*Page: 1308-1323* *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 2**

**2026**

*DOI: https://doi.org/10.70183/lijdlr.2026.v04.202*

# THE FRICTION OF FINANCIAL ERASURE: AN ANALYTICAL STUDY ON THE LEGAL CONFLICT

**Chetanosho Shrikant Chilwant**[1]

## I. ABSTRACT

*The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant development in India's evolving data governance framework by recognizing the right to erasure as an extension of the constitutional right to privacy affirmed in Justice K.S. Puttaswamy v. Union of India. However, the practical implementation of this right generates substantial legal friction when applied within the financial sector, where the Prevention of Money Laundering Act, 2002 (PMLA) and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 require financial institutions to retain transaction records and customer identification data for regulatory and investigative purposes. This tension has acquired additional significance in light of the DPDP Rules, 2025 and the ongoing constitutional scrutiny of the data protection regime in Venkatesh Nayak v. Union of India, which raises broader concerns regarding privacy, surveillance, and governmental access to personal data. This paper critically examines whether the PMLA operates as an absolute legislative override to the right to erasure or whether both regimes can be harmoniously interpreted through principles of statutory construction and constitutional proportionality. Drawing upon comparative jurisprudence under the European Union's General Data Protection Regulation (GDPR), international standards developed by the Financial Action Task Force (FATF), and emerging regulatory technologies, the study argues that privacy and anti-money laundering objectives need not be mutually exclusive. It proposes a three-tiered governance framework consisting of Hard-Delete Protocols for non-regulated data, Encrypted Cold Storage for legally mandated retention records, and a transparent Denial Register to document justified refusals of erasure requests. The paper concludes that a layered data governance strategy offers a legally sustainable mechanism for preserving both individual privacy rights and systemic financial integrity within India's digital economy.*

[1] Ph.D. Research Scholar at Yashwantrao Chavan Law College & Ph.D. Research Centre, Pune (India). Email: oshoo.chilwant@gmail.com

 (ISSN: 2583-7753)

## II. KEYWORDS

Right to Erasure; Prevention of Money Laundering Act (PMLA); Financial Surveillance; GDPR Comparative Analysis; Data Protection Board of India.

## III. INTRODUCTION

The digital transformation of the Indian financial sector has created a sophisticated ecosystem where data serves as the primary currency for both commercial innovation and regulatory oversight. The enactment of the DPDP Act, 2023, signifies a constitutional maturity in Indian data governance, grounding the "right to erasure" in the fundamental right to privacy established by the Supreme Court of India in *Justice K.S. Puttaswamy v. Union of India*.[2]

However, this empowerment of the individual stands in sharp contrast to the Prevention of Money Laundering Act (PMLA), 2002, which imposes rigid, state-mandated obligations upon financial institutions to preserve transaction "memory" to combat financial crime.[3] This friction creates a complex regulatory environment where financial institutions, acting as "Data Fiduciaries," must navigate the competing demands of user privacy and statutory record-keeping. The resulting tension is not merely a technical glitch in compliance software but a fundamental philosophical and legal challenge: how does a digital democracy balance the individual's right to "forget" their financial past against the state's mandate to "remember" it for the sake of financial integrity? This paper explores this intersection, proposing a roadmap for harmonious coexistence between these two pillars of Indian law.

### A. Research Objectives

1. To analyse the statutory conflict between the "right to erasure" under the Digital Personal Data Protection Act, 2023 (DPDP Act) and the mandatory record-keeping obligations of financial institutions under the Prevention of Money Laundering Act, 2002 (PMLA).

[2] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
[3] Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).

2. To evaluate the constitutional validity of balancing privacy rights against state-mandated financial surveillance using the proportionality test established in *Justice K.S. Puttaswamy v. Union of India*.
3. To propose a governance framework, informed by comparative insights from the European Union's General Data Protection Regulation (GDPR), for reconciling individual data privacy with systemic financial integrity.

### B. Research Questions

1. Does the PMLA serve as an absolute legislative override to the data principal's right to erasure under the DPDP Act, 2023?
2. How can financial institutions reconcile the conflicting mandates of data privacy and mandatory financial record-keeping while adhering to the principles of proportionality and legality?
3. To what extent can the "layered" data strategy adopted in the European Union be adapted to the Indian regulatory landscape to resolve the conflict between privacy and financial surveillance?

### C. Hypothesis

The legislative friction between the DPDP Act and the PMLA does not necessitate the total subordination of one regime to the other; rather, it requires a "layered" data management approach where institutions prioritize statutory record-keeping for anti-money laundering compliance while upholding privacy for all non-essential or commercial data processing, thereby achieving a necessary regulatory equilibrium.

### D. Research Methodology

This research utilizes a normative and analytical design, employing a doctrinal methodology focused on statutory interpretation to examine the inherent tension between the data erasure provisions of the DPDP Act, 2023, and the long-term record-retention mandates of the PMLA, 2002. By applying the "Rule of Harmonious Construction" and teleological interpretation, the study critically evaluates whether these frameworks can coexist or if one functions as *lex specialis*, drawing upon primary sources—including the relevant statutes, judicial precedents like *Justice K.S.*

*Puttaswamy v. Union of India*, and subsidiary KYC regulations—alongside secondary academic commentary and comparative analyses of international frameworks such as the GDPR. Through this systematic comparison and conflict analysis, the study seeks to map the points of regulatory divergence to determine how financial entities can navigate competing mandates without compromising legal compliance or public policy objectives.

### E. Literature Review: The Friction of Financial Erasure

The foundational tension in this research arises from the "Privacy-Surveillance Paradox," where the individual's right to erasure under the DPDP Act, 2023, directly conflicts with the stringent, long-term record-retention mandates of the PMLA, 2002. Current academic literature largely treats data privacy and financial regulation as siloed disciplines, with privacy scholars focusing on corporate consent frameworks while financial law experts emphasize the necessity of audit trails for anti-money laundering compliance.

While international discourse notably regarding the EU's GDPR offers comparative insights into reconciling these domains, the Indian legal landscape lacks specific judicial precedents to define the threshold where financial surveillance mandates supersede privacy rights. Consequently, a significant research gap exists while there is ample descriptive analysis of both statutes, there is a distinct void in literature providing a "Harmonious Construction" framework that enables financial intermediaries to practically operationalize these competing legal obligations without incurring excessive regulatory risk.

## IV. STATUTORY ANALYSIS: THE "LAWFUL PURPOSE" DEFENCE

Section 8 of the DPDP Act, 2023, is the main source of conflict between financial monitoring and data privacy. This clause outlines the practical duties of a "Data Fiduciary." The DPDP Act is not absolute, even if its legislative ethos is based on the empowerment of the data principle. Data fiduciaries are required under Section 8(7) to assist in the deletion of personal data either upon the data principal's withdrawal of consent or when the purpose for which the data was gathered has been achieved. However, an important "safe harbour" clause expressly limits this requirement.

"Unless retention of such personal data is necessary for compliance with any law currently in force," the requirement to erase the data is waived."[4]

For financial institutions, this clause is the crucial aspect of their compliance approach. These entities function under a highly regulated system, primarily regulated by the PMLA and the related Prevention of Money Laundering (Maintenance of Records) Rules, 2005.[5] These regulations place a strict, non-negotiable obligation on financial institutions to keep detailed transaction records, documents for identity verification, and Know Your Customer (KYC) files. This requirement is an essential aspect of the national and international framework aimed at preventing money laundering and the financing of terrorism.

As a result, when an individual exercises their right to erasure as per the DPDP Act, a financial institution cannot simply view this request as an automatic and unconditional command for the deletion of data. Rather, the institution is required by law to conduct a thorough "statutory impact assessment." They should assess the request considering their ongoing, mandatory record-keeping duties under the PMLA. If the data such as comprehensive transaction records or Suspicious Transaction Reports (STRs) falls within the compulsory retention periods set by PMLA regulations, the fiduciary's responsibility to adhere to anti-money laundering legislation takes precedence over an individual's right to have their data erased. In these cases, the PMLA functions as the "law for the time being in force," protecting the financial institution from the erasure requirements of the DPDP Act. This framework guarantees that the DPDP Act is not misused by malicious individuals to erase their financial history, which could obstruct legitimate law enforcement inquiries.

## V. THE CONSTITUTIONAL CHALLENGE: SURVEILLANCE VS. PRIVACY

The constitutional validity of certain provisions of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 is presently under

[4] Digital Personal Data Protection Act, 2023, § 8(7), No. 22, Acts of Parliament, 2023 (India).
[5] Prevention of Money Laundering (Maintenance of Records) Rules, 2005, Rule 3 (India).

judicial scrutiny in Venkatesh Nayak v. Union of India, W.P.(C) No. 177/2026 (Supreme Court of India). The petition challenges, inter alia, Sections 17(1)(c), 17(2), 33(1), 36, and 44(3) of the DPDP Act and Rules 17 and 23(2) of the DPDP Rules, 2025. A central grievance concerns the amendment to Section 8(1)(j) of the Right to Information Act, 2005, which the petitioner argues creates an excessively broad exemption from disclosure of personal information, thereby affecting transparency, accountability, and the public's right to information under Articles 14, 19(1)(a), and 21 of the Constitution.

The petition also raises concerns regarding the institutional independence and composition of the Data Protection Board of India. Although the challenge is not directed specifically at financial-sector data retention, it highlights broader constitutional questions concerning the balance between privacy, transparency, governmental authority, and accountability within India's emerging data governance framework. These issues remain relevant to the present discussion because financial institutions must operate within a legal environment where privacy rights, regulatory obligations, and public-interest considerations increasingly intersect.

In order to ensure that they do not infringe upon the fundamental rights recognised in Puttaswamy, institutions must strike a balance between necessary legal disclosures and arbitrary requests. It is the institution's responsibility to show that its retention policies are properly "proportionate" to the danger that has been assessed. According to the Puttaswamy ruling, any invasion of privacy must pass three tests: proportionality, legitimacy, and legality. This test must be used by financial organisations when making retention decisions. The institution runs the danger of failing the "proportionality" test and infringing the data principal's right to erasure under the DPDP Act if data is kept longer than the five-year PMLA rule without a particular, ongoing inquiry.

As of June 2026, the Supreme Court has not granted an interim stay on the operation of the DPDP Act, 2023 or the DPDP Rules, 2025. The Court has, however, considered the constitutional issues raised in the connected petitions to be of substantial importance and has referred key questions for consideration by a larger bench.

Consequently, the legal position regarding several challenged provisions remains unsettled, and future judicial pronouncements may significantly influence the interpretation of privacy rights, transparency obligations, and regulatory governance under the DPDP framework.

## VI. NAVIGATING THE REGULATORY CONFLICT

The philosophy of sectoral priority is used to resolve the tension between the "right to erasure" of the DPDP Act and the "retention mandate" of the PMLA. A growing number of financial organisations are implementing "Purpose-Based Siloing."

### A. The Strategy of Segregation

Financial entities must categorize data based on the underlying legal mandate:

1. **Commercial Data:** PMLA regulations do not apply to data obtained for secondary purposes, such as personalised marketing, which must be deleted right away upon a legitimate request.
2. **AML/KYC Data:** The PMLA mandates that information gathered for KYC requirements, transaction logs, and beneficial ownership records be kept for the required amount of time (five years from the date of the transaction or the account closure).

### B. Managing Transparency vs. Confidentiality

Section 12(2) of the Prevention of Money Laundering Act, 2002, read with Rule 7 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, creates an important legal intersection between transparency obligations and anti-money laundering compliance. Reporting entities are required to maintain the confidentiality of information furnished, maintained, or verified under the PMLA framework and must avoid conduct that could amount to 'tipping-off' a customer or other person regarding the existence, preparation, or submission of a Suspicious Transaction Report (STR).

Consequently, when a data principal seeks access to information concerning personal data processing, a financial institution may be required to confirm the existence of certain processing activities without disclosing the contents of an STR or information

that could compromise ongoing monitoring, regulatory reporting, or law-enforcement functions. This creates a legitimate limitation upon the scope of transparency ordinarily associated with data protection rights. To reconcile these competing obligations, compliance teams should develop carefully structured redacted-disclosure protocols that preserve the confidentiality requirements of anti-money laundering law while ensuring that data principals receive access to information to the fullest extent permitted by law.

## VII. COMPARATIVE JURISPRUDENCE: INDIA VS. THE EUROPEAN UNION

The regulatory conflict between systemic financial surveillance and individual privacy is a major worldwide legal issue rather than a localised anomaly. The battle to strike a balance between the "right to be forgotten" and the necessity of financial openness has taken center stage in international jurisprudence as digital economies develop. The General Data Protection Regulation (GDPR), the world's best privacy law, mediates this dispute in the European Union. Although Article 17 of the GDPR grants a strong "right to erasure," the drafters were well aware of the need to preserve financial integrity and national security. Thus, by expressly removing from the deletion mandate any data processing required for "compliance with a legal obligation" under Union or Member State law, Article 17(3)(b) offers an essential "safety valve".[6]

Statutory retention durations required by successive Anti-Money Laundering Directives (AMLD) serve a fundamental "public interest" goal, according to European authorities led by the European Data Protection Board (EDPB).[7] This interpretation takes procedural primacy over individual privacy rights by establishing that financial integrity is a fundamental need for the operation of the internal market rather than just a sectoral preference. For India, the European experience offers a convincing road map. The idea of proportionality, which requires financial institutions to show that

[6] Regulation (EU) 2016/679 (General Data Protection Regulation), art. 17(3)(b), 2016 O.J. (L 119) 1.
[7] European Data Protection Board, *Respect individuals' rights* (2026), https://edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_en.

the data they store is strictly limited to what is required to fulfil their AML requirements, has been used by the EU in a large body of case law. European authorities have not hesitated to impose harsh penalties if a bank keeps client data for marketing reasons under the pretence of an AML mandate.

The Indian DPDP Act essentially reflects this global consensus by subordinating data subject rights to statutory compliance through the Section 8(7) carve-out, even though it lacks the explicit "legitimate interest" basis found in GDPR Article 6, which offers a more flexible, albeit complex, legal basis for processing. The main, and possibly most important, distinction is the state of judicial oversight today. The development of a clear standard for "proportionate" retention in the financial environment is still in its early stages in Indian jurisprudence. Indian courts must strike this balance in a far shorter amount of time than European courts, which have decades of experience juggling intricate regulatory directives with the privacy requirements of the European Convention on Human Rights.

Due to the seriousness of the financial crimes they target, sectoral laws (like the PMLA) have historically had a significant degree of deference from the judges, which presents another challenge for the Indian approach. It will be wise for Indian authorities to carefully examine the EU's experience with "Article 17(3) denials" as the Data Protection Board of India gets to work. India can create localised standards that respect the privacy core of the DPDP Act while preventing the misuse of its erasing power by examining how European financial controllers record the need for their data retention.

According to the EU model, the remedy is to formalise the procedure by which the right to erasure is restricted rather than to diminish it. India may establish a predictable, transparent, and legally defendable structure that resembles the worldwide gold standard while honouring the particular constitutional requirements of the Indian legal system by codifying stringent guidelines for when and how institutions might reject an erasure request. In order to maintain India's regulatory framework's compatibility with international financial standards while safeguarding its citizens' fundamental digital rights, this comparative progression is crucial.

 (ISSN: 2583-7753)

## VIII. INTERNATIONAL STANDARDS: THE FATF PERSPECTIVE

The international standard for anti-money laundering and counterterrorism financing measures is set by the Financial Action Task Force (FATF). The FATF promotes a "Risk-Based Approach" (RBA), which mandates that financial institutions keep an "audit trail" so that investigators can recreate transactions.[8]

The idea that privacy and anti-money laundering (AML) objectives are not intrinsically opposed is strengthened by this global drive. Institutions can guarantee that AML data is accessible to authorities without disclosing sensitive personal information beyond what is strictly required for legal reconstruction by utilising technical innovations like federated learning or privacy-preserving analytics.[9] In support of this "technological mediation," the FATF's digital transformation guidelines recommend that compliance be "privacy-by-design."

## IX. THE INTERSECTION OF EMERGING REGTECH AND DATA MINIMIZATION

Automating the discrepancy between the DPDP Act and the PMLA becomes critical as financial institutions incorporate RegTech (Regulatory Technology) into their operations. The DPDP Act's fundamental principle of "Data Minimisation" mandates that fiduciaries only gather information that is absolutely essential. However, a wide range of data is needed under the PMLA.

Emerging RegTech solutions increasingly incorporate privacy-preserving technologies such as Zero-Knowledge Proofs (ZKPs), which enable financial institutions to verify a customer's identity, eligibility, or compliance status without retaining or disclosing the underlying sensitive personal data. Such technologies offer a potential mechanism for reconciling the DPDP Act's principle of data minimisation with anti-money laundering record-keeping requirements. By retaining cryptographic proof of compliance rather than excessive personal information,

[8] Fin. Action Task Force, *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* 15-18 (2025).
[9] Fin. Action Task Force, *Stocktake on Data Pooling, Collaborative Analytics and Data Protection* 4-7 (2023), https://www.fatf-gafi.org/en/publications/Digitaltransformation/Digital-transformation.html.

institutions may reduce privacy risks while preserving the auditability required by financial regulators. This approach aligns with broader international efforts to integrate privacy-enhancing technologies into regulatory compliance frameworks and demonstrates how technological innovation can mitigate tensions between data protection and financial surveillance objectives.[10]

## X. VICARIOUS LIABILITY AND GOVERNANCE FRAMEWORKS

Board-level accountability and "Data Protection Officers" (DPOs) are introduced by the DPDP Act's legal liability framework. The DPO and the board of directors may be held vicariously accountable for regulatory negligence if a financial institution mistakenly deletes data that was mandated by the PMLA. Because of the risk-averse attitude this foster, organisations may have a tendency toward "over-retention."

A strong internal governance framework is necessary to combat this. One aspect of this is the establishment of a "Data Retention Committee" (DRC) whose job it is to periodically assess whether saved datasets are still necessary. The DRC must strike a compromise between the external DPDP erasure demands and the internal audit needs. Institutions can establish a "defensible compliance" posture by formalising this internal structure, demonstrating to regulators that the retention choice was not the result of arbitrary data hoarding but rather a well-reasoned, high-level policy decision.

## XI. IMPACT OF CROSS-BORDER DATA FLOWS ON FINANCIAL SOVEREIGNTY

Cross-border data transfers are restricted under the DPDP Act, which frequently mandates that data be processed within India or be subject to particular adequacy procedures. On the other hand, the PMLA deals with international financial networks (like SWIFT) where transaction data frequently crosses national borders.

[10] Financial Action Task Force, Stocktake on Data Pooling, Collaborative Analytics and Data Protection (FATF 2023) 4–7; Bank for International Settlements, Project Aurora: Data Analytics to Combat Money Laundering (BIS Innovation Hub 2023).

Does the exercise of a data principal's right to erasure require that their data be removed from foreign correspondent banks or international payment gateways? As a result, there is a severe clash between international financial system regulations and domestic privacy rules. This article contends that since the sovereignty and financial stability of the State depend upon the interoperability of international financial networks, data retained within cross-border payment and settlement systems may require differentiated treatment under the anti-money laundering framework.

However, any such retention must remain subject to the statutory framework governing cross-border data transfers under the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025. When the territorial scope of the right to erasure intersects with international financial-crime prevention mechanisms, clear regulatory guidance is required to reconcile privacy rights, financial stability concerns, and cross-border compliance obligations. Future guidance issued under the DPDP framework may play an important role in clarifying how these competing objectives should be balanced.[11]

## XII. THE ROLE OF THE DATA PROTECTION BOARD OF INDIA: THE ARBITER OF COMPLIANCE

The Data Protection Board of India (DPB) is positioned to play a pivotal role in resolving the tension between financial monitoring and data privacy. Established under Section 18 of the Digital Personal Data Protection Act, 2023, and operationalised on 13 November 2025, the Board functions as a specialised techno-legal adjudicatory body responsible for enforcing the Act's compliance framework. Pursuant to its statutory powers and functions under Section 27, the Board may inquire into complaints, direct remedial measures, and impose monetary penalties for contraventions of the Act.[12] Beyond its enforcement mandate, the Board is expected to assess the reasonableness and legality of data-retention practices in an evolving digital environment, thereby shaping the practical contours of privacy governance in

[11] Digital Personal Data Protection Act 2023, s 16; Digital Personal Data Protection Rules 2025, rr 14–15.
[12] Digital Personal Data Protection Act 2023, s 18; ibid, s 27.

India. The DPB is the final adjudicator that will establish the functional parameters of the "lawful purpose" defence for financial institutions, not just a regulator.

The DPB's upcoming "legal obligations" standards will be the final yardstick for these institutions' compliance infrastructures. The industry is currently experiencing severe regulatory uncertainty as it wavers between two possible interpretations of the Board's future position. Financial institutions may face a flood of individual erasure requests that they may feel legally obligated to comply with in order to avoid DPDP penalties if the Board adopts a narrow, strictly privacy-centric interpretation of the DPDP Act, even though such actions may conflict with the PMLA's more general requirements. On the other hand, the financial industry would have the much-needed legal certainty to maintain crucial audit trails without the continual risk of regulatory litigation if the Board adopted a more expansive, practical interpretation one that expressly recognises the PMLA's retention requirements as a comprehensive "permanent shield".

The DPB has the authority to accept "Voluntary Undertakings" from fiduciaries in addition to its interpretive role. This crucial mechanism has the potential to completely change the compliance environment. Instead of taking a punitive stance by default, the Board might let banks and fintechs take the initiative to address possible conflicts in their data architecture. For example, an organization could provide the Board a new data governance framework that shows how they have used controlled archiving and pseudonymization to strike a compromise between the DPDP Act's erasure requirements and the PMLA's mandate. The DPB can successfully guide the sector through intricate, fact-specific situations that are not specifically addressed by the statute text by accepting such undertakings and developing a corpus of "precedent-based" regulation.

Additionally, the Reserve Bank of India (RBI) and the Financial Intelligence Unit (FIU-IND) must collaborate deeply and institutionally with the DPB. The conflict between anti-money laundering and privacy is a systemic regulatory difficulty that calls for a coordinated approach. The DPB runs the risk of creating legal blind spots that parties involved in illegal funding could take advantage of if it operates alone. As a result, the

Board's function needs to change to that of a "inter-agency moderator." It must make sure that its privacy decisions do not unintentionally jeopardise the "regulatory memory" needed to track down the proceeds of crime.

In this role, the DPB will be in charge of determining what, in terms of international financial norms, qualifies as "necessary" retention. In order to ensure that the financial sector's voice and the practical realities of AML compliance are balanced with each person's basic right to privacy, the Board must also establish a transparent framework for stakeholder participation as it develops its rules and procedures. The Board's ability to define a precise, dependable legal standard will determine the validity of its rulings. The Board's course will determine whether India's banking industry continues to be a safe haven for economic activity or turns into a disjointed landscape of competing regulatory responsibilities, depending on whether it finally acts as a strict enforcer of erasure or as a balanced architect of data governance. The DPB will define the "reasonable person" norm for data management in the Indian financial sector by shaping the fiduciary standard of care through its adjudicatory output.

## XIII. SUGGESTIONS AND RECOMMENDATIONS

In order to reconcile the competing obligations imposed by the Digital Personal Data Protection Act, 2023 and the Prevention of Money Laundering Act, 2002, financial institutions should adopt a structured and technology-enabled governance framework. The following recommendations seek to ensure compliance with privacy obligations while preserving the regulatory objectives of anti-money laundering enforcement:

1. **Hard-Delete Protocols:** Financial institutions should implement automated deletion mechanisms for data that is not subject to statutory retention obligations, including marketing profiles, behavioural analytics records, temporary session logs, and other non-essential datasets. Such protocols would advance the DPDP Act's principle of data minimisation while reducing unnecessary privacy risks.
2. **Encrypted Cold Storage:** Data that must be retained under the PMLA and related regulatory requirements should be transferred to secure, encrypted

archival environments once the active commercial relationship with the customer has concluded. Restricting operational access while preserving statutory records enables institutions to satisfy both privacy and anti-money laundering objectives.

3. **Denial Register**: Institutions should maintain a formal Denial Register documenting every refusal of a data principal's erasure request. Each entry should identify the applicable legal basis for retention, including relevant PMLA provisions or regulatory obligations. Such a mechanism would enhance accountability, transparency, and regulatory audit readiness.

Collectively, these measures establish a layered governance framework capable of balancing individual privacy rights with the preservation of financial integrity and regulatory memory.

## XIV. CONCLUSION: TOWARDS A HARMONIZED REGULATORY FUTURE

The Prevention of Money Laundering Act, 2002 and the Digital Personal Data Protection Act, 2023 represent two equally important objectives within India's contemporary regulatory framework: the protection of individual privacy and the preservation of financial system integrity. The apparent conflict between the right to erasure and mandatory record-retention obligations should not be understood as a legislative defect but as an inherent feature of modern digital governance.

Through statutory interpretation, constitutional proportionality analysis, comparative examination of the GDPR framework, and consideration of FATF standards, this study demonstrates that neither regime requires complete subordination to the other. Instead, a harmonised approach is both legally possible and institutionally desirable. The future effectiveness of India's data governance architecture will depend upon coordinated action by financial institutions, the Data Protection Board of India, sectoral regulators, and the judiciary. If implemented through coherent regulatory guidance and principled adjudication, the coexistence of privacy protection and anti-money laundering compliance can provide a model for balancing fundamental rights with legitimate public interests in the digital age.

The success of this framework will ultimately be measured not by the absence of regulatory tension, but by the ability of institutions to manage that tension in a transparent, proportionate, and legally accountable manner.

## XV. REFERENCES

### A. Primary Sources: Legislation

1. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
2. Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).
3. Prevention of Money Laundering (Maintenance of Records) Rules, 2005.
4. Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1.
5. Venkatesh Nayak v. Union of India, W.P. (C) 1243/2023 (Del. H.C.).
6. Digital Personal Data Protection Rules, 2025 (particularly Rules 14–15 concerning cross-border data transfer conditions and compliance requirements).

### B. Secondary Sources: International Standards & Regulations

1. European Parliament and Council Regulation 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
2. Financial Action Task Force (FATF), Stocktake on Data Pooling, Collaborative Analytics and Data Protection (2023).
3. Bank for International Settlements (BIS) Innovation Hub, Project Aurora: Data Analytics to Combat Money Laundering (2023).