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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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

ALGORITHMIC SURVEILLANCE VS HUMAN INTENT: EVIDENTIARY CHALLENGES IN PROVING INSIDER TRADING IN INDIA

AUTHORED BY - SUSMITA BISWAL[1] & ARIJIT MAITI[2]

ABSTRACT

The Securities and Exchange Board of India (SEBI) has undergone a fundamental transformation in its enforcement methodology, leveraging the Integrated Market Surveillance System (IMSS) and advanced data analytics to identify suspicious trading activity algorithmically. Yet a profound tension persists: insider trading, as penalised under the SEBI Act, 1992 and the SEBI (Prohibition of Insider Trading) Regulations, 2015 (PIT Regulations), remains a human-element offence requiring proof that an 'insider' traded 'on the basis of' Unpublished Price Sensitive Information (UPSI). Machines can identify patterns; they cannot establish mens rea.

This paper argues that while algorithmic surveillance constitutes an indispensable detection mechanism, it is insufficient as standalone proof under the current Indian insider trading framework, which fundamentally requires human intent and a demonstrable connection to UPSI. The paper maps SEBI's surveillance architecture against legal standards of proof, examines the 'use vs. possession' debate, analyses landmark cases, explores due process risks, and draws comparative insights from U.S. SEC enforcement practice. It concludes with a hybrid evidentiary reform agenda treating algorithmic outputs as structured investigative triggers subject to mandatory human verification.

Keywords: Insider Trading, SEBI, Algorithmic Surveillance, UPSI, IMSS, PIT Regulations 2015, Circumstantial Evidence, Due Process, Securities Law India.

[1] LL.B. Student at Amity Law School Kolkata, Amity University Kolkata, West Bengal
[2] LL.B. Student at Amity Law School Kolkata, Amity University Kolkata, West Bengal

ISSN: 2582-6433

CHAPTER 1 — INTRODUCTION

1.1 The Algorithmic Turn in Financial Regulation

The BSE and NSE together process tens of millions of trades daily, generating a dataset so vast that manual scrutiny is structurally impossible. Into this environment, SEBI has introduced the Integrated Market Surveillance System (IMSS)—a platform that ingests real-time price and volume data, cross-references trades against corporate event timelines, constructs network maps of connected individuals, and flags statistically anomalous trades in real time. SEBI's Annual Reports reveal a sustained increase in enforcement actions directly traceable to algorithmic detection, with a significant proportion of insider trading show-cause notices originating from IMSS alerts.

1.2 The Enduring Human Element

Notwithstanding surveillance sophistication, the substantive legal standard for insider trading liability has not undergone a corresponding evolution. The PIT Regulations define liability through inherently human categories. An algorithm can identify that a trade occurred shortly before a price-sensitive announcement; it cannot determine whether the trader possessed the information, whether they were aware of its price-sensitive character, or whether the trade was caused by that information rather than independent research or coincidence. The leap from 'suspicious pattern' to 'proven insider trade' involves precisely the kind of human intent analysis that algorithms are structurally ill-equipped to perform.

1.3 Statement of the Problem and Hypothesis

The central problem is the evidentiary gap between what SEBI's surveillance infrastructure can demonstrate and what Indian law requires. The paper's hypothesis is: 'While algorithmic surveillance enhances detection efficiency, it is insufficient as standalone proof under the current insider trading framework in India, which fundamentally requires human intent and a demonstrable connection to UPSI.'

CHAPTER 2 — LEGAL FRAMEWORK OF INSIDER TRADING IN INDIA

2.1 Legislative Evolution

Insider trading regulation traces its origins to the Companies Act, 1956, with limited and largely ineffective provisions. The enactment of the SEBI Act, 1992 represented a paradigm shift. The SEBI (Insider Trading) Regulations, 1992 were criticised for definitional ambiguity and

ISSN: 2582-6433

enforcement gaps, leading to their replacement by the PIT Regulations, 2015, following recommendations of the T.K. Viswanathan Committee. The 2015 Regulations remain the operative framework.

2.2 Definitional Architecture

2.2.1 The Insider

Regulation 2(1)(g) defines an 'insider' as any person who is a 'connected person' or who is 'in possession of or having access to' UPSI. A 'connected person' under Regulation 2(1)(d) includes persons associated with a company in any capacity during the six months preceding the trade—directors, employees, advisors, auditors, bankers, and their immediate relatives. The breadth of this definition extends liability far beyond traditional corporate insiders.

2.2.2 Unpublished Price Sensitive Information (UPSI)

UPSI under Regulation 2(1)(n) is information relating to a company or its securities that is (i) not generally available, and (ii) likely to materially affect the price of securities upon becoming available. The illustrative list includes financial results, dividends, mergers and acquisitions, changes in key management, and material litigation. Objective materiality, not subjective belief, is the applicable test.

2.2.3 The Prohibition on Trading

Regulation 4 prohibits an insider from trading in securities 'on the basis of' UPSI. This phrase—the pivot around which the entire evidentiary challenge turns—connotes a causal nexus: the UPSI must have influenced the trading decision. This is an inherently human, cognitive requirement that algorithmic tools cannot satisfy on their own.

2.3 The 'Use vs. Possession' Debate

The PIT Regulations, 2015 employ language closer to a 'use' standard than a pure 'possession' standard, though the distinction is frequently elided in SEBI enforcement proceedings. SEBI has often argued that proof of possession combined with suspicious trading patterns gives rise to a rebuttable presumption of use. The SAT and the Supreme Court have periodically pushed back, requiring a demonstrable causal connection between possession and the specific trade. This judicial resistance confirms that pattern evidence alone cannot satisfy the 'use' element of insider trading liability.

ISSN: 2582-6433

2.4 Standard of Proof

SEBI adjudication applies the civil standard: preponderance of probability. Confirmed by the Supreme Court in SEBI v. Rakhi Trading Pvt. Ltd. (2018), this is a lower threshold than the criminal standard. However, it does not dissolve the requirement to establish every essential ingredient. Even on a balance of probabilities, SEBI must prove: (i) the accused was an insider; (ii) they possessed UPSI; (iii) they traded; and (iv) the trade was 'on the basis of' UPSI. Algorithmic evidence may assist with (iii) and partially (i) but struggles fundamentally with (ii) and (iv).

2.5 Defences

Regulation 4 carves out exceptions where the trade is pursuant to a pre-submitted Trading Plan or where the accused demonstrates the transaction was not 'on the basis of' UPSI—e.g., pre-existing binding contracts or ESOP exercises. These defences are fundamentally dependent on human intent evidence. No algorithm can assess the credibility of such a defence narrative.

CHAPTER 3 — SEBI'S ALGORITHMIC SURVEILLANCE ARCHITECTURE

3.1 The Integrated Market Surveillance System (IMSS)

The IMSS is SEBI's primary technological infrastructure for real-time market monitoring, developed under the Market Intelligence and Investigation Department (MIID). It aggregates trading data from exchanges and processes it through pattern-recognition algorithms at a scale impossible through manual review. For insider trading detection, the relevant modules focus on temporal correlations between trading activity and corporate event announcements.

3.2 Data Inputs and Processing Phases

The IMSS draws on three data streams: (i) exchange-level trading data (broker identity, client account, trade time, security, quantity, price); (ii) corporate disclosure data (filings cross-referenced against trading timelines); and (iii) connectivity data (beneficial ownership, related-party relationships, and connected-person networks). Processing occurs in three phases: identification of pre-event trading, application of statistical anomaly filters, and network analysis mapping accounts to connected persons of the company.

3.3 Algorithmic Red Flags

SEBI enforcement orders reveal a recurring set of red flags:

ISSN: 2582-6433

- Unusual Trade Timing: Purchases or sales immediately before a significant announcement with no apparent public basis.
- Abnormal Volume: Trade size statistically inconsistent with the accused's historical behaviour.
- Price-Volume Correlation: The trade was positioned precisely to benefit from the impending market reaction.
- Account Connectivity: The account is linked to a person with access to the relevant UPSI.
- Coordinated Patterns: Multiple accounts entering or exiting positions in the same security within a narrow window.

3.4 Structured Digital Database (SDD) Requirement

The 2018 amendment inserted Regulation 3(5), requiring listed companies to maintain a Structured Digital Database recording all persons who access UPSI—including names, designations, PAN numbers, and access timestamps—preserved for a minimum of eight years. By cross-referencing the SDD against IMSS alerts, SEBI can construct a formal evidentiary chain: the SDD demonstrates UPSI possession; the IMSS demonstrates proximate suspicious trading. However, this chain still leaves the critical 'on the basis of' causal element inadequately addressed.

3.5 The Human Review Gateway and Its Limitations

SEBI's protocol positions the IMSS as a detection trigger, not a conclusive adjudicatory mechanism. Alerts are assigned to investigation officers who must conduct further analysis before issuing a show-cause notice. In practice, however, the volume of alerts creates institutional pressure that may reduce the depth of independent human analysis, and anchoring bias risks causing investigators to frame inquiry around algorithmic output rather than conducting a genuinely open-minded assessment.

CHAPTER 4 — EVIDENTIARY CHALLENGES: FROM PATTERN TO PROOF

4.1 The Core Evidentiary Gap

An algorithm establishes correlation; insider trading law requires causation. A pattern-recognition system can show that Account A traded Security X within 72 hours of

ISSN: 2582-6433

Announcement Y in unusual volume, and that Account A is connected to Person B in the company's SDD. What it cannot establish is that Person A's trading decision was made because of and on the basis of UPSI accessed by Person B—as opposed to independent analysis, a pre-existing investment thesis, or coincidence. This is not a pedantic distinction; it reflects the fundamental structure of a liability regime built on individual culpability.

4.2 The Inference Problem: Correlation ≠ Causation

The inferential leap—unusual trade + pre-event timing + connectivity = insider trading—is structurally vulnerable to the correlation-causation fallacy. In efficient, information-rich markets, traders routinely act on publicly available signals that may independently cause them to build positions before corporate announcements. The connectivity the algorithm flags does not establish that UPSI was communicated or received; it merely identifies the existence of a link. Only human investigation can determine whether that link was exploited.

4.3 The Mental State Problem

Insider trading is not a strict liability offence. The 'on the basis of' language requires a cognitive connection between the trader's knowledge of UPSI and their decision to trade. Mental states are inherently unobservable and can only be inferred from external conduct. Accused persons regularly advance credible alternative explanations—pre-existing mandates, technical triggers, portfolio rebalancing—that require a human evaluator to assess their credibility. No algorithm can weigh the plausibility of a narrative explanation against the pattern data it generated.

4.4 Admissibility vs. Probative Weight

Under the Information Technology Act, 2000 and Section 65B of the Indian Evidence Act, 1872, electronic records including algorithmic outputs are admissible in evidence. However, admissibility is distinct from probative weight. The 'black box' problem—SEBI has not publicly disclosed the precise parameters, thresholds, or weighting functions of its surveillance algorithms—means an accused cannot meaningfully challenge the methodology of an alert. This structural asymmetry is inconsistent with the audi alteram partem principle that governs SEBI's quasi-judicial proceedings.

CHAPTER 5 — CASE LAW ANALYSIS

5.1 SEBI v. Rakhi Trading Pvt. Ltd. (2018) — Supreme Court

The Supreme Court confirmed that civil preponderance standard governs SEBI penalty proceedings but insisted the regulator must establish every essential ingredient through legally sufficient evidence. The Court's reasoning cautions against inferential leaps unsupported by

ISSN: 2582-6433

evidence beyond mere pattern correlation. The decision provides a structural framework: the pattern must be consistent with guilt and inconsistent with innocent explanation, and SEBI must have adduced sufficient evidence to make the latter improbable on a balance of probabilities.

5.2 SEBI v. Kanaiyalal Baldevbhai Patel — SAT & Supreme Court

Proceedings in this matter generated important jurisprudence on the 'use' element. The SAT held that while possession of UPSI and suspicious timing can raise an inference of insider trading, the inference is rebuttable. The accused's explanation—if credible and supported by objective evidence—must be assessed and cannot be dismissed merely because the algorithmic pattern suggests a different inference. The case also highlights that organisational or social connectivity does not, without more, establish that UPSI was communicated; the evidentiary chain must be completed through documentary evidence or communication records demonstrating actual information flow.

5.3 Patterns in SEBI Adjudication Orders

A review of published SEBI adjudication orders reveals enforcement proceedings initiated substantially on IMSS alerts, with the evidentiary foundation described in terms of statistical correlation and connectivity evidence. Adjudicating Officers have, in several cases, found pattern evidence supplemented by the accused's failure to provide a satisfactory explanation sufficient to establish liability. The SAT has occasionally intervened to set aside SEBI orders where this inferential chain was overstretched—reinforcing the principle that algorithmic pattern data cannot substitute for substantive proof of the causal element. Emerging from this case law is what may be termed the 'credible alternative hypothesis' principle: an accused defeats an inference by adducing a credible alternative explanation, which the algorithm cannot foreclose on its own.

CHAPTER 6 — RISKS OF ALGORITHMIC ENFORCEMENT

6.1 False Positives and Their Consequences

No detection algorithm is infallible. In financial market surveillance, false positives carry severe consequences: reputational damage, trading restrictions, legal costs, and the burden of disproving regulatorily presumed culpability. The statistical properties of large-scale surveillance make false positives structurally inevitable. Market surveillance algorithms rely heavily on network maps constructed from objective criteria—shared addresses, common

ISSN: 2582-6433

directorships, family relationships—that may identify connections that are real but legally irrelevant. The algorithm cannot distinguish between a connection and an active channel of UPSI transmission; only human investigation can make this distinction.

6.2 The Black Box Problem and Epistemic Opacity

SEBI has not publicly disclosed the specific parameters, detection thresholds, or weighting functions of the IMSS algorithms. This opacity creates three interrelated problems: (i) accused parties cannot meaningfully challenge the methodology that generated the alert—a fundamental violation of the right to be heard; (ii) there is no independent audit mechanism to assess whether algorithmic parameters are appropriately calibrated; and (iii) opacity prevents the development of informed judicial supervision of algorithmic enforcement practice.

6.3 Due Process and Constitutional Implications

The natural justice principles governing SEBI's quasi-judicial proceedings—audi alteram partem and nemo judex in sua causa—carry specific implications. Due process requires that the accused be provided with sufficient information about the algorithm's operation, inputs, and outputs to mount a meaningful defence. Additionally, Article 21 of the Constitution, as interpreted by the Supreme Court to protect against arbitrary state action, may be engaged where enforcement proceedings are initiated substantially on the basis of undisclosed algorithmic outputs without adequate human verification.

6.4 Chilling Effects on Legitimate Trading

Excessive reliance on algorithmic enforcement creates systemic risk to market efficiency. If sophisticated investors face investigation whenever their trades correlate with corporate announcements—even where those trades are based on legitimate research—the rational response is to alter trading behaviour to avoid triggering algorithmic alerts. This chilling effect is most acute at the boundary between 'mosaic theory' investing and insider trading, threatening to penalise legitimate analytical skill.

CHAPTER 7 — COMPARATIVE PERSPECTIVE: THE U.S. SEC MODEL

7.1 SEC's Data Analytics Infrastructure

The U.S. SEC has deployed sophisticated algorithmic detection tools—including the National Exam Analytics Tool (NEAT), the Advanced Bluesheet Analysis Program (ABSA), and the

ISSN: 2582-6433

Market Abuse Unit's (MAU) quantitative analytics platform—that conceptually parallel SEBI's IMSS. The MAU, established in 2010, employs quantitative analysts and data scientists specifically to identify suspicious trading patterns through statistical correlations between trades and corporate event announcements.

7.2 U.S. Legal Standard and Judicial Insistence on Intent

U.S. insider trading law under Section 10(b) of the Securities Exchange Act, 1934 and Rule 10b-5 requires proof of a duty-based relationship (classical, misappropriation, or tipping under Chiarella v. United States (1980) and Dirks v. SEC (1983)) and scienter—a knowing or reckless intent to trade on material, non-public information. U.S. courts have consistently held that circumstantial evidence, including trading patterns, can establish scienter, but have equally insisted that the inferential chain be tight enough to foreclose innocent explanations. No U.S. court has held that algorithmic pattern evidence alone is sufficient to establish insider trading liability.

7.3 SEC Enforcement Practice: Detection vs. Proof

SEC enforcement actions typically involve algorithmic pattern evidence supplemented by extensive human investigation—communication records, email forensics, phone records, witness testimony, and documentary evidence of information flow. The algorithm identifies; human investigation constructs the case. The distinction between detection and proof is institutionally embedded in SEC methodology. The SEC has also disclosed the methodological basis of statistical analyses presented as evidence, enabling accused parties to challenge reliability—a transparency practice Indian regulatory enforcement would benefit from adopting.

7.4 Lessons for India

The U.S. model offers three key lessons: (i) institutional separation between the surveillance function and the enforcement function reduces anchoring bias; (ii) transparency requirements for statistical methodologies ensure meaningful challenge rights; and (iii) consistent judicial insistence on proof of scienter provides a principled doctrinal limit on pattern evidence sufficiency. These lessons, appropriately adapted to India's legal and institutional context, inform the reform proposals below.

ISSN: 2582-6433

CHAPTER 8 — SUGGESTIONS AND REFORM AGENDA

8.1 The Hybrid Evidentiary Model

The most important structural reform is the formal adoption of a hybrid evidentiary model that institutionally separates the detection function from the proof function. Algorithmic outputs should serve as structured detection triggers—necessary but not sufficient for initiating formal enforcement proceedings. A mandatory human investigation phase, with defined minimum evidentiary standards, should be required before a show-cause notice is issued. This model already exists in embryonic form in SEBI's stated protocol; the reform proposal is to formalise, standardise, and make it externally auditable.

8.2 Transparency and Algorithmic Disclosure Standards

SEBI should publish regulatory standards governing the disclosure of algorithmic methodologies in enforcement proceedings. At minimum, accused persons should receive a written description of: the algorithmic parameters that generated the alert, the specific statistical thresholds applied, and the precise basis on which their trading was flagged. SEBI should also commission and publish independent audits of IMSS false positive and false negative rates. An independent technical advisory committee—with legal, technical, and market professional representation—should provide ongoing oversight of surveillance methodologies.

8.3 Legislative Amendments to the PIT Regulations

The PIT Regulations, 2015 should be amended to insert a provision clarifying that algorithmic pattern evidence is admissible but does not, without more, give rise to a presumption of insider trading. Pattern evidence must be supplemented by: (i) evidence of actual UPSI possession; (ii) a plausible information channel; and (iii) the absence of a credible innocent explanation. A minimum evidence disclosure requirement should also be codified, giving legislative backing to the transparency recommendations above.

8.4 Safe Harbour for Research-Based Trading

SEBI should develop a structured safe harbour for trades demonstrably based on legitimate research. This could take the form of a voluntary pre-trade research documentation mechanism, under which institutional investors record the analytical basis for significant position changes in a timestamped repository. In the event of a subsequent IMSS alert, SEBI investigators would be required to examine the documented research basis before proceeding. This would reduce

ISSN: 2582-6433

chilling effects, provide a strong rebuttal in clear cases, and create positive incentives for maintaining robust investment research documentation.

8.5 Judicial Guidance on Evidentiary Standards

The SAT and higher courts should, in appropriate cases, issue guidance on the evidentiary treatment of algorithmic outputs in insider trading proceedings, addressing: minimum evidentiary requirements for pattern-based proof; the accused's right to disclosure of surveillance methodologies; and the relationship between algorithmic evidence and the standard of proof. A formal Practice Direction from the SAT, or an advisory from SEBI, could provide doctrinal clarity currently lacking in this area.

CHAPTER 9 — CONCLUSION

This paper has examined the fundamental tension between SEBI's algorithmic surveillance capabilities and the legal requirements for proving insider trading liability under Indian securities law. The analysis demonstrates that this tension is not merely technical but structural: it arises from the inherent limitation of computational pattern recognition when applied to a legal framework built around individual intent, causal proof, and due process.

Algorithmic surveillance, as embodied in the IMSS and associated analytical tools, is indispensable. Without it, a significant proportion of insider trading would escape detection entirely. The argument is about scope and limits—what algorithmic evidence can establish, what it cannot, and what procedural safeguards must accompany its use. The PIT Regulations require proof that an insider traded 'on the basis of' UPSI. Algorithms detect correlation; they cannot establish causation. They identify suspicious timing; they cannot prove mental state. They map connectivity; they cannot demonstrate information flow. Each gap must be filled by human investigation, documentary evidence, and legally adequate inferential reasoning.

The risks of ignoring these limits are real: false positives destroy reputations, opacity undermines natural justice, anchoring bias compromises enforcement quality, and chilling effects damage the very market efficiency that insider trading regulation is designed to protect.

The reform agenda proposed—a hybrid evidentiary model, transparency standards for algorithmic disclosures, legislative amendments to the PIT Regulations, safe harbours for research-based trading, and judicial guidance—addresses these risks without sacrificing detection benefits.

The thesis advanced at the outset has been validated: while algorithmic surveillance enhances

ISSN: 2582-6433

detection efficiency, it is insufficient as standalone proof under the current Indian insider trading framework, which fundamentally requires human intent and a demonstrable connection to UPSI. Indian law must evolve to formally address the evidentiary status of data-driven inference—but that evolution must be guided by, not a departure from, the foundational principles of due process, burden of proof, and individual accountability that give insider trading regulation its legitimacy. The challenge is not to slow the march of technology in regulatory enforcement, but to ensure that law keeps pace with it—not by lowering the evidentiary bar, but by building the procedural infrastructure that allows algorithmic capabilities to be deployed consistently with justice.

BIBLIOGRAPHY

Statutes and Regulations

- Securities and Exchange Board of India Act, 1992
- SEBI (Prohibition of Insider Trading) Regulations, 2015 (as amended 2018, 2019)
- SEBI (Procedure for Holding Inquiry and Imposing Penalties) Rules, 1995
- Indian Evidence Act, 1872 | Information Technology Act, 2000
- Constitution of India, 1950 (Articles 14, 21)
- Securities Exchange Act, 1934 (U.S.) § 10(b); Rule 10b-5 | Insider Trading Sanctions Act, 1984 (U.S.)

Cases

- SEBI v. Rakhi Trading Pvt. Ltd., (2018) 13 SCC 678 (Supreme Court of India)
- SEBI v. Kanaiyalal Baldevbhai Patel, Civil Appeal No. 1303 of 2006 (Supreme Court of India)
- Chiarella v. United States, 445 U.S. 222 (1980)
- Dirks v. SEC, 463 U.S. 646 (1983)
- United States v. O'Hagan, 521 U.S. 642 (1997)

Committee Reports and Regulatory Documents

- T.K. Viswanathan Committee Report on Insider Trading Regulations, 2015
- J.R. Varma Committee Report on Insider Trading, 1998
- SEBI Annual Reports 2018–2024 | SEBI Consultation Paper on Algorithmic Trading Regulations, 2016

ISSN: 2582-6433

- SEC, 'Algorithmic Trading: A Primer' (Office of Compliance Inspections and Examinations, 2019)

Books and Articles

- Taxmann's Guide to SEBI (Prohibition of Insider Trading) Regulations, 2015 (Latest Edition)
- M.R. Mallya, SEBI: Law and Practice (LexisNexis)
- Donald Langevoort, 'Insider Trading Regulation, Enforcement, and Prevention' (Thomson Reuters)
- Frank Pasquale, 'The Black Box Society' (Harvard University Press, 2016)
- Yesha Yadav, 'Insider Trading and Market Structure', UCLA Law Review (2016)
- Rajesh Chakrabarti, 'Insider Trading Law in India: A Critical Assessment', Indian Law Review (2017)