The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

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

The Right to be Forgotten: Can You Actually Force Apps to Delete Your Data under the DPDPA?

Saachi Srivastava

Part I: Introduction and Abstract — The Constitutional Myth of the Clean Slate

Abstract

The present paper examines the feasibility of the Right to Erasure prescribed by Section 12 of the Digital Personal Data Protection (DPDP) Act, 2023. Despite its official claim to be India's adoption of the "Right to be Forgotten" (RTBF), a deeper dive into implementing such a right as part of corporate processes exposes the struggle between the right of users and the duty to retain data according to the mandate of the state. In contrast to general descriptions of regulatory requirements of the DPDP Act, this paper will explore the specific sources of conflict, including the superior compliance systems set forth by the federal government (PMLA, tax laws, and cybersecurity regulations); "Data Resurrection" in distributed cloud storage systems; and "continuous processing purposes" enshrined in standard Terms of Service for corporations. Finally, it is argued here that in the absence of strict standardisation by the DPBI, the right to delete becomes only an illusion for consumers.

Introduction

Over the past few decades, the Indian internet existed as a storage system that forgot nothing. As soon as an individual had to share their personal information with any digital application, that personal information would stay permanently detached from them forevermore. It would be an eternal piece of data, which would get stored within corporate systems, be used by data brokers and keep getting monetised beyond the user's lifespan on the application itself.

With the introduction of the Digital Personal Data Protection Act (DPDPA), 2023, this paradigm might well get turned on its head. With the inclusion of the Right to Erasure within Section 12, the legislation hopes to bake a basic premise of privacy into corporate processes: the ability to disappear off of the application's server itself.

A corporate architecture, however, isn't just a simple database that one can clear by pressing the "delete" button. On the contrary, today's digital applications represent complex ecosystems made up of APIs of external vendors, cloud-based storage, and immutable backups. When a citizen utilises their right to erase personal data from company records, the compliance situation turns into a catch-22 for corporate lawyers and IT staff. To determine the viability of such a right or the fiction of the corporate world, it is necessary to assess the friction between the key players involved in this Act:

- **The Data Principal:** The individual citizen who demands the erasing of his digital footprint.
- **The Data Fiduciary:** The primary app or platform that is responsible for performing the request to erase.
- **The Data Processor:** The cloud provider or external vendor which stores backed up copies of the Principal's data.

Part II: Background and Legal Framework — The Jurisprudential Architecture of Digital Erasure

For determining the boundaries for the implementation of erasure of data, we need to follow the path this concept took from being a judicial rule to being a statutory rule.

Constitutional Origins: Right to Informational Privacy under Article 21

The right to petition for deleting one's personal information emanates from Article 21 of the Constitution of India. The Supreme Court of India, in a unanimous decision in the case of Justice K.S. Puttaswamy (Retd) v. Union of India (2017), ruled that the right to privacy is an integral part of the right to life and personal liberty under the constitution of India. Importantly,

informational self-determination was seen as one of the core rights.

It should be noted that individuals do not surrender their proprietary rights on their personal information just by temporarily giving out this information to some commercial app. The platform remains a mere caretaker. Storing user data forever against his/her express wish amounts to continued infringement of his/her fundamental right to informational privacy.

This constitutional ideology has been subsequently put to test in different high courts. Cases such as Ashutosh Kaushik v. Union of India have highlighted issues of the "Right to be Forgotten", compelling search engines to erase all outdated content that has no present public utility. This shows that the freedom to forget the online past is fundamental for the liberty of an individual.

Deconstructing Section 12 of the DPDPA

The DPDPA turns the aforementioned constitutional principle into a statutory requirement via Section 12. The statute uses an extremely stringent and objective trigger mechanism:

1. **The Trigger:** Per Section 6, the Data Principal may withdraw his consent at any point in time. On the other hand, there is automatic erasure once the specific commercial purpose for the collection of the data is satisfied.
2. **The Mandate:** Post-Trigger, Section 12, mandates the data fiduciary to erase the personal data.
3. **The Timeline:** The system makes this purge take place without delay.

Part III: The Operational Friction — The Retain-vs.-Delete Compliance Wall

Nevertheless, even with the straightforward wording of Section 12, it is impossible for a company to focus on the DPDPA alone. Within the business environment, the need of the application to immediately delete user data confronts a barricade of parallel federal legislation insisting on data retention.

Overriding Federal Statutes

The DPDPA clearly identifies that the right to data erasure should give way if there is any obligation under another existing law for data retention. The resultant operational conflict arises

in numerous highly regulated industries:

Regulatory Scope	**Applicable Law/Jurisdiction**	**Period for Compulsory Retention**	**Effect on Erasure under Section 12**
Fintech and Banking Sector	The Prevention of Money Laundering Act (PMLA), 2002	**5 Years** after account closure	Deleting KYC records, ID tokens, and financial transaction records is prohibited by law.
Corporate Tax	Income Tax Act, 1961 / Companies Act, 2013	**8 Years**	Transaction records, payment records, and billing addresses need to be retained for audit trail purposes.
E-Commerce	Consumer Protection (E-Commerce) Rules, 2020	Specific audit period	Dispute record of consumers, invoice information, and communication from the vendors cannot be deleted beforehand.
Cyber Security	CERT-In Cyber Security Directions (IT Act, 2000)	Upto **5 Years**	Access logs of technical systems and ip logs of users

			need to be retained for investigation by the states.

Reflect on the practicality of a user deleting their account on a popular digital wallet or neobank. application. It is expected that all traces of the user's information, including account registration data, transaction records, and identification documents issued by the government, should get wiped out.

But in case the fintech fiduciary complies with the guidelines in their totality, then the executives are instantly exposed to a felony charge under the PMLA in case audit trails necessary for fraud investigations are destroyed. This means that the corporate lawyers need to create a dual process lifecycle; while the account is “cosmetically deleted”, the underlying data is shifted to an extremely encrypted read-only archive.

The "Data Resurrection" Vulnerability in Vendor Networks

Without any overriding retention legislation in force, however, completely wiping out the online identity of a user raises some serious technical problems within today’s corporate cloud infrastructure.

With the data principal requesting that his data be erased, the main data fiduciary becomes legally responsible for deleting the data from the whole chain of its downstream processing. But modern software doesn’t keep the information in one secluded bucket; instead, it uses a complex network of data processors, including cloud providers, analytics plugins, marketing automation systems, and remote backup services. This creates the technical paradox known as “Data Resurrection”:

- **Active versus Archived Silos:** The organisation may have been successful in executing the script that deletes the record of the particular user from the active production database. This data continues to remain intact on immutable cold storage tapes that are used for disaster recovery.
- **Systemic Issue:** In case the organisation experiences a network crash after three months

and restores the whole system from a backup copy, there is a possibility that the deleted record may be inadvertently resurrected in the active database. This is a violation of DPDPA, where the fiduciary is exposed to regulatory sanctions from the DPBI due to lack of proper monitoring of data processors.

Part IV: Critical Analysis and Evaluation — The Ambiguity of "Purpose Fulfillment"

In light of a comprehensive legal analysis of the DPDPA, there is one serious structural flaw associated with the subjective nature of the definition of the term “Purpose Fulfillment” stated in Article 12 of the Act.The legislation mandates that a business organisation delete the personally identifiable information upon the accomplishment of the purpose for which it was originally collected. Yet, since the Act does not provide clear limits on what constitutes a legitimate purpose, businesses can devise an extremely vague privacy policy to circumvent the issue.

The Elasticity of Corporate Terms of Service

“If your ride-sharing, food delivery, or social media app collects user data 'to continuously optimise platform algorithms, train machine learning models, enhance predictive user safety, and prevent systemic security fraud,' then when does that purpose get fulfilled?”

Since such processes happen continuously, the legal counsel of that company can confidently assert that so long as the platform is operating, then the primary purpose of processing the data will never be exhausted, even though the user may not be actively using the app anymore. Such a situation creates a dire problem of compliance:

- **The Evasion Track:** The companies can keep processing the user metrics based on “platform security and safety analytics”, making Section 12 effectively useless to the ordinary user.
- **The Regulatory Risk:** On the other hand, if the corporate lawyers abuse the elasticity of the wording above, they would be risking the wrath of the DPBI, as they could be accused of violating the legislative intent of data minimisation.

Such an uncertain regulatory environment compels corporate law firms to take a gamble on how far the DPBI will go with "fulfilling purposes".

Part V: Conclusion and Actionable Reforms — Engineering True Digital Sovereignty

It permanently changes how corporate data governance will be carried out in India, converting a voluntary public relations practice into a public law requirement of data erasure. However, despite that, the Right to be forgotten is still stuck in-between the theoretical framework of informational autonomy and practical corporate technologies along with conflicting federal laws. In order to solve these legislative discrepancies and create an operational standard, there are three necessary structural reforms India's data protection framework needs to adopt the following:

- **Standardisation of Cryptographic Erasure Requirements:** For situations when data is stored in unchangeable distributed cloud backups and physical erasure is impossible, the DPBI should codify cryptographic erasure as a form of compliance-ready erasure. By destroying the cryptographic key connecting the user's data profile, the data becomes irreversibly unreadable, which makes it erased according to the Section 12 statute.
- **Mandatory Lifecycle Tagging on Ingestion:** The enterprise must shift from manual tagging to an automatic tagging regime of data upon its ingestion. When a person submits their data, each individual piece of metadata must be tagged separately with a legal lifecycle that is unique (for example, a billing address would automatically get tagged for an eight-year read-only archive lifecycle, and casual app tracking metrics and searches would get permanently deleted after 30 days of closing the account).
- **Regulatory Caps on Purpose Drafts:** The DPBI should release specific guidelines prohibiting the use of elastic terms like "system optimisation" to explain the need for retaining any of the submitted data. Once the account has been closed, the primary commercial purpose of processing should be considered as legally served.

In conclusion, the companies that not only survive but also succeed in the DPDPA era will be the ones that will move away from cosmetic fixes at the frontend of operations and embed compliance by design at the backend level in their network. Through transparency and recognising the sovereign identity of the data principal, corporate India could leverage its

compliance into a competitive edge on the global stage.

References and Citations

1. Digital Personal Data Protection Act, No. 22 of 2023, § 12, Gazette of India (Aug. 11, 2023).
2. Digital Personal Data Protection Act, No. 22 of 2023, § 6, Gazette of India (Aug. 11, 2023).
3. *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, (2017) 10 SCC 1.
4. *Ashutosh Kaushik v. Union of India & Ors.*, W.P.(C) 6218/2021 (Delhi HC).
5. Prevention of Money Laundering Act, No. 15 of 2003, Gazette of India (Jan. 17, 2003).
6. Consumer Protection (E-Commerce) Rules, 2020, Ministry of Consumer Affairs, Food and Public Distribution, Government of India (2020).
7. Companies Act, No. 18 of 2013, § 128, Gazette of India (Aug. 29, 2013).
8. Income Tax Act, No. 43 of 1961, Gazette of India (Sept. 13, 1961).