Page: 2131-2145 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.94

SEBI AND DATA GOVERNANCE: EXAMINING JURISDICTIONAL OVERLAPS UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION FRAMEWORK

Rethiga Ramesh[1]

I. ABSTRACT

The role of financial market authorities has changed due to the growing datafication of securities market. The securities exchange board of India (SEBI) in India now heavily depends on the mandatory know your customer (KYC) regulations, centralized registries, transaction level surveillance, algorithmic trading oversights, and digital grievance redressal system, all of which entail the large-scale collection, processing, sharing, and retention of transactional and personal data. While these practices are justified in the interests of market integrity and investor protection, they raise significant legal questions in the context of the DPDPA, which establishes a comprehensive framework for personal data protection grounded in consent, purpose limitation, data minimization, the accountability. This article addresses whether SEBI's data intensive regulatory framework effectively positions it as a de facto data regulator, given the absence of any explicit legislation stating the same. In addition to the DPDPA and the constitutional privacy jurisprudence under justice case K.S.Puttaswamy vs union of India, this article examines SEBI rules, circulars, and surveillance in systems using a doctrinal and analytical methodology. It illustrates how SEBI has functional authority over the data life cycle insecurities markets, leading to jurisdiction overlap and conflicts between data protection law and security regulation. This article makes the case that the DPDPA assumes regulatory coexistence without offering clear institutional hierarchy or conflict resolution procedures, therefore failing to effectively handle the function of sectoral regulators. This regulatory silence risks diluting investor privacy protection, increasing compliance uncertainty for intermediaries, and undermining constitutional requirements of proportionality and democratic accountability. This article suggests a harmonized

[1] Student, LLM in Business Law, Tamil Nadu Dr. Ambedkar Law University, School of Excellence in Law, Tamil Nadu, Chennai (India). Email: rethigaramesh@gmail.com

regulatory structure that acknowledges SEBI functional data governance role while incorporating strong data privacy protections, drawing on limited comparative observations from the US and the UK. It concludes that an order to meet in both market integrity and constitutional legitimacy in India's data driven financial ecosystem, it is imperative to explain the interaction between securities regulation and data privacy laws.

II. KEYWORDS

Securities and Exchange Board of India (SEBI), Digital Personal Data Protection Act, 2023, Financial Market Regulation, Data Governance, Sectoral Regulators.

III. INTRODUCTION

Globally, capital markets on a heavily depend on data. Today, security is regulation depending more and more on continuous data flows, real time monitoring, and predictive analytics rather than just disclosure standards and post fact enforcement. This trend is especially apparent in the SEBI regulatory procedures in India. Investors and intermediaries financial, transactional, and personal data are now gathered, stored, and processed extensively to get in the market integrity.

Know your customer standards, centralized KYC registries, trade level monitoring, algorithmic trading supervision, and digital grievance redressal mechanism are all examples of how SEBI regulatory framework has progressively grown. These actions put SEBI at the center of India's financial data eco system, even though they are justified in the name of market efficiency and investor safety. SEBI exercises significant control over the gathering storing and sharing of application of invested data and its securities market.

Simultaneously, India has passed the DPDPA 2023, which creates a thorough framework for protecting personal information based on the concept of accountability, consent, purpose limitation, and data minimization. The central challenge arises from the coexistence of the DPDP Act with SEBI's data intensive regulatory framework: does SEBI's functional control over investor data amount to de facto regulation, and if so, how does this interact with India's formal data protection regime?

This article argues that SEBI carries out a number of tasks typically of a data regulator even though it does not legally recognize as the data protection body. Privacy of distinct jurisdiction boundaries between the data protection legislation and security regulation raises constitutional questions about accountability and proportionality, increases complaints uncertainty, and puts privacy rights at risk. In order to harmony SEBI is Market mandate with India's data protection duties, this article looks at this legislative overlap, identifies the consequent conflicts, and suggest a framework.[2]

A. Research Problem

While data protection law in India is formally governed by DPDPA, sectoral regulators, especially the securities and exchange board of India, have considerable control over transactional and personal data through mandatory data sharing requirements, surveillance methods, and KYC standards. Because there are no distinct jurisdictional borders between market regulation and data protection legislation, this results in regulatory blind hole.

B. Research Objectives

The objectives of this article are:

1. To examine whether SEBI's data intensive regulatory framework effectively positions it as a de facto data regulator within the securities market.
2. To analyse the interaction and potential conflicts between SEBI's regulatory practices and the Digital Personal Data Protection Act, 2023.
3. To evaluate the constitutional implications of such overlap, particularly in relation to the right to privacy and the principles of necessity and proportionality.
4. To identify gaps in the existing legal framework governing sectoral regulators and data protection authorities.

[2] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 19–22 (Harvard Univ. Press 2015).

C. Research Questions

The article is guided by the following research questions:

1. Does SEBI's regulatory structure effectively render it a de facto data regulator within the securities market?
2. To what extent do SEBI's data governance practices conflict with the Digital Personal Data Protection Act, 2023?
3. What constitutional concerns arise from the overlap between securities regulation and data protection law, particularly in relation to privacy and proportionality?
4. How can regulatory coordination be structured to resolve jurisdictional conflicts while preserving both market integrity and data protection standards?

D. Research Gap

By analyzing SEBI's changing function as a de facto regulator in the post DPDP act landscape, this research aims to fill a substantial gap in Indian regulatory literature. Although the existing literature treats securities regulation and data protection as separate fields, this article demonstrates how SEBI's data intensive regulatory techniques result in jurisdictional overlaps that are yet unsettled legally. By evaluating SEBI's monitoring infrastructure through the length of data protection principles unconstitutional proportionality, the article presents a unique methodology for harmonizing market regulation with investor privacy:

1. SEBI is not studied as a data regulator.
2. No post DPDPA analysis
3. Assume regulatory harmony and missing constitutional analysis.

This article tries to bridge three silos.

E. Research Methodology

This article adopts a doctrinal analytical methodology, examining surveillance framework, SEBIs rules, circular, along with the DPDPA 2023 and constitutional privacy jurisprudence. Comparative references to EU and UK regulatory coordination are used illustratively to examine institutional architecture.

Although this article does not adopt an empirical methodology, it relies on institutional evidence in the form of binding SEBI circulars, surveillance mandates, compliance obligations imposed on intermediaries, and statutory data retention requirements. These instruments provide verifiable evidence of SEBI's functional control over the data lifecycle in securities markets. For the purposes of constitutional and regulatory analysis, such institutional practices constitute sufficient proof of regulatory power, making empirical validation unnecessary.

IV. CONCEPTUALIZING SEBI'S DATA CONTROL

SEBI's power to overseas securities l market comes from the law that created it and other official documents like regulation circulars and guidelines. Although these documents don't directly give SEBI control over data, we require a lot of data related actions which influence how personal and financial information is handled by SEBI in the market.

A. KYC and CKYC Norms

KYC norms serve as a foundation of the SEBI system by identifying investors. Entities like brokers, mutual funds, and depositories must gather comprehensive person information such as identity documents, proof of address, bank details, and tax identifiers[3]. The central KYC system consolidates its data, allowing it to be reused verified across financial institutions.

From the standpoint of data governance, KYC regulation defines the type of data collected, the reason for collecting it, and the duration it is kept. Investors have limited options in this process since following these rules is necessary to take part in the market.

[3] Securities & Exch. Bd. of India, *Know Your Customer (KYC) Registration Agency Regulations*, No. LAD-NRO/GN/2011-12/24/18333 (Aug. 23, 2011) (India).

While the aim is to stop fraud and money laundering, the way the regulations' structure gives SEBI the ability to control how much personal data is gathered in the securities market.

B. Transaction level surveillance

SEBI uses advanced monitoring tools to track market activities at the level of individual transactions. Each trade conducted on the stock exchange is documented, examined, and kept for the purpose of identifying inside a trading, market manipulation, and potential risks to the system. This monitoring process includes ongoing analysis of how investors behave, the patterns of the trades, and their financial backgrounds.

This type of detailed transaction tracking goes beyond standard regulatory checks and the similar to large scale analysis of how people behave financially. The data collected is not only used to take action against violation but also to forecast potential issues in access risks. In practice, SEBI sets out the reason for using transaction data and how long it should be kept, which art key aspects of managing data properly[4].

C. Algorithmic Trading Data

The increasing use of algorithmic and high frequency trading has led to a greater focus on data by SEBI[5]. Using algorithms must provide information about the technical setup, trading strategies, and system designs. SEBI and stock exchange perform regular audits, stress tests, and continuous monitoring of these algorithmic systems.

The data involved in algorithmic trading is very sensitive, often containing exclusive strategies and real time market information. SEBI's supervision of this data shows the regulators growing power and handling complex state environments where market regulation and data management overlap.

D. Investor Grievance Databases

[4] Securities & Exch. Bd. of India, *Integrated Market Surveillance System*, Circular No. MRD/DoP/SE/Cir-28/2008 (Dec. 15, 2008) (India).
[5] Securities & Exch. Bd. of India, *Framework for Algorithmic Trading*, Circular No. CIR/MRD/DP/09/2012 (Mar. 30, 2012) (India).

SEBI's process for handling complaints depends on the digital platform that he complains about, supporting documents, and personal messages between investors and intermediaries.[6] These platforms store sensitive personal and financial details, and information is kept for a long time.

By creating and requiring the use of these platforms, how complaint related data is gathered, accessed and stored. This supports the idea that SEBI has control over data, even if it is not officially recognized by law. These actions show that SEBI's rules play a vital role in managing data effectively. Even though there is no specific legal framework for this, it is clear SEBI influences how data is handled in the securities market.

E. Disclosure and Insider Trading Data Governance

SEBI's data governance role is further evident in its administration of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 and the SEBI (Prohibition of Insider Trading) Regulations, 2015. Under the LODR Regulations, listed entities are required to make continuous disclosures relating to financial performance, material events, corporate governance practices, and shareholding patterns. These obligations generate extensive flows of structured and periodic data, which are standardized, monitored, and enforced by SEBI, thereby placing the regulator at the center of corporate data dissemination and market transparency.

Similarly, the Insider Trading Regulations impose strict controls over the handling of unpublished price sensitive information. Entities are required to establish structured digital databases, maintain audit trails of information sharing, implement internal codes of conduct, and restrict access to sensitive data through information barriers. SEBI's oversight of these mechanisms includes surveillance of trading patterns, enforcement of disclosure norms, and investigation of data misuse.

[6] Securities & Exch. Bd. of India, *SEBI Complaints Redress System (SCORES)*, Circular No. CIR/OIAE/2/2011 (June 3, 2011) (India).

From a data governance perspective, these frameworks go beyond conventional financial regulation by prescribing how data is generated, accessed, shared, and retained within market institutions. This further strengthens the argument that SEBI exercises functional control over critical aspects of the data lifecycle, in a manner analogous to a sector specific data regulator.

V. DPDP ACT, 2023 AND DPDP RULES, 2025 AND SECTORAL REGULATORS

The Digital Personal Data Protection Act, 2023, read together with the Digital Personal Data Protection Rules, 2025, constitutes India's primary legal framework for the protection of personal data. The Rules, notified by the Ministry of Electronics and Information Technology, operationalize the Act through a phased implementation structure, including the establishment of the Data Protection Board of India, the regulation of consent managers, and the gradual enforcement of compliance obligations. This framework seeks to balance individual privacy with lawful data processing, while introducing institutional mechanisms for enforcement and oversight.

A. Scope and Objectives of the DPDP Act

The Digital Data Protection Act covers the processing of digital personal data and is based on principles like lawful purpose, consent, data minimization, accuracy, limited storage and accountability.[7] The act also allows data processing without consent in exceptional cases, such as when complying with legal requirements. While the Act provides for certain exemptions, the Rules introduce procedural clarity in areas such as consent architecture, data fiduciary obligations, and security safeguards. However, they do not comprehensively resolve how sector specific regulatory mandates, such as those imposed by SEBI, are to be reconciled with core data protection principles.

B. Sectoral Regulators and Regulatory Ambiguity

[7] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–8 (India).

The DPDPA framework, as supplemented by the Rules, formally establishes the Data Protection Board of India as the primary enforcement authority. While this development addresses earlier concerns regarding institutional absence, the framework still does not clearly define the interaction between the Board and sectoral regulators. It assumes regulatory coexistence without establishing a clear hierarchy or conflict resolution mechanism between authorities such as SEBI and the data protection regime. This lack of clarity causes confusion when sectoral rules require data practices that might go against data protection principles. For example, in the case of SEBI, intermediaries are required to handle personal data under securities laws, even if this may contradict the principles of purpose limitation or data minimization.

C. Absence of Regulatory Precedence

Although the Rules introduce phased compliance timelines, which provide transitional clarity for regulated entities, they do not eliminate overlapping obligations. SEBI regulated intermediaries must now align their existing data intensive practices with evolving data protection requirements across different implementation phases. This layered compliance structure may continue to generate legal uncertainty and increase the cost of regulatory adherence.

VI. JURISDICTIONAL OVERLAP AND COMPLIANCE CONFLICTS

The combination of SEBI's regulatory responsibilities and the DPDP Act leads to real compliance challenges, which are central to the argument in this article.

1. **Consent versus Regulatory Compulsion:** Data protection laws emphasize consent as the foundation for legal data processing. On the other hand, SEBI's regulatory structure mainly depends on mandatory data collection. Investors cannot reasonably refuse to have their data collected without being barred from participating in the market. Although the DPDP Act permits data processing to meet legal requirements, the wide scope of SEBI's data demands raises concerns about whether consent is being replaced rather than supported.

2. **Purpose Limitation vs Open Ended Surveillance:** Purpose limitation requires that data be used only for specific and legitimate reasons. However, SEBI's surveillance tools often involve broad purposes, such as maintaining market integrity, managing risks, and preparing for future enforcement. This ongoing and flexible use of data makes it difficult to establish clear purpose boundaries, which undermines a key data protection principle.
3. **Data Minimization versus Market-Wide Retention:** SEBI's approach focuses on keeping comprehensive data to support detailed past analysis. This contrasts with the data minimization principle, which requires collecting and keeping only the data that is essential. The lack of clear guidelines on how long data should be kept or when it should be deleted intensifies this conflict.

VII. CONSTITUTIONAL AND JURISPRUDENTIAL CONCERNS

The overlapping roles of SEBI and data protection framework should also be considered from the constitutional perspective.

1. **Right to Privacy:** The right to privacy, as established by the supreme court of India, includes the production of personal information and the ability to control once own personal data.[8] Any action that affects this right must be lawful, necessary, and proportionate. SEBI's regulations involving large amounts of data meet the legal requirements through delegated legislation. However, the necessity and proportionality of some data practices have not been thoroughly examined.
2. **Proportionality and Necessity:** Proportionality demands a logical connection between the regulatory goals and the methods used to achieve them. Without regular reviews of specific safeguards, SEBI's data practices could fail the test for proportionality.
3. **Democratic Accountability:** SEBI exercises significant control over data, mainly through subordinate legislation rather than through laws passed by the

[8] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

parliament. This raises serious concerns about democratic supervision and the legitimacy of regulatory actions, especially when fundamental rights are at stake.

VIII. COMPARATIVE PERSPECTIVES

A limited comparison indicates that the challenge of balancing financial regulation with data protection is not unique to India; however, unlike the Indian data protection framework, more developed legal systems have established institutional mechanisms to handle overlapping regulatory responsibilities while maintaining both market stability and individual privacy rights.

In the United Kingdom, oversight of financial markets and data protection operates within a well-structured system of regulatory cooperation. The Financial Conduct Authority (FCA) has broad authority over data related activities, including transaction reporting, market monitoring, oversight of algorithmic trading, and handling of investor complaints. At the same time, the Information Commissioner's Office is responsible for enforcement and data protection laws under the UKG DPR. And the UK system does not depend on regulators moving silently. Sector specific regulators are considered laughing data processes under the law, but they are still subject to principles its proportionality, necessity, and accountability, which are enforced by the information commissioner's office to guidance and collaborative oversite.

The United States employees a more fragmented it functionally limited method for regulating financial markets. The primary responsibility for monitoring these markets lies with a securities exchange commission, which requires detailed data disclosures is reporting at the transaction level. While the United States does not have a single overarching federal data protection law, the Securities and Exchange Commission operates within a sector specific framework governed by instruments such as the Privacy Act of 1974 and Regulation S P under the Gramm Leach Bliley Act, which impose obligations relating to the protection and confidentiality of customer information. These practices are further shaped by administrative law principles and are subject to judicial

oversight by federal courts. Quotes of as external checks by reviewing the data collection activities of regulates events are they are not arbitrary or excessive.

These approaches offer 3 key insights for India:

1. Financial regulators naturally half control over data, the absence of coordination between the regulators creates uncertainty for compliance, and constitutional account ability depends on either an independent privacy watchdog or pure legal guidance.
2. In contrast, India's DPDP assumes that different regulatory bodies can operate together without defining their roles of how conflict will be resolved. This resulted in SEBI data heavy regulation being in a legal grey area under the constitution. This comparison highlights the necessity of a unified regulatory system, rather than simply designing SEBI as sole data protection authority.
3. Rather than treating foreign jurisdictions as transplantable models, this article uses comparative regulatory design to extract structural principles relevant to India. The UK and US experiences demonstrate that large-scale financial data governance is constitutionally legitimate only when accompanied by either (a) an independent privacy oversight authority with supervisory competence over sectoral regulators, or (b) explicit statutory constraints coupled with robust judicial review. The absence of both mechanisms in the Indian framework renders SEBI's data-intensive regulation uniquely vulnerable to constitutional challenge.

IX. TOWARDS A COORDINATED REGULATORY RESOLUTION FRAMEWORK

This article does not argue for the subordination of securities regulation to data protection law, nor for the elevation of SEBI as a parallel data protection authority. In light of the Digital Personal Data Protection Rules, 2025, which establish the Data Protection Board of India and introduce phased compliance obligations, the need for coordinated regulatory interaction becomes more pronounced. First, sectoral regulators such as SEBI

should be statutorily recognized as data fiduciaries for limited regulatory purposes, subject to data protection principles of necessity and proportionality as clarified under the 2025 Rules. Second, the Data Protection Board of India should exercise supervisory competence to review sectoral data practices that materially affect fundamental rights, while respecting the functional autonomy of financial regulators. Third, structured coordination mechanisms, including formal consultation processes and joint regulatory guidance, should be institutionalized to address interpretive conflicts between SEBI obligations and phased data protection compliance requirements. Such a framework aligns the operational realities introduced by the Rules with the need for constitutional accountability and regulatory clarity.

1. The article shows that even though the securities exchange board of India is not officially recognised as a data protection authority by law, its wide-ranging regulatory actions make it act like one in practice, when it comes to managing investors and regulating market data.
2. This analysis shows that DPDPA 2023 does not clearly define the role of sectors specific regulators, leading to tussle and unclear overlaps India authority and challenges in meeting both securities in data protection rules.
3. SEBI's regulatory system, which handles large amounts of data and also deals with activities like monitoring, keeping records, and recording disclosures, brings up important concerns about consent, limiting data used to specific purposes, and collecting only necessary data, all of which are key aspects of data protection.
4. From a constitutional perspective, the lack of clear legal boundaries and oversight of SEBI data management powers could affect the fairness, privacy and accountability of the regulatory system.
5. With respect to the other regulatory models around The World shows the cooperation between the financial regulator and the data protection bodies is not

only possible but also required to keep the financial market honest while protecting the individual privacy.

6. The article concludes that without proper coordination and agreement between different regulatory bodies, SEBI growing control over data mid damage public confidence and the overall effectiveness of its regulation, even though its goals are to ensure a stable and safe market environment for investors.
7. A balanced system that acknowledges SEBI's important role in managing data while also ensuring the data protection measures or increases vital for a lining securities regulation with the growing data protection laws in India.

X. CONCLUSION

SEBI may not be officially recognized as a data regulator, but it operates as one in practice. It has broad, ongoing control over invested data which is crucial for modern security regulation. However, this practice role creates a conflict with India's developing data protection laws which do not have clear ways to handle overlapping areas of authority. If this issue is not resolved, it could harm the investor privacy, make compliance more difficult, and reduce accountability. Balance approach that acknowledges is SEBI's effective role and data governance, which also includes strong data protection measures, is necessary to maintain market and legal authority.

XI. BIBLIOGRAPHY

A. Primary Sources

1. Digital Personal Data Protection Act, 2023.
2. Digital Personal Data Protection Rules, 2025.
3. Securities and Exchange Board of India Act, 1992.
4. Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.
5. Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015.

6. Information Technology Act, 2000.
7. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
8. Justice K.S. Puttaswamy (Retd.) v Union of India, Writ Petition (Civil) No 494 of 2012 (Supreme Court of India, 24 August 2017).

B. Secondary Sources

1. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
2. Julia Black, Decentering Regulation: Understanding the Role of Regulation and Self-Regulation in a Post Regulatory World' (2001) 54 Current Legal Problems 103.
3. Roger Brownsword, Regulatory Theory, Technology, and the Rule of Law' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press 2017).
4. European Union General Data Protection Regulation (Regulation (EU) 2016/679).