue that algorithms should be reconceived as a novel legal category: pure legal agents without legal personhood. This suggests that "vicarious liability" is the most promising strategy to ground tort liability for autonomous-machine-caused harm. Under this model, the corporate deployer is held responsible for the tortious acts of the algorithm in the course of deployment, similar to the historical development of corporate criminal liability.

| Liability Theory | Basis for Accountability | Application to AI Trading |
|---|---|---|
| Vicarious Liability | Principal responsible for agent's acts | Broker held liable for empaneled vendor's code |
| Strict Liability | Liability regardless of fault | Holds firms responsible for high-risk systemic shocks |
| Product Liability | Manufacturing/Design defect | Applicable if the algorithm's base code is fundamentally flawed |
| Active Diligence | Affirmative duty of care | Directors liable for failing to oversee technical risk |

ISSN: 2582-6433

The SEBI 2026 framework incorporates elements of both vicarious and strict liability through its designation of brokers as "principals" and the implementation of mandatory pre-trade risk checks. This shift addresses the "NAT" (Normal Accident Theory) characteristics of modern markets, where large-scale technological accidents are inevitable due to the speed and interconnection of automated systems. By ensuring that every trade is tagged and every broker is accountable, the framework forces organizations to internalize the costs of their technological risks.

**Global Comparative Analysis and Regional Regulatory Trends**

India's 2026 framework is among the most structured in the world, particularly concerning retail participation. While global standards for AI governance remain high-level, implementation is fragmenting across distinct regional approaches to risk and innovation.

- **European Union (ESMA)**: The February 2026 supervisory briefing on algorithmic trading under MiFID II clarifies that any system determining an individual order parameter is algorithmic. ESMA emphasizes "lifecycle testing" and has reinforced pre-trade controls as technically non-bypassable.
- **United States (SEC/CFTC)**: The March 2026 joint interpretation focuses on a transaction-based analysis, applying the *Howey* test to determine if digital asset arrangements constitute securities. The U.S. remains focused on preventing "AI-washing" through aggressive enforcement of existing anti-fraud statutes.
- **Singapore (MAS)**: Through "Project Guardian," MAS is pioneering the use of permissioned blockchain infrastructure to customize and rebalance discretionary portfolios at scale, while its 2026 AI guidelines focus on board-level oversight and risk materiality assessments.
- **India (SEBI)**: India's approach is uniquely prescriptive regarding the "black box" provider's credentials, requiring both exchange empanelment and Research Analyst registration, a move that provides greater protection for a retail-dominated market.

**Future Outlook: SupTech and the Digital Personal Data Protection Act**

As the market continues to scale—with India leading global IPO activity in 2025 and total market capitalization exceeding ₹470 trillion—regulation is moving from silos to a coordinated, dynamic architecture. SEBI is currently deploying advanced AI tools for "Regulatory Intelligence," using behavior analytics to detect real-time signals of insider trading and herding dynamics on social media. This proactive enforcement model uses "SupTech" to

ISSN: 2582-6433

analyze content from financial influencers and flag gaps in the cybersecurity infrastructure of over 4,900 intermediaries.

Furthermore, any firm deploying AI in the Indian capital market must now navigate the Digital Personal Data Protection (DPDP) Act. SEBI requires that AI models be tested for privacy risks to ensure that the sensitive financial data of investors is not exposed through unintended model leakage. The proposed Digital India Act is expected to further codify these rules, potentially integrating algorithmic due diligence mandates within India's broader corporate governance framework.

**Conclusions and Practical Implications for Market Participants**

The SEBI 2026 mandate for the pre-approval of AI-driven strategies marks a fundamental shift toward a technology-agnostic yet system-aware regulatory regime. By mandating strategy registration, unique Algo-IDs, and the broker-principal liability model, SEBI has structured the automated retail market in a way that minimizes systemic fragility without stifling innovation.

For brokers and algo providers, the roadmap to compliance requires:

1. **Investment in Traceability**: Implementing the "Algo-ID" tagging for all order modifications and cancellations to maintain a five-year audit trail.
2. **Logic Transparency**: Ensuring that all "Black Box" models are backed by a SEBI-registered Research Analyst and that reasoning logs are maintained for all automated outcomes.
3. **Infrastructure Resilience**: Adhering to the 2026 Technical Glitch Framework, including the implementation of non-bypassable kill switches and disaster recovery sites for larger entities.
4. **Strategic Tokenization**: Developing fractional ownership platforms within the established SM-REIT or AIF frameworks while monitoring the progress of the 2026 Asset Tokenisation Bill.

The 2026 regulatory reset ensures that as AI becomes the digital extension of the market, it operates within a framework of accountability, fairness, and trust. The successful integration of these technologies depends on a hybrid approach that combines algorithmic precision with the "active diligence" of human overseers, ensuring that market integrity remains the primary anchor of India's fast-growing financial ecosystem.