



The PMLA–DPDP Tension: Reconciling Anti-Money Laundering Obligations with India's Data Protection Framework

Anushka Acharya

Student, BA LLB (HONS.) CMR School of legal studies

Abstract

India's anti-money laundering regime and its new data protection regime are converging on the same underlying resource the transaction, identity and behavioural data that banks, financial institutions and other reporting entities collect from every customer while pulling in opposite doctrinal directions. The Prevention of Money Laundering Act, 2002 (“PMLA”) requires reporting entities to identify customers and beneficial owners, retain client and transaction records for five to ten years, and report suspicious transactions using an expansive evidentiary base that regulatory guidance now explicitly extends to IP addresses, device identifiers and behavioural patterns. The Digital Personal Data Protection Act, 2023 (“DPDP Act”), now partially in force following its phased notification between November 2025 and May 2027, is built on the opposite premise: purpose limitation, storage limitation, and a data principal's rights to correction and erasure. This paper maps the resulting tension across five fronts retention versus erasure, purpose limitation versus algorithmic suspicion-generation, consent fiction versus deemed consent, an asymmetric exemption structure that shields enforcement agencies from DPDP obligations while binding the private reporting entities that feed them data, and the friction between the DPDP Act's rights architecture and the Enforcement Directorate's entrenched practice of non-disclosure, upheld by the Supreme Court in *Vijay Madanlal Choudhary v. Union of India* (2022) and currently, as of a reconstituted bench in August 2026, under review. The paper traces this tension to a deeper constitutional history: the Supreme Court's 2018 ruling in the Aadhaar case that mandatory Aadhaar–bank account linking under the PMLA Rules failed the Puttaswamy proportionality test, a precedent that anticipated, by five years, the very conflict the DPDP Act's law-enforcement exemptions were designed to pre-empt. The paper concludes with a set of proposals scoped retention definitions, siloing of AML analytics from ordinary commercial processing, and proportionality-anchored limits on the state-instrumentality exemption for reconciling the two regimes as DPDP's remaining provisions come into force.

Keywords: Prevention of Money Laundering Act, 2002; Digital Personal Data Protection Act, 2023; anti-money laundering; data protection; financial privacy; Puttaswamy; Vijay Madanlal Choudhary; purpose limitation; data retention; Enforcement Directorate.

1. Introduction

On 20 August 2026, the Supreme Court of India reconstituted the bench hearing a batch of review petitions against its own July 2022 judgment in *Vijay Madanlal Choudhary v. Union of India*, the ruling that had upheld the Enforcement Directorate's expansive search, seizure, arrest

and non-disclosure powers under the Prevention of Money Laundering Act, 2002 (“PMLA”).¹ The review, now before a three-judge bench led by Chief Justice Surya Kant, is confined to two questions: whether the Enforcement Directorate (“ED”) must supply the accused with the Enforcement Case Information Report (“ECIR”) that triggers a PMLA investigation, and whether the Act's reversal of the presumption of innocence survives constitutional scrutiny.² This live constitutional contest is unfolding just as India's first comprehensive data protection statute, the Digital Personal Data Protection Act, 2023 (“DPDP Act”), completes its own staggered commencement partially in force since 13 November 2025, with the bulk of its substantive obligations, including the data principal's rights of correction and erasure, due to take full effect on 13 May 2027.³

These two timelines are not unrelated. Both regimes govern, in overlapping and sometimes contradictory ways, the same underlying resource: the identity, transaction and behavioural data that banks, non-banking financial companies, securities intermediaries and a growing list of “reporting entities” collect from every customer under PMLA's know-your-customer (“KYC”) and customer due diligence (“CDD”) obligations. The PMLA compels the collection, verification, retention for years, and onward reporting of this data to the Financial Intelligence Unit India (“FIU-IND”) and, where a suspicious transaction report matures into an investigation, to the ED. The DPDP Act, built on the opposite premise of purpose limitation, storage limitation, and an individual's right to correct or erase her own data, now sits directly on top of this pre-existing surveillance architecture. This paper maps the resulting tension: where the two regimes formally reconcile through statutory exemption, where that reconciliation is incomplete or untested, and what a coherent resolution would require.

Part II traces the constitutional prehistory of this tension, beginning with the Supreme Court's own 2018 finding that mandatory Aadhaar bank linkage under the PMLA Rules failed the proportionality test the Court had itself laid down a year earlier in *K.S. Puttaswamy v. Union of India*, and continuing through *Vijay Madanlal Choudhary*'s 2022 endorsement of PMLA's investigative architecture and the review now pending. *Part III* sets out the two statutes' data provisions in outline. *Part IV* identifies five specific points of doctrinal tension. *Part V* examines a little-noticed statutory bridge between the two regimes an amendment to PMLA's confidentiality clause that now expressly references the DPDP Act. *Part VI* offers a brief comparative note on the European Union's parallel AMLD/GDPR interface, and *Part VII* proposes a path to reconciliation.

¹On Trial Again, INDIA LEGAL (Aug. 2026), <https://indialegalive.com/cover-story-articles/il-feature-news/pmla-review-supreme-court-constitution-bench-vijay-madanlal-choudhary-ruling/>.

²Review of the SC's ‘Vijay Madanlal’ Judgement, SUPREME COURT OBSERVER, <https://www.scobserver.in/cases/karti-p-chidambaram-v-enforcement-directorate-review-of-the-scs-vijay-madanlal-judgement/> (last visited Sept. 2, 2026).

³Digital Personal Data Protection Act, 2023, WIKIPEDIA, https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Act,_2023 (last visited Sept. 2, 2026) (recording the three-phase commencement schedule under G.S.R. 843(E) and G.S.R. 846(E), dated 13 November 2025).

2. Constitutional and Doctrinal Foundations

2.1 Puttaswamy and financial informational privacy

In *K.S. Puttaswamy v. Union of India* (2017), a nine-judge bench of the Supreme Court recognised privacy as a fundamental right under Article 21 of the Constitution and held that any state measure restricting it must satisfy a four-part proportionality test: legality (the measure must be backed by law), legitimate aim, a rational connection between the measure and that aim, and necessity the absence of a less restrictive alternative equally capable of achieving the goal.⁴ This proportionality framework, later formalised further in the 2018 Aadhaar ruling, is the constitutional lens through which every subsequent PMLA data-collection requirement must, in principle, be read.

2.2 The 2018 Aadhaar ruling: PMLA Rule 9 fails the proportionality test

The clearest, and most frequently overlooked, precedent for the PMLA–data protection tension examined in this paper is not a data protection case at all: it is the Supreme Court's 2018 Aadhaar judgment itself. Among the several questions before the Constitution Bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (the Aadhaar case) was whether Rule 9 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, which mandated the linking of Aadhaar numbers with bank accounts, was constitutionally valid. The majority held that it was not: mandatory Aadhaar–bank linkage in the form then prescribed did not meet the proportionality test and therefore violated the right to privacy as it extends to banking details.⁵ This finding sits at the exact intersection this paper examines PMLA's identity-verification apparatus colliding with the constitutional limits on compelled disclosure of financial identity and it predates the DPDP Act by five years. Parliament's response was not to abandon Aadhaar-based verification but to make it voluntary and consent-based: subsequent amendments to the PMLA Rules and the Aadhaar Act itself permit, rather than compel, Aadhaar authentication for KYC purposes, a legislative recalibration that anticipated the DPDP Act's own consent-centric architecture.

2.3 Vijay Madanlal Choudhary (2022): PMLA's wide berth

If the 2018 Aadhaar ruling constrained PMLA's data-collection architecture at the identity-verification stage, *Vijay Madanlal Choudhary v. Union of India* expanded it dramatically at the investigation and enforcement stage. A three-judge bench upheld, against a challenge brought in more than 240 tagged petitions, the PMLA's provisions for provisional attachment of property, search and seizure, arrest without prior judicial approval, and the reversal of the

⁴Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India); see The Supreme Court's Aadhaar Judgement and the Right to Privacy, MONDAQ (2018), <https://www.mondaq.com/india/privacy-protection/744522/the-supreme-court39s-aadhaar-judgement-and-the-right-to-privacy>.

⁵Justice K.S. Puttaswamy and Ors. v. Union of India (Aadhaar Case), (2019) 1 SCC 1 (India); see Justice KS Puttaswamy and Ors. vs. Union of India, MANUPATRA (2018), https://www.manupatracademy.com/LegalPost/MANU_SC_1054_2018 (recording the holding that PMLA Rule 9's mandatory Aadhaar–bank linkage failed the proportionality test).

burden of proof onto the accused under Section 24.⁶ Central to this paper's concerns, the Court held that the ED is not a “police officer” for the purposes of the Code of Criminal Procedure, and therefore need not supply the accused with a copy of the ECIR the internal document that initiates a PMLA investigation in the manner an FIR would be disclosed, and that statements recorded by ED officers under Section 50 of the Act are admissible in evidence notwithstanding the accused's right against self-incrimination under Article 20(3).⁷ The cumulative effect is an investigative regime in which the state can compel, retain and act upon an individual's financial data the same data the DPDP Act elsewhere treats as belonging, in a qualified sense, to the individual without disclosing to that individual the specific allegations or evidentiary basis on which it is doing so.

2.4 The 2026 review: a live constitutional question

The Supreme Court itself signalled unease with this architecture as early as August 2022, when a bench led by then-Chief Justice N.V. Ramana agreed to review two aspects of the judgment ECIR non-disclosure and the reversed burden of proof while declining to reopen the remainder.⁸ That review, led by Karti P. Chidambaram's petition, was tagged with five others and has proceeded in fits and starts through 2024 and 2025, with the ED's counsel arguing the petitions amount to a disguised appeal that does not meet the narrow “error apparent on the face of the record” threshold for review.⁹ Intervening decisions have already qualified the practical edges of *Vijay Madanlal* without disturbing its core: in *Pankaj Bansal v. Union of India* (2023), the Supreme Court required the ED to furnish written grounds of arrest, a partial procedural correction that leaves the larger ECIR-disclosure and reverse-burden questions for the reconstituted bench to resolve.¹⁰ As of this writing, the outcome of the review is unknown; but its very pendency confirms that the boundary between PMLA's investigative secrecy and an individual's informational rights over her own financial data remains constitutionally unsettled at precisely the moment the DPDP Act is being phased into force.

3. The Two Statutory Regimes in Outline

3.1 PMLA's data architecture

Chapter IV of the PMLA imposes a dense set of data obligations on “reporting entities” banking companies, financial institutions, securities intermediaries, and a growing list of notified professions including real estate agents and dealers in precious metals. Section 11A requires

⁶*Vijay Madanlal Choudhary v. Union of India*, 2022 SCC OnLine SC 929 (India); see *Vijay Madanlal Choudhary v. Union of India*, (2022) 10 SCC, RECORD OF LAW, <https://recordoflaw.in/vijay-madanlal-choudhary-v-union-of-india-2022-10-scc/>.

⁷Review of the SC's ‘Vijay Madanlal’ Judgement, *supra* note 3; *Vijay Madanlal Choudhary V. Union Of India*, LAWFUL LEGAL (2025), <https://lawfullegal.in/vijay-madanlal-choudhary-v-union-of-india/>.

⁸Review of *Vijay Madanlal Choudhary Judgement*, LAWCHAKRA (Mar. 2025), <https://lawchakra.in/supreme-court/vijay-madanlal-choudhary-judgement/>.

⁹Review of SC's *Vijay Madanlal Judgement* | Day 2, SUPREME COURT OBSERVER (2025), <https://www.scobserver.in/reports/review-of-scs-vijay-madanlal-judgement-day-2-petitioners-grounds-dont-meet-maintainability-threshold-argues-ed/>.

¹⁰*Vijay Madanlal Choudhary v. Union of India* (PMLA Judgment), MODEL DIPLOMAT (2026), <https://modeldiplomat.com/learn/glossary/vijay-madanlal-choudhary-case> (discussing *Pankaj Bansal v. Union of India* (2023) and the pending review).

verification of client identity, including Aadhaar-based authentication where applicable, and examination of the client's ownership, financial position and source of funds.¹¹ Rule 9 of the PMLA (Maintenance of Records) Rules, 2005 requires customer due diligence identity verification, beneficial-ownership determination, and an assessment of the purpose and nature of the relationship for any account-based relationship of ₹50,000 or more.¹² Section 12 requires reporting entities to maintain records of all transactions for five years from the date of the transaction, and records of client identity, account files and business correspondence for five years from the end of the business relationship periods that FIU-IND guidance and sector-specific rules in practice extend to ten years for certain record classes.¹³ Reporting entities must additionally file suspicious transaction reports (“STRs”) with FIU-IND, and current FIU-IND guidance directs reporting entities to draw on the fullest available evidentiary base in compiling an STR explicitly including, alongside KYC and transactional data, IP addresses, device identifiers, and behavioural patterns and risk indicators with STRs required irrespective of any monetary threshold wherever reasonable grounds exist to suspect proceeds of crime or terrorism financing.¹⁴

3.2 The DPDP Act's data architecture

The DPDP Act inverts this logic. A “data fiduciary” may process personal data only for a lawful purpose for which the data principal has given consent, or for a narrower set of “legitimate uses” specified in Section 7, and must limit collection to what is necessary for that purpose.¹⁵ Section 8(7) requires a data fiduciary to erase personal data once the purpose for which it was collected is no longer being served and retention is not otherwise necessary for legal compliance, and Section 12 gives a data principal a corresponding right to correction, completion, updating and erasure of her personal data, including a right to request erasure directly.¹⁶ Section 17 exempts a defined set of processing activities from most of the Act's obligations, including processing necessary for enforcing a legal right or claim, processing by a court or tribunal exercising judicial or quasi-judicial functions, and most significantly for this paper processing “in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India.”¹⁷ Separately, Section

¹¹Prevention of Money Laundering Act, 2002, No. 15 of 2003, § 11A (India).

¹²Prevention of Money Laundering (Maintenance of Records) Rules, 2005, Rule 9 (India); see Snapshot: AML Requirements for Covered Institutions and Individuals in India, LEXOLOGY (2024), <https://www.lexology.com/library/detail.aspx?g=051102c5-9058-43c8-99c0-9c1def734dc4>.

¹³Prevention of Money Laundering Act, 2002, § 12(1) (India); Changes to Anti-Money Laundering Laws in India, IRCCL (2023), <https://www.irccl.in/post/changes-to-anti-money-laundering-laws-in-india-a-step-in-the-right-direction> (noting that while § 12 prescribes a five-year period, the PMLA Rules prescribe ten years for certain record classes).

¹⁴Obligations for Maintenance of Records under PMLA — FIU-IND, RAJPUT JAIN & ASSOCIATES (2026), <https://carajput.com/blog/obligations-for-maintenance-of-records-under-pmla-fiu-ind/> (describing FIU-IND guidance directing reporting entities to leverage IP addresses, device identifiers and behavioural patterns in compiling STRs).

¹⁵Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 4–7 (India).

¹⁶Digital Personal Data Protection Act, 2023, §§ 8(7), 12 (India); see also DPDP Section 12 with Interpretation, DPDP.COM, <https://www.dpdpa.com/dpdpa2023/chapter-3/section12.html> (last visited Sept. 2, 2026).

¹⁷Digital Personal Data Protection Act, 2023, § 17(1)(c) (India); Section 17 — Digital Personal Data Protection Act (DPDP) — Exemptions, APNILAW, <https://www.apnilaw.com/bare-act/dpdp/section-17-digital-personal-data-protection-act-dpdp-exemptions/> (last visited Sept. 2, 2026).

17(2) empowers the Central Government to exempt, by Gazette notification and without prior parliamentary approval, any “instrumentality of the State” from all or part of the Act's provisions on broadly framed grounds including sovereignty, security, public order and friendly relations with foreign states a power that has attracted sustained academic criticism for lacking any built-in proportionality requirement of the kind Puttaswamy demands.¹⁸

3.3 A staggered commencement

The interaction between these two regimes must be assessed against the DPDP Act's own incomplete rollout. The Ministry of Electronics and Information Technology notified the Act and the Digital Personal Data Protection Rules, 2025 on 13 November 2025, bringing into force the Data Protection Board's constitution and a limited set of procedural provisions on that date; a second tranche, covering Consent Manager registration and the enforcement and penalty machinery, is due on 13 November 2026; and the remaining substantive core notice and consent standards, the full suite of data principal rights including erasure, security safeguards, breach reporting, and retention and deletion rules does not take effect until 13 May 2027.¹⁹ As of the date of this paper, therefore, reporting entities' PMLA obligations are fully operative while their correlative DPDP obligations erasure rights chief among them remain prospective. This creates a compliance environment in which the tensions identified in Part IV are, for the moment, latent rather than actively litigated, but will crystallise rapidly once the May 2027 provisions take effect and data principals begin asserting erasure and correction rights against data that PMLA simultaneously requires reporting entities to retain.

4. Five Points of Doctrinal Tension

4.1 Retention versus erasure

The most direct collision is definitional. PMLA Section 12 requires retention of transaction records for five years and client-identity records for five years from the end of the relationship, extended to ten years for some record classes under the Rules; the DPDP Act's Section 8(7) erasure duty and Section 12 correction/erasure right point the opposite way. Industry compliance commentary has already begun to resolve this through the DPDP Act's own “compliance with law” carve-out: retention mandated by a named statutory instrument the RBI's Master Direction on KYC or the applicable PMLA Rule survives an erasure request, confined strictly to the fields and duration that instrument actually mandates, with everything else in the same customer file subject to the ordinary erasure obligation.²⁰ This is a workable interpretive resolution, but it is untested: no DPDP Rule or Data Protection Board guidance yet specifies how a reporting entity should partition a single customer record into “PMLA-

¹⁸DPDP Act Exemptions — State, Research & National Security, DPDPINDIA.IN, <https://www.dpdindia.in/dpdp-exemptions.html> (last visited Sept. 2, 2026) (arguing that Section 17's exemption grounds satisfy legality and legitimate aim but build in no proportionality constraint).

¹⁹Enforcement of the DPDP Act and Notification of the DPDP Rules, SHARDUL AMARCHAND MANGALDAS & CO. (Nov. 2025), <https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/>; DPDP Rules 2025 Timeline: Every Date and Deadline, PROTECTCOMPLY (Aug. 2026), <https://protectcomply.com/blog/dpdp-rules-2025-timeline>.

²⁰KYC Record Retention Period: RBI, PMLA & DPDP (2026), CONSENTOS (July 2026), <https://consentos.in/learn/kyc-record-retention-period/> (proposing that retention carve-outs be tied to a named legal instrument and confined to its mandated fields and duration).

mandated” fields that survive an erasure request and “ordinary commercial” fields marketing preferences, product cross-sell data, app usage analytics that do not, particularly where both categories of data have historically been stored in a single undifferentiated customer profile.

4.2 Purpose limitation versus algorithmic suspicion-generation

A subtler tension arises from the DPDP Act's purpose-limitation principle. Data collected for one purpose of opening a savings account, say is not, under ordinary DPDP logic, freely available for an unrelated purpose without fresh notice or a Section 7 legitimate-use basis. FIU-IND's own STR guidance, however, instructs reporting entities to draw on “all available data,” including IP addresses, device identifiers and behavioural patterns collected in the ordinary course of digital banking, when compiling a suspicious transaction report in effect directing the repurposing of data collected for transactional convenience into an input for algorithmic suspicion-generation about the same customer.²¹ Section 17(1)(c)'s law-enforcement exemption plainly covers the STR itself once filed with FIU-IND, but the antecedent step a private reporting entity mining its own commercially collected behavioural data to build the suspicion profile that becomes an STR occurs before the exemption's law-enforcement nexus is established, and sits uneasily with the purpose-limitation principle that otherwise governs that same reporting entity's processing of the identical data for its ordinary banking relationship with the customer.

4.3 Consent fiction versus deemed consent

The DPDP Act's default lawful basis for processing is consent free, specific, informed, unconditional and unambiguous, per Section 6 but Section 7 supplies a list of “legitimate uses”, akin to a deemed-consent basis, that includes processing for compliance with any law. In practice, PMLA-driven KYC and CDD processing has always proceeded on a basis closer to compulsion than consent: a prospective customer who declines to supply the identity and beneficial-ownership information Rule 9 demands simply cannot open the account or execute the transaction. The DPDP Act's Section 7 legitimate-use basis accommodates this reality without friction at the level of legal form, but it does so by removing PMLA-driven financial-identity processing almost entirely from the consent architecture that is the Act's central innovation meaning the single largest, most sensitive category of routinely collected financial data in the country (KYC and CDD records across every bank, NBFC and securities account in India) is processed on a basis that never engages the data principal's actual choice at all.

4.4 The asymmetric exemption: who answers to the DPDP Act?

The most structurally significant tension is the exemption architecture itself. Section 17(1)(c) exempts law-enforcement processing from most Chapter II and III obligations, and Section 17(2) allows the Central Government to exempt any state instrumentality from the Act altogether by simple Gazette notification.²² FIU-IND and the ED the two agencies that ultimately receive, aggregate and act upon the entire PMLA data pipeline sit squarely within

²¹Obligations for Maintenance of Records under PMLA — FIU-IND, *supra* note 12.

²²India's Data Protection Law Allows Government to Exempt Itself, *MEDIANAMA* (2024), <https://www.medianama.com/2023/08/223-dpdp-bill-2023-government-exemptions-3/>.

the class of bodies these provisions are designed to reach. The result is a pronounced two-tier structure: the private reporting entities that collect, verify and initially process the data (banks, NBFCs, securities intermediaries) face the full weight of DPDP obligations consent architecture, security safeguards, breach notification, and, from May 2027, correction and erasure rights for exactly the same data that, the moment it crosses into an STR filed with FIU-IND or an ECIR opened by the ED, becomes subject to little or none of that architecture. A data principal seeking to correct an error in her own KYC record can, in principle, do so at her bank; the same data principal has no comparable DPDP-based avenue to correct or even access the version of that data sitting in an FIU-IND database or an ED case file, since Section 17 exempts precisely that downstream processing. This asymmetry mirrors, in the data protection register, the exact structural criticism the Supreme Court's pending review of *Vijay Madanlal Choudhary* is currently examining in the criminal-procedure register: that PMLA's enforcement architecture affords the state broad access to and control over an individual's financial information while affording the individual correspondingly little visibility into, or recourse against, how that information is used.

4.5 Access and erasure rights versus ECIR secrecy

A final, more speculative tension concerns the DPDP Act's rights architecture once fully in force from May 2027. Sections 11 and 12 give a data principal rights of access to a summary of her personal data and its processing, and of correction and erasure. *Vijay Madanlal Choudhary* holds that the ED need not disclose the ECIR the document that would reveal what financial data has been gathered about a person and why to the person under investigation, treating it as an internal document analogous to, but importantly distinct from, a First Information Report.²³ Because Section 17(1)(c)'s law-enforcement exemption formally removes ED and FIU-IND processing from the DPDP Act's access-rights provisions in the first place, there is no direct doctrinal collision the exemption pre-empts the conflict by design. The friction is at the level of legislative policy rather than positive law: the DPDP Act's stated purpose is to recognise “the right of individuals to protect their personal data,” yet the single category of government body most likely to hold extensive, consequential financial data on a named individual, and most likely to use it to justify arrest, attachment or prosecution, is the category the Act exempts most completely from the individual's ability to know what that body holds.

5. The Section 12(4) Cross-Reference: A Statutory Bridge, Untested

One provision suggests Parliament was, at least partially, alert to this tension. PMLA Section 12(4) imposes a confidentiality obligation on reporting entities in respect of the records they maintain and furnish, and secondary commentary on the amended provision indicates that this confidentiality obligation is now expressed as being “subject to the provisions of the Digital Personal Data Protection Act 2023” an express cross-reference, if the secondary reporting is accurate, that would make the DPDP Act's confidentiality and security standards the operative floor for how reporting entities handle PMLA records, layered onto PMLA's own

²³*Vijay Madanlal Choudhary vs Union of India*, INDIAN KANOON, <https://indiankanoon.org/doc/14485072/> (last visited Sept. 2, 2026).

confidentiality rule.²⁴ If accurate, this cross-reference is significant precisely because it runs in only one direction: it binds reporting entities' confidentiality practices to DPDP standards without similarly binding FIU-IND's or the ED's downstream handling of the same records once furnished reinforcing, rather than resolving, the asymmetric exemption structure identified in section 4.4. The provision deserves close doctrinal attention once the DPDP Act's security-safeguard obligations take full effect in May 2027, since it may be the clearest textual anchor available for arguing that reporting entities' PMLA confidentiality duties and DPDP data-security duties are, by Parliament's own design, meant to operate as a single integrated standard rather than two independent and potentially conflicting ones.

6. A Comparative Glance: the EU's AMLD/GDPR Interface

India is not alone in needing to reconcile an anti-money-laundering regime with a general data protection statute. The European Union's Anti-Money Laundering Directives operate alongside the General Data Protection Regulation ("GDPR"), and Article 23 GDPR permits member states to restrict data-subject rights, including erasure, where necessary to safeguard the prevention, investigation, detection or prosecution of criminal offences a structural analogue to DPDP Section 17(1)(c). The EU's Financial Action Task Force-aligned retention rules similarly require several years of transaction-record retention notwithstanding GDPR's storage-limitation principle. The salient difference is architectural rather than substantive: GDPR's Article 23 restrictions must be provided for by a specific legislative measure respecting the essence of the fundamental rights and freedoms and satisfying a proportionality test enumerated in the Article itself, whereas DPDP Section 17(2)'s state-instrumentality exemption operates by executive notification without an equivalent statutory proportionality checklist the same gap that Indian commentators have identified as DPDP's most significant departure from the Puttaswamy standard the Supreme Court itself established in the domestic constitutional order that both Section 17 and the PMLA must, in principle, satisfy.

7. Toward Reconciliation: Proposals

Five reforms, each addressed to a specific tension identified in Part IV, would move the two regimes toward genuine reconciliation rather than the current arrangement of parallel statutes bridged only by broad exemption language.

- Scope retention carve-outs to named fields and durations. DPDP Rules or Data Protection Board guidance should specify, for PMLA-regulated entities, precisely which data fields (client identity, beneficial ownership, transaction particulars) are covered by the Section 8(7) compliance-with-law carve-out and for how long, leaving all other data in a customer's file marketing, app-usage analytics, and any behavioural or device data not itself mandated by the PMLA Rules subject to ordinary erasure rights.
- Silo AML-analytics processing from ordinary commercial processing. Given FIU-IND guidance encouraging use of IP addresses, device identifiers and behavioural patterns

²⁴Snapshot: AML Requirements for Covered Institutions and Individuals in India, *supra* note 11 (reporting that PMLA § 12 confidentiality obligations are now expressed as subject to the DPDP Act, 2023; this cross-reference should be verified against the official amended text of the PMLA before reliance in formal submissions, as it was not independently located in the Act's consolidated text for this paper).

in STR compilation, reporting entities should be required to process such data for AML purposes in a logically and, where feasible, technically segregated system from the data used for ordinary product and marketing purposes, so that a purpose-limitation breach in one function does not silently occur through unrestricted internal data-sharing.

- Anchor the Section 17(2) state-instrumentality exemption to a proportionality test. Consistent with the Puttaswamy framework the Supreme Court itself applied to strike down mandatory Aadhaar–bank linkage in 2018, any notification exempting FIU-IND or the ED from DPDP obligations should be required to state the specific legitimate aim served, the necessity of the exemption's scope, and be subject to periodic review rather than standing as an open-ended, indefinitely renewable carve-out.
- Build a Data Protection Board–FIU-IND coordination mechanism. Because reporting entities' DPDP obligations and their PMLA reporting obligations govern the same data at different points in its lifecycle, the Data Protection Board of India and FIU-IND should establish a formal information-sharing and interpretive-coordination protocol, akin to the RBI's existing role in KYC standard-setting, to prevent reporting entities from receiving conflicting guidance from the two regulators as DPDP's May 2027 provisions take effect.
- Clarify the Section 12(4) cross-reference through express amendment or rules. If PMLA Section 12(4)'s confidentiality obligation is indeed now expressed as subject to the DPDP Act, this cross-reference should be extended, through amendment or DPDP Rules, to bind FIU-IND's and the ED's downstream handling of PMLA-sourced data as well, so the confidentiality and security standard travels with the data rather than lapsing once it leaves the reporting entity's hands.

8. Conclusion

The PMLA and the DPDP Act were drafted twenty-one years apart, by different ministries, in response to entirely different policy imperatives — one to satisfy India's Financial Action Task Force commitments and choke the financing of organised crime and terrorism, the other to give constitutional content to the right to privacy the Supreme Court recognised in 2017. Neither statute was designed with sustained reference to the other, and the DPDP Act's Section 17 exemptions function, in practice, as the entire mechanism by which the two are reconciled: a broad, largely unconditional carve-out for law-enforcement and state-instrumentality processing that removes most of the tension from positive law by removing PMLA's downstream state actors from the DPDP Act's reach almost entirely. This is a reconciliation of convenience rather than of principle, and it reproduces, in data protection terms, the same asymmetry between state access and individual recourse that the Supreme Court is currently revisiting in the pending review of *Vijay Madanlal Choudhary*. As the DPDP Act's remaining provisions take effect in May 2027 and the first data principals attempt to correct or erase KYC records their bank is simultaneously obliged to retain for the Enforcement Directorate's benefit, this paper's central claim will move from doctrinal analysis to live dispute: that a data protection statute built on consent, purpose limitation and individual recourse, and an anti-money-laundering statute built on compulsion, retention and state access, cannot be reconciled by



exemption alone only by the kind of proportionality-anchored, field-specific, institutionally coordinated framework this paper has proposed, and that neither statute, as currently drafted, yet supplies.

Bibliography

Changes to Anti-Money Laundering Laws in India: A Step in the Right Direction ?, IRCCL (2023).

DPDP Act Exemptions — State, Research & National Security, DPDPINDIA.IN (last visited Sept. 2, 2026).

DPDP Rules 2025 Timeline: Every Date and Deadline, PROTECTCOMPLY (Aug. 2026).

DPDPA Section 12 with Interpretation, DPDPA.COM (last visited Sept. 2, 2026).

Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

Digital Personal Data Protection Act, 2023, WIKIPEDIA (last visited Sept. 2, 2026).

Enforcement of the DPDP Act and Notification of the DPDP Rules, SHARDUL AMARCHAND MANGALDAS & CO. (Nov. 2025).

India's Data Protection Law Allows Government to Exempt Itself, MEDIANAMA (2024).

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

Justice K.S. Puttaswamy and Ors. v. Union of India (Aadhaar Case), (2019) 1 SCC 1 (India).

Justice KS Puttaswamy and Ors. vs. Union of India, MANUPATRA (2018).

KYC Record Retention Period: RBI, PMLA & DPDP (2026), CONSENTOS (July 2026).

Obligations for Maintenance of Records under PMLA — FIU-IND, RAJPUT JAIN & ASSOCIATES (2026).

On Trial Again, INDIA LEGAL (Aug. 2026).

Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (India).

Prevention of Money Laundering Act, 2002, No. 15 of 2003 (India).

Review of SC's Vijay Madanlal Judgement | Day 2, SUPREME COURT OBSERVER (2025).

Review of Vijay Madanlal Choudhary Judgement, LAWCHAKRA (Mar. 2025).

Review of the SC's 'Vijay Madanlal' Judgement, SUPREME COURT OBSERVER (last visited Sept. 2, 2026).

Section 17 — Digital Personal Data Protection Act (DPDP) — Exemptions, APNILAW (last visited Sept. 2, 2026).

Snapshot: AML Requirements for Covered Institutions and Individuals in India, LEXOLOGY (2024).



The Supreme Court's Aadhaar Judgement and the Right to Privacy, MONDAQ (2018).

Vijay Madanlal Choudhary V. Union Of India, LAWFUL LEGAL (2025).

Vijay Madanlal Choudhary v. Union of India (PMLA Judgment), MODEL DIPLOMAT (2026).

Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929 (India).

Vijay Madanlal Choudhary vs Union of India, INDIAN KANOON (last visited Sept. 2, 2026).

