

---

# PRIVACY VS. PROPERTY: RECONCILING DPDP ERASURE WITH DATABASE COPYRIGHT IN INDIA

---

Jaynam Shah, B.Com & LL.B., SVKM's Jitendra Chauhan College of Law, University of  
Mumbai

Adv Sanika Kurlekar, B.Com & LL.B., Padmashree Dr DY Patil University

## ABSTRACT

The emergence of the digital economy has rendered structured databases valuable business assets for companies active in industries like finance, healthcare, retail, technology and research. Computer databases and compilations are classified under the category of 'literary works' in India's copyright regime in case of the necessary originality of selection or arrangement. Further, the DPDP Act 2023 provides statutory rights and duties regarding the processing of personal data records, including consent withdrawal and erasure. Thus, the relationship between the two legal regimes poses an interesting legal and commercial question of what would happen to the usefulness and value of a database in case of the illegality of further processing or erasure of the personal-data records in it. In this article, it is argued that the problem is not one of the direct destruction of the copyright by data protection law, because copyright arises from the originality of selection or arrangement of the records in the database, while DPDP Act regulates processing of the personal data records. However, deletion might change the structure, completeness, analytic utility and economic value of the database. While Section 38 of DPDP Act provides the rule of conflict with other laws, there is no detailed statutory framework dealing with the intellectual property issues, contractual considerations, valuation issues, and technical implications of database thinning. The article thus outlines ways that include privacy-enabled database design, consent mechanism and data lineage system, contractual arrangements in data-driven transactions, anonymization standards, and improvements to research and archival aspects.

**Keywords:** DPDP Act 2023, database copyright, consent withdrawal, erasure, personal data, Section 38, Section 8(7), Section 12, anonymisation, data assets.

## INTRODUCTION

Data has become an essential element in contemporary commercial activities. Businesses gather, organize and analyze data related to their customers, transactions, behavior, usage and operational practices. Such data can be used for marketing, risk assessment, research, innovation, artificial intelligence and many other business purposes. Thus, organized databases may have considerable commercial value.

Under Indian law on copyright, computerized databases are included in the definition of “literary work” under Section 2(o) of the Copyright Act, 1957<sup>1</sup>. Protection under Section 13 of the Act covers original literary works, provided that such protection meets the requirements set forth in the Act. It is important, though, that the copyright in such cases does not imply protection of all facts or items of information included in the databases.

The decision of the Supreme Court of India in *Eastern Book Company v. D.B. Modak*<sup>2</sup> is very significant in this regard. The Court did not support the so-called “sweat of the brow” doctrine and stated that a compilation should contain some amount of intellectual effort in its selection, coordination or arrangement in order to qualify for copyright protection. The underlying facts do not become copyrighted only because somebody has collected them.

However, the regime regulating personal data has another set of considerations. In *K.S. Puttaswamy v. Union of India*<sup>3</sup>, the Supreme Court held that the right to privacy is a fundamental right related to dignity and autonomy. Later, DPDP Act<sup>4</sup> created statutory regulations regarding the processing of digital personal data and provided rights for Data Principals, such as the right to withdraw consent where the processing is based on consent.

Thus, the actual legal question at hand is a little more complicated than the opposition between “corporate property” and “individual privacy.” While the company holds a copyright on its compilation, this does not necessarily mean that it owns the personal data as such. Similarly, the withdrawal of consent and removal of personal data do not necessarily mean that the copyright on the remaining compilation is extinguished.

---

<sup>1</sup> The Copyright Act, 1957

<sup>2</sup> *Eastern Book Co. v. D.B. Modak*, (2008) 1 S.C.C. 1 (India).

<sup>3</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

<sup>4</sup> The Digital Personal Data Protection Act, 2023

The more concrete question is whether the exercise of the right for data protection can have any impact on a commercially valuable database and, if so, whether there are enough means in Indian law to handle that impact.

In this article, we analyze that question from the doctrinal and practical perspective.

## **RESEARCH QUESTIONS, OBJECTIVES AND METHODOLOGY**

### **A. Research Questions**

The research focuses on the following main issues:

1. What effect can withdrawal of consent and erasure provisions of the DPDP Act have on the commercial value of databases that might be protected by copyright?
2. Does Indian law make sufficient distinction between copyright protection of the original selection or compilation of a database and provisions concerning personal data within it?
3. Which technical, contractual and legislative approaches may reduce the legal uncertainty without compromising the rights of Data Principals?

### **B. Objectives**

The main aim of the research is to assess the interaction of Indian copyright legislation and DPDP Act with regard to commercial databases containing personal information. The other objective of the research is to examine practical problems related to data deletion and data processing operations and offer solutions that would balance the privacy obligations and commercial interests.

### **C. Methodology**

This research will follow a doctrinal/analytical approach. It will consider the Copyright Act of 1957, the DPDP Act of 2023, the DPDP Rules of 2025, case law and the statutory provisions regulating contractual frustration<sup>5</sup>. Hypothetical examples will be provided to show possible

---

<sup>5</sup> The Indian Contract Act, 1872

implications for practice. The research is prospective as well, since DPDP Act comes into effect gradually.

## **COPYRIGHT IN DATABASES AND THE LIMITS OF PROTECTION**

### **A. Section 2(o) and Section 13 of the Copyright Act**

Computer databases and compilations fall within the category of “literary work” as per Section 2(o) of the Copyright Act. But it needs to be remembered that the copyrightability of a work is subject to the satisfaction of certain requirements of Section 13, amongst other things, including originality.

This is very important from the perspective of business operations based on large-scale collection of data. A company can create thousands or millions of factual records, but mere expenditure of effort and labour may not necessarily mean creation of a copyrightable work in each item of data.

This has been made clear by the Supreme Court in its ruling in *Eastern Book Company v. D.B. Modak* where the requirement of originality for copyright in compilation of facts has been decided. It was held that it is only a compilation resulting from application of skill and judgment that will qualify as a copyrightable compilation. The Court has accepted that there is a difference between the facts collected by a company and the compilation of the same.

Therefore, the subject matter of legal protection may be the selection, coordination and arrangement of information as against the proprietary rights in the information.

### **B. Copyright Does Not Amount to Ownership of Personal Data**

The current debate should, thus, not describe a corporation as the owner of all personal data simply on account of the data being present in the corporate database.

Copyright and data protection laws deal with distinct areas of law. Copyright deals with original expressions that are protected while the Data Protection and Privacy Act deals with processing of digital personal data and has statutory obligations on Data Fiduciaries and their processors.

This means that a corporation may have copyright on the structure of a database while at the

same time having a legal obligation to desist from processing some personal data records in the database.

## **THE DPDP ACT: CONSENT WITHDRAWAL AND ERASURE**

### **A. Withdrawal of Consent**

Under Section 6(4) of the DPDP Act, a Data Principal is entitled to withdraw his consent if such consent serves as the legal basis for the processing, the same being as easy to withdraw as to give such consent.

But Section 6(5) allows the processing that has taken place prior to the withdrawal to remain valid. Also, Section 6(6) makes it compulsory for the Data Fiduciary to terminate such processing if consent is withdrawn by him within a reasonable time, unless such processing is justified on some other ground under the DPDP Act, Rules or other law.

Hence, the withdrawal of consent cannot be termed as an absolute right to delete all records irrespective of the justification for retaining or processing them.

### **B. Erasure**

Section 8(7) deals with the obligation of erasure upon ceasing to process, and it has an exception where retention is required for purposes of complying with the law. It further requires that the Data Fiduciary causes its Data Processor to erase personal data provided for processing, in accordance with the relevant statutory provisions.

Section 12 on its own gives the Data Principal the right to correction and erasure of personal data under certain conditions, still within the statutory constraints.

An important clarification regarding the article at hand must thus be made: Section 8(6) does not confer the downstream obligation of erasure. Rather, it relates to the issue of notifying about personal data breach. The obligation of erasure by the Data Processor is provided in Section 8(7).

### **C. Section 38 and the Relationship with Other Laws**

The presence of Section 38 is particularly significant in relation to the research problem since

it stipulates that while the DPDP Act applies alongside other legislation, in the event of any clash, then the DPDP Act takes precedence in so far as the clash is concerned.

In other words, there is no total absence of Indian law in relation to precedence between the DPDP Act and other legislation.

What emerges as a much stronger argument is that Section 38 provides a general conflict rule, but not an elaborate one dealing with the database and the economic, intellectual property, and contractual implications of deletion.

This distinction makes the research much more legally precise.

### **IS THERE A REAL STATUTORY GAP?**

The Copyright Act provides provisions regarding copyright in compilations and databases. The DPDP Act provides rights and obligations concerning digital personal-data processing. Neither of these regimes explicitly addresses the question of how a commercially valuable database is treated when some personal-data records stored therein need to be deleted.

Let us assume that there is a database with 500,000 records of customers. Let us assume that the selection, coordination, and arrangement of data contained therein fulfill the originality requirement and qualify it for copyright. In case 100,000 people who have agreed to participate in it exercise their right of erasure, the database will become smaller and less commercially valuable.

There are at least three possible effects of this.

1. The completeness of the database will decrease. Some historical or demographic segments of the database may become less representative.
2. analysis utility will decrease. Continuous and voluminous models may become less effective.
3. The commercial value of the database may decrease. The database which was licensed or valued on the basis of its volume and completeness may lose its economic rationale.

None of these outcomes means that copyright ceases to exist.

This is the main point made by the author of this article:

**It is possible that the deletion of information in accordance with the law will diminish the commercial value of the database protected by copyright without destroying the copyright in the qualifying original compilation.**

In other words, the regulatory void relates to the control of the consequences of the decay of databases, and not the incompatibility of the property rights.

## **OPERATIONAL AND COMMERCIAL CONSEQUENCES**

### **A. Structural Changes to Databases**

Modern databases are living things. Records might be related to identifiers, classifications, indexing, relationships, and analysis. Deletion of records results in transformation of the database itself.

Nevertheless, transformation does not necessarily imply the termination of copyrightability of the database. The law of copyright does not require constant presence of every underlying factual entry in order to grant copyright.

The more logical approach here is that deletion could have influence on the functionality and economic importance of the database, whereas copyright of the selection and the arrangement of the database remains untouched.

### **B. Downstream Processors**

The challenge becomes greater when the data has been processed by third parties.

In a contemporary business environment, there could be a Data Fiduciary, cloud computing provider, analytics firm, marketing firm, research institute, and many others. A withdrawal or deletion request would require more than just deleting a single row in one central database.

The processor obligations under the DPDP framework mean that a practical need exists for firms to know where their personal data has been transmitted and to ensure that they have the ability to implement cessation and deletion requirements on the data.

It follows, therefore, that there is a compelling reason for implementing data lineage tools that will capture the information about where, why, how, and when personal data was processed.

### **C. Mergers and Acquisitions**

Data intensive M&A transactions present yet another significant issue.

For instance, consider a situation in which Company A buys HealthTech company and the transaction in question is partially motivated by the ability to acquire access to a huge database that includes personal health information.

In the case when a significant amount of the data will be made unavailable due to certain data protection laws, the commercial value of the transaction in question may be adversely impacted.

Nevertheless, it is quite premature to say that Section 56 of Indian Contract Act necessarily gives rise to frustration and protects the seller in any way.

Thus, in *Satyabrata Ghose v. Mugneeram Bangur & Co.*<sup>6</sup> The Supreme Court described frustration as discharge by supervening impossibility or illegality and stressed that the issue of contractual frustration always depends on the context and on the nature of the supervening event.

A more realistic approach is to allocate risks between the contracting parties in the contract itself.

There may be various representations and warranties in data intensive transactions regarding:

- data source;
- legality of collecting and processing data;
- requests for data deletion/withdrawal;
- processor arrangements;

---

<sup>6</sup> *Satyabrata Ghose v. Mugneeram Bangur & Co.*, A.I.R. 1954 S.C. 44 (India)

- data retention obligations;
- expected data attrition; and
- valuation assumptions.

## **PHASED COMMENCEMENT AND THE PROSPECTIVE NATURE OF THE ISSUE**

It should be noted that one of the main drawbacks of the current analysis is the phased implementation of the DPDP Act.

The Commencement Notification issued by the Central Government on 13 November 2025<sup>7</sup> introduced into effect some of the provisions, including Section 38. Other substantive provisions, namely Sections 3-5, except for Clause (b) of Section 5; Sections 6(1)(a)-(f), 7, 8, 9, 10, 11 to 17, were intended to enter into effect eighteen months after publication of the Notification.

Thus, as of September 2026, the substantive provisions on consent withdrawal, processing and erasure examined in this article are predominantly being studied in the context of developing a compliance framework, not the one which gave rise to a considerable amount of Indian judicial precedents.

## **PRACTICAL SOLUTIONS**

### **A. Privacy-Preserving Database Architecture**

One solution is to split direct identifiers from analysis datasets whenever this is feasible.

The identity layer can hold names, contact details, and other identifiers alongside the records of consents and legal basis for processing.

The analytical layer can hold data that are processed statistically or operationally using appropriately controlled identifiers.

---

<sup>7</sup> Ministry of Electronics and Information Technology, Notification S.O. 4930(E), Gazette of India, Extraordinary, Part II, Sec. 3(ii) (Nov. 13, 2025).

In this manner, deletion would become much more straightforward.

But there is a necessary caveat to consider: deletion of an encryption key is not the same thing as anonymization per se.

Encryption and pseudonymization can decrease accessibility or identifiability risk, but still the retained data may qualify as personal data as long as it is reasonably possible to identify or link a person.

Therefore, the goal should be proper de-identification and controlled deletion, not just destroying the cryptographic key.

## **B. Consent and Data-Lineage Management**

Businesses should maintain records showing:

**data item → purpose → legal basis → consent status → processor → location → retention period.**

When consent is withdrawn, the system should be capable of determining:

1. whether the relevant processing is consent-based;
2. whether another lawful basis permits continued processing;
3. where the information has been transferred; and
4. which records must be erased or isolated.

This would transform deletion from a manual database exercise into a structured compliance process.

## **C. Legal-Basis Classification**

Enterprises should clearly delineate between processing operations based on consent and other legitimate processing methods that can be used according to the DPDP Act.

It is especially important since revoking consent does not necessarily mean that all processing

activities will be unlawful. There are instances where processing may be conducted without obtaining consent.

Therefore, the database structure of an enterprise should be connected to the legal basis register rather than only to the consent register.

#### **D. Contractual Protection for M&A and Licensing**

Data-intensive business deals need to take into account the fact that the volume and utility of legal personal data will vary from time to time.

The issue can be dealt with by way of representations, warranties, indemnifications, disclosures, and price adjustment clauses concerning data.

Some examples would be disclosure of:

- number of live personal data records;
- pending deletion requests;
- data retention requirements;
- processor details;
- legitimate reasons for processing; and
- regulatory constraints.

The parties would thus be able to factor in the eventual reduction in the database as part of their price determination instead of dealing with the matter post-transaction.

#### **E. Clearer Standards for Anonymisation**

Indian law would benefit from greater clarity concerning the distinction between:

**identifiable personal data → pseudonymised information → irreversibly anonymised information → aggregate non-personal information.**

This kind of classification would enable companies to know what material is still under the ambit of the personal data requirement and what data could rightly be kept for analysis.

In any standard that will be developed in the future, re-identification should be the key criterion rather than just relying on encryption technology.

#### **F. Research, Archiving and Statistical Processing**

The original paper suggested establishing a novel exemption for research or archival databases. This suggestion should be reconsidered since an exemption already exists under section 17 in respect of processing required for research, archiving or statistical purposes under the specified conditions.

A more productive change would be a clarification of the above-mentioned framework, especially as regards:

- research financed by commercial organizations;
- longitudinal researches;
- archival databases;
- anonymization;
- storage period;
- measures against re-identification; and
- derived databases.

The objective should be to preserve legitimate research and archival functions without creating an uncontrolled exception to data-protection rights.

#### **FINDINGS AND DISCUSSION**

Four key conclusions arise from the above analysis.

1. The copyright in the database and the rights over personal data are legally separate.

Copyright may exist in the selection and/or arrangement of material, whereas the DPDP Act controls the processing of personal data in digital form.

2. withdrawal and erasure may still carry significant business consequences. The deletion of large amounts of personal data may shrink, fragment, render less useful or valuable the database as a whole.
3. The DPDP Act does not entirely ignore the interaction with other legislation. Sections 38 sets out a broad priority rule, and Sections 6 and 8 set out important rules concerning withdrawal, processing, retention and erasure. The presence of these sections suggests that it is inaccurate to claim that there exists a complete statutory void.
4. The residual problem is more focused. Indian law at present lacks any comprehensive statutory framework concerning how the attrition of personal data within the bounds of legality impacts the commercial valuation, treatment under contract and technical management of a database in which copyright might subsist.

The problem is accordingly more one of coordination and regulation rather than outright contradiction.

## **SUGGESTIONS FOR LEGAL AND POLICY REFORM**

Firstly, there needs to be clearer guidance about how the issue of personal-data erasure fits with databases of copyrightable compilations.

This will serve the dual purpose of making clear that the mere fact of deleting personal data is insufficient to invalidate copyright in a qualifying compilation, while at the same time ensuring that copyright cannot be used to stop a Data Fiduciary from fulfilling its obligations to erase.

Secondly, there needs to be a push towards more technical granularity in terms of data governance. This means that businesses need to have data maps, consent records, processor registers and systems for erasing that make it possible to isolate and delete individual entries, without destroying information that should not be deleted.

Thirdly, in commercial transactions with substantial amounts of data involved, standard contractual practice in terms of the possibility of subsequent deletion or withdrawal is needed.

Fourthly, there could be clearer standards regarding anonymisation, which will allow companies to tell which data should be erased and which has become genuinely non-personal.

Fifthly, there needs to be clarification of the research, archiving and statistics regime, rather than an attempt to introduce a blanket exemption.

## **LIMITATIONS OF THE STUDY**

It must be noted at the outset that this paper does not suggest that copyright grants the business proprietor ownership of personal data or that the destruction of personal data will automatically result in the loss of copyright of the database.

The paper restricts its discussion to the conflict between copyright of qualified databases and data protection requirements related to personal data. Further, it does not make the claim that all commercial databases will qualify for originality requirement of the Copyright Act.

Finally, the paper is prospective as the actual DPDP regime is going through different phases of implementation and no precedent by the Indian judiciary is available on the issue of conflict between DPDP deletion provisions and database copyright.

## **CONCLUSION**

The intersection of data protection and copyright of databases poses a new question for India's digital economy. On the surface, the two systems seem to have contradictory requirements on the same database, with copyright protecting qualifying original works, while the data protection system requiring the cessation of processing of personal data.

On second thoughts, however, the two legal systems have separate concerns. The copyright system protects the originality of expression and selection and/or arrangement of qualifying works; the DPDP Act covers the processing of digital personal data and gives rules regarding consent, processing and erasure.

Hence, the main question is not that the DPDP Act necessarily undermines copyright. It is rather that the lawful deletion of personal data will affect the structure, utility and economic value of the database but not necessarily negate copyright protection on the original work.

There are already means under Indian law for the management of the relation. Under section

38 of the DPDP Act, there is the principle of prioritization of the DPDP Act where conflicts arise, and in the Act itself, there are provisions on consent withdrawal, processing, erasure, processors, and exemptions. It is only in a database-specific scheme that is yet to be fully developed that the economic and operational implications of personal data attrition need to be addressed.

The proper course of action therefore should be both balanced and pragmatic. The enterprise needs to establish privacy-respecting databases, have precise systems of consent and data lineage, understand the different legal grounds for processing and incorporate data attrition into mergers and acquisitions and licensing contracts. With respect to legislations and regulations, greater clarity with regard to anonymization, derived information, research, archiving and database related consequences could prove useful.

In the future, data governance in India will need to do more than decide between privacy and business. A better course of action would be to devise systems in which lawful privacy protection can coexist alongside intellectual property rights and other legitimate commercial interests. That approach can protect Data Principals without treating every exercise of a data-protection right as the destruction of a valuable commercial asset.