



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

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

THE DATABASE DILEMMA: RESOLVING THE CONFLICT BETWEEN DATA ERASURE RIGHTS AND PROPRIETARY TRADE SECRETS

~ Biswarup Saha

ABSTRACT

The permanence of digital information has generated one of the most complex conflicts in modern commercial law: the tension between a data principal's statutory right to privacy and an enterprise's intellectual property rights. This report provides an in-depth doctrinal and comparative analysis of the "Database Dilemma" – the legal clash that occurs when a person, particularly a former senior executive, exercises his right to erasure or data portability under law, and the company claims that complying with the request would disturb its copyrighted database structure or expose confidential trade secrets. The paper critically examines Section 12 and Section 7(i) of the Digital Personal Data Protection (DPDP) Act, 2023, in juxtaposition with the protection provided to sui generis databases under Section 2(o) of the Copyright Act, 1957 and the mandate to protect undisclosed commercial information under Article 39 of the TRIPS Agreement, based on the Indian legal framework. This report synthesises a proportionality framework by reviewing the jurisprudence of the Court of Justice of the European Union (CJEU) under the General Data Protection Regulation (GDPR). To summarise, the right to erasure, while absolute in intent, must be harmonised with intellectual property laws, through rigorous necessity tests, cryptographic pseudonymisation and contractual abstraction of analytical methodologies as found in modern enterprise terms of service.

INTRODUCTION

We have transitioned from analogue record keeping to sophisticated digital asset management, and it has dramatically transformed the relationship between people and the companies that employ or serve them. In the era of digital economy, personal data has a dual (and sometimes antagonistic) function. Personal data is inextricably linked to individual identity and dignity from a constitutional and human rights perspective. The landmark Supreme Court judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* ruled the right to privacy as a fundamental right giving permanent constitutional jurisprudence to this principle.¹ Conversely, from the point of view of corporations, the aggregation, structuring and relational mapping of personal data is the raw material of modern commerce, often crystallising into highly valuable and legally protected intellectual property.

This dichotomy serves as the foundation of the "Database Dilemma." The tension is at its peak when a data principal, like a former C-level executive whose past decisions metadata and performance data are hard-coded in an enterprise's proprietary systems, attempts to exercise a statutory right to data erasure or portability. The enterprise is subsequently confronted with an existential legal problem: the potential consequences of complying with the privacy mandate by extracting or deleting the executive's specific data node include the irreparable destruction of the relational graph of a copyrighted database, the corruption of an algorithmic model, or the disclosure of a highly guarded trade secret. This tension has been codified formally with considerable ambiguities in India with the enactment of the Digital Personal Data Protection (DPDP) Act, 2023.² The fundamental right to privacy is operationalised by the legislation, which grants individuals the ability to request the correction, updating, and erasure of their personal data.³ Nevertheless, the DPDP Act does not contain an explicit, highly detailed statutory carve-out within its erasure provision to safeguard the intellectual property rights of the fiduciary, in contrast to its European counterpart, the General Data Protection Regulation (GDPR). At the same time, the Indian Copyright Act, 1957, protects computer databases specially as "literary works" under Section 2(o).⁴ Additionally, India is subject to the obligation to safeguard undisclosed commercial information, which is commonly referred to as "trade secrets," as a signatory to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) under Article 39.⁵ As a result, a direct conflict arises between the statutory

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

² Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

³ *Id.* at § 12.

⁴ Copyright Act, 1957, § 2(o), No. 14, Acts of Parliament, 1957 (India).

⁵ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh

mandate to erase personal data and the statutory and treaty-based mandates to preserve the structural integrity of copyrighted databases and commercial trade secrets.

RESEARCH METHODOLOGY

The primary methodology in this research involves a thorough statutory examination of the current legislative frameworks in India, notably the Digital Personal Data Protection (DPDP) Act, 2023 and the Copyright Act, 1957. The domestic framework is considered along with India's international treaty commitments, in particular, Article 39 of TRIPS Agreement on protection of undisclosed commercial information. The research uses a comparative methodology, taking advantage of the strong regulatory framework of the General Data Protection Regulation (GDPR) of the European Union, to fill the jurisprudential void in Indian law concerning the balancing of data privacy and intellectual property. The research systematically evaluates landmark decisions of the Court of Justice of the European Union (CJEU) to distil a proportionality framework that can be transplanted into the Indian context. The methodology further encompasses an analysis of standard corporate Terms of Service and Data Processing Agreements regarding data deletion and anonymisation practices to connect legal theory with management practice. The findings and harmonisation strategies suggested in this paper are derived from the synthesis of these primary statutes, international treaties, judicial precedents and industry practices.

THE STATUTORY ARCHITECTURE OF ERASURE IN INDIA

To appreciate the full scope of the conflict between privacy and intellectual property, a breakdown of the statutory mechanics of the right to erasure as set out in India's principal data protection statute is necessary. With the Digital Personal Data Protection Act, 2023, Indian law undergoes a paradigm shift from a largely unregulated digital space to a strict consent-based compliance regime, overseen by the Data Protection Board of India.⁶ The legislation is applicable to the processing of digital personal data within the territory of India and imposes severe financial penalties for non-compliance, with the maximum penalty being Rs. 250 crores for significant breaches.⁷ The DPDP Act's Section 12 is the foundation of a Data Principal's control over their digital footprint, ensuring that they have the right to correct, complete, update, and erase their personal data.⁸ Unless retention is strictly necessary for compliance

Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS Agreement].

⁶ Digital Personal Data Protection Act, *supra* note 2, at § 18.

⁷ *Id.* at Schedule.

⁸ *Id.* at § 12(1).

with any law currently in force or for the specified purpose for which it was originally collected, the Data Fiduciary is required to erase personal data upon receiving a request for erasure.⁹ Moreover, Section 8(7) imposes a proactive duty of storage limitation, requiring the fiduciary to delete personal data as soon as it is reasonable to assume that the specified purpose is no longer being served.¹⁰

The absence of an explicit, dedicated exemption for the preservation of a Data Fiduciary's intellectual property or trade secrets within the erasure provisions themselves is the central legal friction within these sections. The statute requires that the data be purged when the purpose is served, or when an individual withdraws consent and asks for erasure.¹¹ But within enterprise software and predictive analytics, personal data rarely lives in isolated silos. The entire database's utility could be diminished by the necessity of unravelling intricate relational schemas in order to erase the data of a specific individual. Thus, Section 7 of the DPDP Act is commonly used as a defensive tool by Data Fiduciaries, as it permits "certain legitimate uses" of processing personal data without explicit consent.¹² Processing is permitted for "purposes of employment or those related to safeguarding the employer from loss or liability, such as the prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, and classified information" under Section 7(i). This provision is of the utmost importance.¹³ This explicit addition gives businesses a statutory anchor.¹⁴ An enterprise could contend that the refusal to delete the data of a former executive is a legitimate processing activity that is essential for the preservation of a trade secret, as the definition of "processing" under Section 2(x) includes storage and retrieval.¹⁵ However, Section 7(i) functions as an exception to consent, but it does not entirely neutralise the overarching responsibilities of a Data Fiduciary or explicitly override the right to erasure once the employment relationship has concluded.¹⁶ Attempting to use this section to justify broad, perpetual retention for commercial convenience would likely fail a proportionality test, which necessitates enterprises to establish

⁹ *Id.* at § 12(3).

¹⁰ *Id.* at § 8(7).

¹¹ Sowmya, *The Right to be Forgotten in India: A Comparative Analysis*, 3 INT'L J. LEGAL RSCH. & ANALYSIS 515, 516 (2026).

¹² Digital Personal Data Protection Act, *supra* note 2, at § 7.

¹³ *Id.* at § 7(i).

¹⁴ Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023*, GAZETTE OF INDIA, Aug. 11, 2023, at § 7.

¹⁵ Digital Personal Data Protection Act, *supra* note 2, at § 2(x).

¹⁶ *Legitimate Uses Under DPDP*, COMPLYZERO (Dec. 18, 2025), <https://www.complyzero.com/blog/legitimate-uses-under-dpdp>.

a direct, inseparable connection between the data and the survival of the trade secret.¹⁷

COPYRIGHT AND THE STRUCTURAL INTEGRITY OF DATABASES

A company's assertion that data erasure would compromise its intellectual property is predicated on the safeguards that are afforded to curated information systems. The erasure mandate of the DPDP Act is in direct conflict with the robust protection of the structural architecture of a database in India, as stipulated by the Copyright Act, 1957. The unique selection, coordination, and arrangement of data hold immense proprietary value, in contrast to raw, isolated data points, which are generally considered unprotectable facts. Section 2(o) of the Copyright Act offers a comprehensive definition of a "literary work," specifically indicating that it encompasses "computer programs, tables, and compilations, including computer databases".¹⁸ This statutory inclusion guarantees that the architectural schema, relational links, and the specific curation of data points within an enterprise system are acknowledged as protectable intellectual property.¹⁹

Copyright protection is not automatically conferred upon a database by the mere expenditure of financial capital to compile it. The Supreme Court of India in the landmark judgment of *Eastern Book Company v. D.B. Modak* laid down the bar for originality in Indian copyright law.²⁰ The traditional "sweat of the brow" doctrine was definitively rejected by the Court, which assessed whether copy-edited versions of judicial pronouncements constituted original literary works.^{21, 22} Rather, the Supreme Court implemented a middle-ground standard that necessitates the author to exhibit the exercise of independent "skill and judgment" that contributes a minimal amount of creativity to the work.^{23, 24} Although the standard of creativity does not need to be excessively high, it must be more than a trivial variation or a purely mechanical exercise.²⁵ By applying this standard to the contemporary Database Dilemma, the performance analytics matrix of an enterprise can effortlessly surpass the threshold of originality. The algorithms and structural hierarchy of the data are a significant demonstration

¹⁷ Shreyas, *Eyes Everywhere: The Erosion of Employee Privacy Under the DPDP Act*, VIDHI CTR. FOR LEGAL POL'Y (2025), <https://vidhilegalpolicy.in/blog/eyes-everywhere>.

¹⁸ Copyright Act, *supra* note 4, at § 2(o).

¹⁹ *Copyright Protection in India for Startups*, TREELIFE (2023), <https://treelife.in/legal/copyright-protection-in-india-for-startups>.

²⁰ *Eastern Book Co. v. D.B. Modak*, (2008) 1 SCC 1.

²¹ *Id.* at 5.

²² *Id.* at 7.

²³ *Id.* at 9.

²⁴ *Id.*

²⁵ *Eastern Book Company & Ors. v. D.B. Modak & Anr.*, LAW FOYER (2023), <https://lawfoyer.in/eastern-book-company-ors-v-d-b-modak-anr-air-2008-sc-809-2008-1-scc-1-2008-air-scw-49>.

of structural creativity and technical proficiency.²⁶ The author is granted the exclusive right to create any adaptation of the work if a database qualifies as an original literary work by Section 14 of the Copyright Act.²⁷ When a Data Principal exercises their right to erasure under the DPDP Act, they are essentially compelling the Data Fiduciary to modify a copyrighted work. In databases that are highly interdependent, the deletion of a primary node can result in the disruption of internal cross-references and a fundamental change in the "selection and arrangement" that provided the database with copyright protection. While Section 52 contains "fair dealing" provisions, there is no explicit exception for alterations made to implement a data principal's privacy request, leaving a legal void that has yet to be definitively addressed by the courts.²⁸

THE COMMERCIAL SANCTITY OF UNDISCLOSED INFORMATION

The assertion of trade secrets is the most potent intellectual property defence an enterprise possesses against an erasure request, in addition to copyright protection for structural schema. India is a signatory to the TRIPS Agreement and a member of the World Trade Organization.²⁹ Article 39 of the TRIPS Agreement mandates that member states safeguard undisclosed information from being acquired or disclosed without consent in a manner that is inconsistent with truthful commercial practices.³⁰ Information that qualifies as a trade secret must be secret, have commercial value due to its secrecy, and be subject to reasonable measures to maintain its secrecy.³¹ Although India does not have a specific statutory enactment for trade secrets, it strictly enforces TRIPS obligations through the application of common law principles and contract law.³² This framework is now strengthened by Section 7(i) of the DPDP Act, which acknowledges the preservation of trade secret confidentiality as a valid basis for data processing.³³

Complex, algorithmic inferences regarding employee and client behaviour are the source of the competitive advantage of the contemporary enterprise. Such a company, forced to wipe out the data of a departing executive, might suffer a catastrophic loss of commercial value. Machine learning models that have been trained on the strategic data of the executive are unable

²⁶ *Eastern Book Co. v. D.B. Modak*, (2008) 1 SCC 35.

²⁷ Copyright Act, *supra* note 4, at § 14.

²⁸ *Id.* at § 52.

²⁹ TRIPS Agreement, *supra* note 5.

³⁰ *Id.* at art. 39(1).

³¹ *Id.* at art. 39(2).

³² *Understanding Digital Data Protection in India: Key Frequently Asked Questions*, ACUITY LAW (2025), <https://acuitylaw.co.in/faqs/understanding-digital-data-protection-in-india-key-frequently-asked-questions-faqs>.

³³ Digital Personal Data Protection Act, *supra* note 2, at § 7(i).

to "forget" a single data point without undergoing "machine unlearning." This process is computationally expensive, mathematically imprecise, and frequently necessitates the complete destruction and retraining of the model from scratch, thereby effectively destroying the intellectual property.³⁴ As a result, enterprises contend that the absolute enforcement of the right to erasure would lead to the disproportionate destruction of undisclosed commercial information that is protected under international law, thereby violating the very essence of the TRIPS Agreement.

THE EUROPEAN BLUEPRINT ON DATA PRIVACY AND TRADE SECRETS

Indian legal practitioners must seek guidance from mature jurisdictions due to the DPDP Act's nascent regulatory framework and its absolute language. The definitive blueprint for reconciling intellectual property rights with data privacy is the EU's GDPR and the corresponding jurisprudence of the CJEU. The conflict between intellectual property and privacy is specifically anticipated by the GDPR. The right to obtain a copy of personal data "shall not adversely affect the rights and freedoms of others," as stated in Article 15(4).^{35, 36} Recital 63 specifies that this encompasses "trade secrets or intellectual property, and in particular the copyright that safeguards the software".³⁷ Nevertheless, European regulators have consistently maintained that the mere invocation of a trade secret is not a magical incantation that relieves a data controller of their privacy obligations.

The CJEU addressed the scope of a data subject's rights when they intersect with proprietary methodologies in the landmark case of *F.F. v. Österreichische Datenschutzbehörde and CRIF GmbH* (C-487/21).³⁸ In order to safeguard its proprietary credit-scoring methodologies, CRIF, a credit rating agency, declined to provide structural extracts from its database.^{39, 40} The Court of Justice of the European Union (CJEU) asserted that the General Data Protection Regulation (GDPR) necessitates a "faithful reproduction or transcription of an original" and confirmed that algorithmic conclusions and derived data pertaining to an individual are considered personal.^{41, 42} Consequently, the controller is unable to withhold an assessment solely on the

³⁴ *DPDP Act for HR Teams: Employee Data*, JUNTRAX (2025), <https://juntrax.com/blog/dpdp-rules-employee-data>.

³⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 [hereinafter GDPR].

³⁶ *Id.* at art. 15(4).

³⁷ *Id.* at recital 63.

³⁸ Case C-487/21, *F.F. v. Österreichische Datenschutzbehörde*, ECLI:EU:C:2023:369 (May 4, 2023).

³⁹ *Id.* at ¶ 20.

⁴⁰ *Id.* at ¶ 21.

⁴¹ *Id.* at ¶ 28.

basis that it was generated by a proprietary system.⁴³ Nevertheless, the Court concurrently acknowledged the constraints imposed by Article 15(4), reaffirming that the right of access must be reconciled with third-party rights, such as trade secrets.^{44, 45} The operational conclusion is that an enterprise is required to provide meaningful access or erasure, but it is allowed to withhold the underlying mathematical formula if doing so would significantly compromise a trade secret.⁴⁶ A critical mechanism for the separation of personal data from proprietary analytical frameworks is provided by an earlier CJEU decision, Joined Cases C-141/12 and C-372/12 (*Y.S. v. Minister voor Immigratie*).⁴⁷ While raw data points regarding an applicant were considered personal data by the Court, the legal analysis that was conducted on these facts was not.^{48, 49} The Court concluded that the methodology's definition as personal data would unreasonably broaden privacy legislation.⁵⁰ Courts can safeguard privacy without mandating the destruction of trade secrets by legally separating the data from the architecture.⁵¹

FINDINGS

The research has produced a number of critical findings that address the legal impasse of the Database Dilemma. First, an absolute interpretation of the right to erasure under Section 12 of the DPDP Act would directly contradict the protections afforded to sui generis databases under Section 2(o) of the Copyright Act and the preservation of commercial information under TRIPS Article 39. The strict adherence to one regime results in the violation of another in the absence of judicial harmonisation. Second, the jurisprudential standard derived from European frameworks imposes on fiduciaries a rigorous three-part proportionality test before rejecting an erasure request. This involves establishing that no less restrictive technological alternative exists, demonstrating severe prejudice to the structural integrity of the copyrighted compilation, and establishing a direct nexus between the personal data and the trade secret.⁵²

⁴² *Id.* at ¶ 26.

⁴³ *CRIF: When a Copy of Your Personal Data Requires More Than a Data List*, DE LA TORRE REV. (May 4, 2023), <https://www.thedelatorrereview.com/crif-when-a-copy-of-your-personal-data-requires-more-than-a-data-list>.

⁴⁴ Case C-487/21, *F.F. v. Österreichische Datenschutzbehörde*, ECLI:EU:C:2023:369, at ¶ 43.

⁴⁵ *Id.* at ¶ 44.

⁴⁶ *What Changes for Data Controllers After the Italian DPA's Decision*, SIMMONS & SIMMONS (2023), <https://www.simmons-simmons.com/en/publications/cmsip0rpz0070tvty89i59p940/what-changes-for-data-controllers-after-the-italian-dpa-s-decision>.

⁴⁷ Joined Cases C-141/12 & C-372/12, *Y.S. v. Minister voor Immigratie*, ECLI:EU:C:2014:2081 (July 17, 2014).

⁴⁸ *Id.* at ¶ 38.

⁴⁹ *Id.* at ¶ 39.

⁵⁰ *EU Court of Justice Clarifies the Definition of Personal Data and Scope of Access Requests*, INSIDE PRIVACY (July 17, 2014), <https://www.insideprivacy.com/international/european-union/eu-court-of-justice-clarifies-the-definition-of-personal-data-and-scope-of-access-requests>.

⁵¹ Joined Cases C-141/12 & C-372/12, *Y.S. v. Minister voor Immigratie*, ECLI:EU:C:2014:2081, at ¶ 41.

⁵² Case C-487/21, *F.F. v. Österreichische Datenschutzbehörde*, ECLI:EU:C:2023:369, at ¶ 44.

⁵³ Abstract claims of database integrity are legally insufficient to bypass statutory privacy rights.

Third, a review of corporate management practices reveals that standard industry terms of service are redefining “erasure” through irreversible anonymisation and de-identification. Consequently, the statistical validity of the trade secret is preserved without violating privacy norms, as the database schema and relational integrity are preserved by replacing personally identifiable information with generic placeholders from an intellectual property perspective. The research ultimately determines that the most viable course of action is technological harmonisation through privacy-enhancing technologies, specifically cryptographic pseudonymisation and modular artificial intelligence architectures. Upon receiving an erasure request, enterprises can perform "crypto-shredding" by substituting direct identifiers with cryptographic hashes. This process involves the deletion of the cryptographic key while allowing the unidentifiable data token to remain in the database to maintain its architectural continuity.⁵⁴

RECOMMENDATIONS

In order to reconcile the conflict between proprietary trade secrets and data erasure rights, stakeholders must implement a multifaceted strategy that includes technological, corporate, and regulatory measures. First, from a regulatory standpoint, it is important for the Data Protection Board of India to come up with clear guidelines or delegated legislation so that Section 12 of the DPDP Act is in line with the existing intellectual property protections. The Board should formally adopt a proportionality framework that is similar to the European model. This framework will require Data Fiduciaries to demonstrate a direct nexus between the requested data and the trade secret, as well as severe prejudice to the database's structural integrity, before an erasure request can be legally denied.

Secondly, at the corporate level, companies should proactively amend their Terms of Service and Data Processing Agreements. These contractual frameworks should specify the process of “erasure” as irreversible anonymisation or de-identification. Enterprises can guarantee that the relational integrity of their copyrighted compilations is preserved while statutory privacy mandates are satisfied by establishing clear contractual expectations, which involves overwriting personally identifiable information with generic placeholders.

Finally, for the technological implementation, enterprises need to integrate privacy-enhancing

⁵³ *Eastern Book Co. v. D.B. Modak*, (2008) 1 SCC 35.

⁵⁴ Shreyas, *supra* note 17.

technologies into the basic architecture. The implementation of cryptographic pseudonymisation and the transition from monolithic data storage to modular artificial intelligence architectures will enable organisations to execute crypto-shredding. This harmonises compliance with both the DPDP Act and the Copyright Act by guaranteeing the permanent inaccessibility of a data principal's information without necessitating the physical destruction of the underlying algorithmic models or relational database schemas.

CONCLUSION

The conflict between proprietary trade secrets and data erasure rights is a significant philosophical and legal clash between the enterprise's right to commercial property and the individual's right to digital self-determination. The DPDP Act, 2023 is a landmark in protecting the privacy rights of Indian citizens, but it leaves a lot of room for doubt on the issue of protection of intellectual property. The blanket exceptions like Section 7(i) carry the burden of complex commercial realities. Simultaneously, the Copyright Act, 1957, provides strong protection to the structure of arrangement of databases and international obligations under TRIPS require full protection of undisclosed information. Forcing a company to indiscriminately extract data from a highly engineered relational matrix poses a threat to the very "skill and judgment" that intellectual property law is designed to safeguard.

However, as European jurisprudence has shown in cases such as CRIF and Y.S., this dilemma is not insurmountable. The resolution lies in a sophisticated, dual-track approach. In terms of legality, courts and regulatory boards are required to implement a rigorous proportionality test that excludes generic intellectual property defences and safeguards demonstrable, specific trade secrets through the abstraction of analysis. In order to transition from monolithic data storage to tokenised, mathematically abstract architectures, enterprises must re-engineer their systems and Terms of Service from a technological and contractual perspective. This will enable data to be cryptographically severed or irreversibly anonymised without compromising the structural integrity of the intellectual property it is contained within. By integrating the absolute privacy mandate of the DPDP Act with the architectural protections of the Copyright Act, India can create a formidable digital ecosystem that respects the dignity of the individual without stifling proprietary innovation of the enterprise.