The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

ROLE OF SEBI AND DPDP ACT IN TRADING SECTOR

Lovisha Prajapati

Introduction

In India, the digitally driven financial environment is growing gradually, making individuals adopt modern "tech-driven" financial investment options instead of traditional investment options. It leaves the personal data of individuals at the mercy of the 'Data Fiduciary', who determines the purpose and means of processing the personal data of the 'Data Principal'. Therefore, to safeguard the interests of all the stakeholders, the Central government has enacted the 'Digital Personal Data Protection Act, 2023'.

"Law and technology must evolve together to protect fundamental rights in the digital era."

— Justice B.N. Srikrishna, Chairperson of the Committee on Data Protection in India

Data, often referred to as **"new oil",** characteristically has three main components: Non rivalrous, infinite, and the centre of modern economics. The processing power of data defines competitive advantage, driving both corporate strategy and global geopolitical influence.

In an increasingly digitalised economy, data has emerged as a crucial asset, especially in the trading sector, where real-time access to financial data, personal identifiers, and transactional information drives market decisions. As India modernises its data governance landscape, the ***Digital Personal Data Protection (DPDP) Act, 2023,*** **and the** ***Securities and Exchange Board of India (SEBI)*** have become key regulatory players. Together, they shape how data flows within and beyond India's borders, raising both compliance challenges and global friction.

This plight poses a question: ***Does access to data flow within the trading sector jeopardise the right to privacy?***

This article looks into the convergence of the DPDP Act and SEBI's regulatory ambit in the trading area. It discusses, thereby, how the newly introduced data protection law may alter the regulatory landscape of SEBI, the definition of intermediary functions, and legal methods of data governance in the capital markets of India, and the clash between the right to privacy and the legal bandwidth of the DPDP Act and SEBI.

SEBI & Its Role in Data Governance

The Securities and Exchange Board of India (SEBI) was established in 1988 through a resolution of the Government of India. Later, in 1992, it was accorded statutory status through the SEBI Act of 1992. The main aim of creating SEBI was to safeguard investors' interests in securities and to encourage the growth and regulation of the securities market via a strong data governance framework. SEBI ensures that information pertaining to financial markets is accurate, transparent, secure, and reasonably accessible through its data governance standards**.**

To effectively govern data, SEBI mandates that exchanges, brokers, and intermediaries gather, retain, and frequently share sensitive information, including KYC details, financial data, and occasionally trading patterns, within the trading ecosystem. This regulatory process fosters confidence and responsibility while advancing rigorous cybersecurity and data management standards. SEBI employs real-time data monitoring systems to identify fraud, insider trading, dabba trading, price manipulation, and different systemic risks.

SEBI guarantees that different credit rating agencies like CRISIL, ICRA, Brickworks Ratings, and CARE deliver trustworthy and impartial information. Data-driven complaint resolution systems such as SCORES (SEBI Complaints Redress System) are utilized to monitor grievances and safeguard the interests of investors. SEBI also enforces rules that promote the retention of essential financial information within India's geographical boundaries to ensure regulatory supervision.

SEBI has recently launched its 'Data Lake and Analytics Platform' that could process a large amount of structured and unstructured data with a view to enhance monitoring and surveillance mechanism. SEBI's 'Data Governance Framework (2023-24)' designates norms for regulation of Financial Benchmarks and Data Repositories focusing on data accuracy, elaborate audit trails, and strengthening accountability. Brokers are required to create an institutional deterrent mechanism to prevent and detect fraud or market abuse under the Chapter IVA of the Securities and Exchange Board of India (Stock Brokers) (Amendment) Regulations, 2024

The broker's Industry Standards Forum (ISF), in consultation with SEBI, will develop the standards for implementation of the same, including operational modalities.

DPDP Act: Reinventing Privacy in India

The ***Digital Personal Data Protection Act, 2023 (DPDP)*** is India's first overarching Personal data protection law which enshrines rights of 'data principals' regarding their data, obligations of 'data fiduciaries' and mandates for data minimization and purpose limitation. This is particularly challenging for the trading industry, as intermediaries now have to seek prior consent, legitimate the purposes of data collection and limit sharing, especially in the context of algorithmic electronic trading, client profiling and international outsourcing of financial services.

The act is modelled in the inspiration of the worlds' legal systems such as the ***EU General Data Protection Regulations (GDPR)*** regarding the articulation of Privacy and Data protection obligations being brought in six years post the ***KS Puttaswamy 2017*** judgement of the Supreme Court where it was upheld that a fundamental right of privacy is a part of **Article 21.**

Furthermore, ***B.N Saikrishna Committee*** strangle recommended for the stringer privacy laws in India, including **data processing restrictions**, a **Data Protection Authority**, the **right to be forgotten**, and **data localization.**

Data Principals (individuals whose personal data is being processed) shall have the right to access information, request modification or correction, request grievance redressal, and nominate a representative in case of death or incapacity.

The **Data Fiduciaries** (the entity or organization that collects, stores, processes, or uses personal data of an individual) must ensure the accuracy of data, implement security measures to prevent

a breach, and notify the DPBI (Data Protection Board of India) and affected individuals if a breach occurs. They must also delete the data once the purpose for which it was used has been fulfilled and the retention of the same is no longer justified legally.

The concept of **Significant Data Fiduciary (SDF),** one of the key innovations of the act enables those designated as SDFs shall meet the enhanced compliance requirements, reflecting the higher risk of the data processing activities that might pose to either individual or national interests.

The **section 10 of DPDP act**, empowers the Central Government to classify a data fiduciary based on nuanced risk assessment.

Global Privacy Standards: a Clash of Interests?

The Modern day trade heavily relies on the cross border data flow which is one of the most crucial aspect in underscoring the importance of the data handling and the privacy norms, thus creating " privacy-trade dilemma".

The challenges related to data collection, use, and recycling in the field of privacy have rendered data protection the entry of legislators, leading to various enactments on data protection laws such as the **EU's GDPR and India's DPDPA**. But, protection of data with privacy spells a price for all nations. GATS is the first step towards solving the problem.

GATS asks WTO members to provide national treatment for foreign service providers in certain selected services since it extends international trade regulation to services. The privacy provisions in GATS are fundamental in setting how countries address the privacy-trade conflict; thus, their analysis is of utmost importance.

GATS instituted a Privacy Framework with some exceptions enumerated under Article XIV. The Convention thus empowers member states to take certain actions that from the standpoint of the treaty are forbidden, so long as such actions satisfy certain conditions of protecting public order, safeguarding human health, and preventing deceptive practices. One of the most prominent exceptions is given by **Article XIV(c)(ii),** which provides that the Agreement shall not prevent the member states from adopting measures necessary to secure compliance with laws relating to protection of the privacy of individuals in respect of the processing and dissemination of personal data.

Hence, GATS does not just institute a privacy provision; instead, it limits the application of that provision. Like all other exceptions, **Article XIV** was codified to prevent possible abuse of exceptions. **Article IV** further confirms that such measures should not imply arbitrary or unjustifiable discrimination.

In China, the **Data Security Law (DSL)** requires the categorization of business data by risk and creates new limitations on cross-border data transfers. The **Personal Information Protection Law (PIPL)** gives Chinese data principals additional rights to prevent the unauthorized use of personal data.

The **United States** does not have a general privacy law like the GDPR in Europe, but instead has laws that are sector-specific instead. Government use of data is subject to top-level laws, like the Privacy Act. The private sector is subject to some limited laws that are sector-specific.

The New Era of Algorithmic Trading

High-Frequency Trading (HFT) and Algorithmic Trading have significantly transformed how securities are bought and sold in the current trading landscape. These systems, which demand operational and algorithmic automation, enable traders to execute large volumes of orders in under a second. HFT and Algorithmic Trading significantly boost and highlight the critical role of speed in the investment environment by eliminating human mistakes, augmenting market liquidity, and improving pricing efficiency. As reported by **SEBI (2023),** algorithmic strategies, or algo, make up around **60%** of the overall trading volume in the **National Stock Exchange (NSE),** with a significant portion consisting of **High Frequency Trading (HFT**).

While these developments bring technological and economic benefits, they also raise legitimate concerns about data privacy and market fairness. Algorithmic trading platforms are dependent on real-time personal and behavioural data on its customers with respect to their trading preferences, trading frequency, portfolio sizes, trading algorithms, and, in some cases, biometric identifiers for access to wallets (i.e., fingerprint or facial recognition). After the algo and HFT platforms process the data - especially in real time when AI-based decision-making tools are used, and across country boundaries - that data can be used, profiled, and disclosed without consent if there are not sufficient data protection measures in place.

Globally, HFT raises concerns. The **U.S. Securities and Exchange Commission (SEC)** articulated concerns on the risks of front-running and data loss due to co-location aka HFT firms put their servers right beside the stock exchange data centres, so they can access data microseconds before other traders. Similarly, the **European Securities and Markets Authority (ESMA)** as required by MiFID II will do audits, assess risk, and provide transparency to fashion regulations to doesn't advantage or unfairly access, or use data.

SEBI was trying to regulate this field with distinct client codes, pre-trade risk management, and requiring audit trails to be implemented for algorithmic orders. There still is a gap in privacy as traders often do not know how data is collected, profiled, and if/or how their data is used in algorithms. Further, **Foreign Institutional Investors (FIIs)** using a HFT strategy could face additional barriers that may arise from India's changing stance on cross-border data localization and issues around the free-flow of data and how that may impact its ability to bring in capital.

Trading Sector Challenges

The instantaneous aspect of HFT depends on obtaining large quantities of user data—ranging from behavioral patterns and risk attitudes to demographic information. Numerous AI tools currently analyze retail traders to enhance trade outcomes or forecast price shifts. According to the DPDP Act, this type of profiling could now necessitate:

i. Clear permission from individuals.

ii. Concise explanation of the intent behind data processing.

iii. Steps to prevent automated decision-making lacking human supervision (a principle endorsed by EU GDPR but still unclear under DPDP).

This puts brokers in a pivotal position—navigating SEBI’s requirement for comprehensive trade monitoring and openness alongside the DPDP’s focus on privacy.

Furthermore, traders and brokers face the challenge of adapting to swiftly evolving compliance environments while maintaining seamless platform functionality and user contentment.

Incorporating data protection measures without interrupting real-time trading processes demands significant investment in cybersecurity systems and human supervision. Smaller companies, especially, might find it difficult to cope with increasing compliance expenses, legal ambiguities concerning cross-border activities, and possible service interruptions if a foreign technology provider is limited by DPDP's cross-border regulations. These challenges generate a complicated operational landscape that requires both legal insight and technological flexibility.

Conclusion

With the growth of India's fintech landscape, achieving the proper equilibrium between innovation and regulation becomes ever more essential. Although High-Frequency Trading and algorithmic systems have opened up new efficiencies in the securities market, their dependence on sensitive personal and transactional information necessitates a strong privacy-first strategy. The enactment of the DPDP Act, 2023, signifies a significant step forward in creating a rights-driven data governance framework; nonetheless, its successful implementation will rely on seamless integration with SEBI's financial market rules.

A **2023 NASSCOM report** indicates that **more than 70%** of fintech companies in India depend on cloud infrastructure, with many of these services located in regions that could encounter limitations due to India's changing data transfer regulations. In this situation, clarity in regulations is crucial.

In the future, India ought to think about creating a clear adequacy framework for cross-border data transfers, akin to the EU's GDPR model, in order to prevent interruptions in global investment and data movement. Additionally, SEBI and the Data Protection Board of India must work together to create privacy standards for the sector that address the urgent, high-risk trading environment. Funding domestic cloud and AI infrastructure, offering incentives for privacy-focused technology, and creating training programs for compliance officers within trading firms can similarly connect privacy with performance. Though algorithmic trading has the potential to reshape finance, we

must not aim to hinder its progress. Instead, we should pursue a responsible acceleration, prioritizing individual rights, regulatory transparency, and digital trust.

References:

1.Baxi, Upendra. *The State and the Market as Power.* 6 SCC J. 1 (1995).

2.Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*. Ministry of Electronics and Information Technology, Government of India, 2018. https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

3. Bhattacharya, D., & Saha, S. (2016). *A review of SEBI's regulatory framework: Ensuring financial market integrity* in India. International Journal of Law and Management, 60(5), 1193-1212. https://doi.org/10.1108/IJLMA-01-2016-0010.

4.General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183.

5. *A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023*, https://www.journalsalliancepub.com/index.php/ijls/article/view/114

6. *Trade, Privacy, and DPDPA: Crafting India's Response to the Privacy-Trade Dilemma*. NLIU Law Review, October 23, 2024. https://nliulawreview.nliu.ac.in/blog/trade-privacy-and-dpdpa-crafting-indias-response-to-the-privacy-trade-dilemma/.

7.NASSCOM. *India FinTech: A $100 Bn Opportunity.* 2023. https://nasscom.in/knowledge-center/publications/india-fintech-opportunity-report.

8.Securities and Exchange Board of India. *Annual Report 2022–23*. https://www.sebi.gov.in/sebiweb/investment/annualreport.jsp.

9.Securities and Exchange Board of India. *Data Governance Framework (2023–24)*. SEBI Circular, March 2024. https://www.sebi.gov.in/legal/circulars.

10.The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

11.The Securities and Exchange Board of India Act, 1992, No. 15, Acts of Parliament, 1992 (India).

12.Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

13.Constitution of India, art. 21.

14.Privacy Act of 1974, 5 U.S.C. § 552a (United States).

15.China Clarifies Cross-Border Data Transfer Rules: Practical Guidance ... https://www.arnoldporter.com/en/perspectives/advisories/2025/06/china-clarifies-cross-border-data-transfer-rules

16.*Securities and Exchange Board of India (Stock Brokers) (Amendment) Regulations, 2024*, Gazette Notification, SEBI. https://www.sebi.gov.in/legal/regulations.