
RIGHT TO ERASURE, PRIVACY AND DATA PROTECTION UNDER DPDP ACT, 2023: A COMPARATIVE STUDY OF INDIA AND OTHER JURISDICTIONS AND EMERGING LEGAL CHALLENGES

***¹Dhruv Malik, ²Dr. Chetan Trivedi**

¹LL.M. Specialisation: Criminal Law Semester 1 Faculty

²(Assistant Professor of Law)

Amity Institute of Advanced Legal Studies Amity University Noida, Uttar Pradesh.

Article Received: 23 August 2026

Article Revised: 11 September 2026

Published on: 01 October 2026

***Corresponding Author: Dhruv Malik**

LL.M. Specialisation: Criminal Law Semester 1 Faculty, Amity Institute of Advanced Legal Studies Amity University Noida, Uttar Pradesh.

DOI: <https://doi-doi.org/101555/ijrpa.8683>

ABSTRACT

This Research Article primarily focuses on the statutory Right to Erasure which is guaranteed to an individual regarding their personal data and information given under Section 12 of the Digital Personal Data Protection (DPDP) Act of 2023. It also explores certain legislative restrictions and boundaries on the Right to Erasure in India in comparison to other jurisdictions like- General Data Protection Regulation (GDPR), 2016 formulated by the European Union. While GDPR under Section 17 provides an extensive "Right to be Erasure (Right to be Forgotten)" which is aided by various legal precedents while allowing limited exceptions, on the other hand, the DPDP Act provides a highly restrictive approach which is subject to certain conditions and exceptions allowing erasure only on Withdrawal of consent by the user or Fulfilment of specified purpose or Removal of Misleading, Incorrect or Outdated Information. This Research Article is a critical doctrinal and analytical research, which highlights the emerging legal challenges and structural shortcomings in the laws including various points of contention like the multiple exemptions granted to state under Section 17 of DPDP Act, which undermines the autonomy of a person, and it also affects operational ability of Data Protection Board (DPB) which has been established under Section 18. Essentially, this article argues that although DPDP Act has been a significant step in providing Legal Recognition and Organisational Accountability for Data Protection and Digital Privacy in India, prevailing implementation gaps, executive shortcomings, and

technological complexities including Artificial Research remain key in building a resilient data privacy framework.

KEYWORDS: Right to Erasure, Privacy, DPDP Act, Data Protection Board of India, GDPR, Article -21.

INTRODUCTION

The world has seen a rapid change in the digital sphere and framework due to the increase in access to internet which has eased the facility to produce, collect, store and transmit the personal data of an individual which is available on the internet. Just like Oil was one of the most valuable commodity in the 20th century, now the personal data and information related to any person has become a valuable commodity in this century. Since everybody is sharing their lives on the internet, it is very easy to get to know about anyone from basic details like-name, picture, address and contact to highly sensitive information like financial details like the PAN Card details, biometric records and AADHAR details. All of this pose a great risk to the life and liberty of an individual since all your information could be out in the open. Numerous incidents of Data breach, like the Cambridge Analytica case¹. people doing unauthorized surveillance, and the misuse of personal details have sadly become a norm in the world Sensing the need to prevent such harm, countries around the world have been engaged in formulating systematic legal framework in order to safeguard the Fundamental Right of Privacy and to punish those violating it. The European Union is the pioneer as they enacted the General Data Protection Regulation (GDPR) in mid-2018, making it an ideal role model for other countries to replicate. India on the other hand until 2023, did not have any legislation resembling it. Although, India lacked a law specifically targeting Data Privacy and its protection, the provisions and rules provided under the Information Technology Act, 2000 provided some remedy. The Supreme Court in 2017 in the historical case of K. Puttaswamy vs Union of India, held that “the Right to Privacy as a fundamental right under Article 21 of the Indian Constitution”² which required a robust legislation and system to implement it. In 2022, a draft copy of The Digital Personal Data Protection Bill was formulated and issued by the Ministry of Information Technology which after being passed by the Parliament became The Digital Personal Data Protection Act, 2023 (DPDP Act), which is to regulate data protection and maintain data privacy in India by constituting various bodies like the Data

¹ University of Greater Manchester, "The Cambridge Analytica Scandal and What It Teaches Us,"

² AIR 2017 SC 4161

protection Board to implement it. The Justice B.N. Srikrishna Committee³, laid down the basic groundwork for the required legislation while keeping the Right to Erasure as one of the main facet of data privacy as it could prevent personal or frivolous or harmful data of an individual being leaked or allowing it to be erased from the internet by putting an obligation on the concerned entity.

In Nov 2025, the Central government notified the Digital Personal Data Protection Rules⁴. Till the sections, rules and provisions come into force in a phased manner until May 2027, the privacy regime will be regulated by the IT Act and Rules similar to the past.

STATEMENT OF PROBLEM - Section 12 of the Digital Personal Data Protection (DPDP) Act, 2023 has introduced the “Right to Erasure”, although the practical enforcement of it faces some critical legal and structural flaws that threaten to render it ineffective. For example- Broad exemptions under Section 17 allow state agencies to bypass erasure mandates, enabling indefinite data retention and profiling that undermines the Fundamental Rights to Privacy under Article 21. Also unlike GDPR of the European Union, the DPDP Act lacks explicit timelines for deletion, omits data portability, and excludes non-digital records, which results in a weaker statutory framework for maintaining data privacy and sovereignty. Also this legislation lacks a clear balancing test to settle conflicts between the Data Principal’s Right to Erasure or modification of the personal data and information and the “Fundamental Right to freedom of speech”⁵ (Article 19(1)(a)) and Right to information in the media services. Also while maintaining and keeping the historical archives.

RESEARCH QUESTIONS-

1. What are the major legal shortcomings in the Right to Erasure under DPDP Act, 2023?
2. What is the effect of the multiple state exemptions provided under Section 17 on the efficacy of right to erasure?
3. How does “Right to erasure” differ from the "Right to be Forgotten" under GDPR of the European Union?
4. How does the Fundamental Right to freedom of speech and keeping of Public Archives affect Right to Erasure?

³ Ministry of Information and Technology, “Report of the Committee of Experts on a Data Protection Framework for India: A Free and Fair Digital Economy” (2018)

⁴ Ministry of Information and Technology, “Digital Personal Data Protection Rules, 2025”, GSR 847(E) (Notified- 13 Nov, 2025)

⁵ The Constitution of India, art. 19(1)(a)

5. What are the legal and technological challenges in the enforcement of Right to erasure due to recurring technologies like the Artificial Intelligence?

RESEARCH OBJECTIVES

1. To analyse the efficacy, effectiveness, legality and enforcement mechanisms of the right to erasure under Section 12 of the DPDP Act, 2023..
2. To differentiate between the Right to Erasure under the DPDP Act and the "Right to be Forgotten" under GDPR of the European Union in order to identify gaps in the Right to Erasure.
3. To examine the conflict of the Fundamental Rights "Freedom of Speech and Expression" under Article 19(1)(a) with the request of erasure.
4. To analyse the effectiveness, autonomy, independence, duties and powers of the Data Protection Board while dealing with erasure requests.

RESEARCH METHODOLOGY- This Research Article will employ a doctrinal and comparative research methodology. The Research will primarily focus on the analysis of contemporary legal frameworks, statutory provisions, judicial precedents, Journals, Books, Relevant Committee reports and international conventions. Because the DPDP Act, 2023 is relatively new, the study will focus heavily on analytical, critical, and evaluative legal interpretation rather than empirical data collection. The study will utilize a combination of certain Primary and Secondary sources. The Legislations like- The Digital Personal Data Protection Act, 2023; Information Technology Act, 2000; Right to Information (RTI) Act, 2005; the legislation of General Data Protection Regulation (GDPR). Judicial Precedents like- *K.S. Puttaswamy*, EU's *Google Spain vs. AEPD* ⁶[2014], and other relevant high court orders. Official Reports: Law Commission of India reports, and parliamentary standing committee debates are considered a part of the Primary Sources. The Secondary Sources include various Legal journals, Books on privacy and data protection law, treatises and international law reviews.

RESEARCH HYPOTHESIS- Section 12 of the Digital Personal Data Protection Act, 2023 guarantees the statutory Right to Erasure in India, but because of expansive state exemptions its practical efficacy in protecting individual privacy is structurally limited compared to global standards like the GDPR legislation formulated by the European Union, the exclusion

⁶ [2014] Q.B. 1022 [2014] 3 C.M.L.R. 50

of data which is not digital and a systematic friction with certain Fundamental Rights like the Right to Freedom of Speech and Expression given under (Article 19(1)(a)) and Right to Information Act, 2005 while facing certain enforcement challenges created by emerging technologies like Artificial Intelligence. Although such shortcomings could be corrected with the introduction of systematic changes which are enshrined in the data privacy laws in other countries.

LITERATURE REVIEW- The academic discourse of the learned academicians around Right to Erasure given under the Digital Personal Data Protection Act, 2023 has shifted from constitutional thought to legally binding statutory implementation. Leading legal experts analyse its multiple flaws and implementation hurdles-

In Commentary on DPDP Act⁷, 2023, D.P. Mittal states that while the Act does codify the privacy after Puttaswamy, however the sole focus on the facet of digital data brings about flaws in the skeletal framework. Excluding non-digital and digitised physical records are not covered, it is not meeting the goal of achieving data sovereignty.

In his book “The Future of Human Rights”⁸, Prof. U Baxi distinguishes between institutionalized human rights and the fundamental “right to be and remain human”. He argues that “human rights must protect an individual's dignity, autonomy, and immunity against suffering or loss of identity inflicted by structures of power”. In the current age, digital records make a clone of the identity an individual which will be there indefinitely- example- any acquittal in the past, which hampers their reputation. The Right to Erasure could be an antidote to this theory and allow an individual to preserve their autonomy and to how their identity is perceived in the society.

In A Treatise and Commentary on DPDP Act⁹, 2023, Dr. K.K. Khandelwal and Apoorva K. Singh criticise the enactment while emphasizing that India's framework is hugely narrower than Article 17 of the EU GDPR.

LEGAL AND JUDICIAL ANALYSIS-

Sections 12, Section 17 and Section 8(7) of the Digital Personal Data Protection Act, 2023 (DPDP Act), form core legal framework which defines how the Right to Erasure operates in

⁷ D.P. Mittal, “Commentary on The Digital Personal Data Protection Act, 2023” (Commercial Law Publishers, Delhi, 2024)

⁸ U. Baxi, “The Future of Human Rights” (Oxford Uni. Press, New Delhi, 3rd ed., 2008)

⁹ K.K. Khandelwal, Apoorva K. Singh and Anu Singh, A Treatise and Commentary on Digital Personal Data Protection Act, 2023 (OakBridge Publishing, New Delhi, 2026)

India. They outline right to demand deletion, the company's obligation to delete, and the government's exemptions from deleting data.

Section 12 (Provides the User's Right): The Right to Erasure under Section 12 of the DPDP Act provides a legal basis for data erasure rights in India. It provides the individual rights to erase, modify, update the accuracy and legitimacy of the personal data and information held by Data Fiduciaries online. According to Section 12(1) "A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force."

Exceptions to the Right to Erasure- Section 12(1) provides the right to erasure while Section 12(3) gives certain grounds for rejecting the request. It states: "A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force." These exceptions cause great confusion and ambiguity and provide the companies an excuse to not comply. For example- there is no definition of the term "necessary" under this Act.¹⁰

Section 8(Imposes Duty on Fiduciary) - This provision puts an obligation that "a Data Fiduciary must erase personal data (and ensure its Data Processors do the same) under two conditions, unless retention is legally required: If the Data Principal withdraws consent or as soon as it is reasonable to assume that the specified purpose for which the data was collected is no longer being served". However, Section 8(7) acts independently of Section 12.

Section-17 (Exemptions) - Section 17 sets certain exemptions on Right to Erasure-

- **State & Security Exemptions:** The Central Government can exempt its agencies from erasure citing that it is not particularly in interest of security of state, sovereignty, integrity of India, public law and order.
- **Legal and Judicial Proceedings or Regulatory Inquiry:** Data cannot be erased if it is needed for enforcing legal rights, or if it is being processed by a court, tribunal, or quasi-judicial body performing a judicial function. For example- If any investigation regarding inaccuracies regarding any trading account is underway SEBI cannot comply with any request of erasure as it would make the investigation obsolete.

¹⁰ Data Secure, "Why the "Right to be Forgotten" is still hard to implement?," DPO India Blogs.

- **Legal obligation to retain data:** The RBI through its Master Direction on KYC¹¹ 2016 legally requires the preservation of KYC for a period of five years after its purpose has ceased to exist. A customer demanding the bank to delete of his KYC details is not feasible, the bank has to retain the data while informing the user about the refusal and on which legal basis the request has been declined.
- **Crime Prevention:** The Investigative agencies do not have to erase data which is or might be helpful in the prevention, detection, or investigation of any crime.

Section 15 (Data Principal Duties) - Section 15 (e), puts an obligation on the Data Principal where he "shall be permitted to provide only such information the authenticity of which can be verified," being in accordance with right to Erasure. Any failure to comply with these duties will be punishable with penalties.

LEADING CASES- The journey of Judicial Recognition of Right to Erasure in India has majorly been covered through judicial interpretation by the courts rather than an active role by the legislative body. The Judiciary has been instrumental in shaping and defining and shaping boundaries of the Right to Erasure.

Google Spain vs. AEPD (2014)¹², This case is regarded as the **Birthplace of the modern Right to be Forgotten**, EU's Court of justice held that "citizens of the European Union have the right to request search engines like Google to de-index or remove the links related to personal info which have become inadequate or are no longer relevant", this ruling serves as the foundational text cited by Indian courts to shape the analytical boundaries of how Section 12 should be executed globally.

Case- Justice K. Puttaswamy vs. Union of India (2017) – A Constitutional Bench of 9 judges held that "the Right to Privacy is a fundamental right under Article 21". Crucially, the court identified "informational self-determination"— as the right of an individual to control their dissemination of personal data an essential part of human dignity. Further, it was also recognized that a person should have the right to get their data removed if it serves no ongoing public interest, though they clarified that the right is not absolute.

Venkatesh Nayak vs. Union of India¹³ (February 2026) (Supreme Court / Pending Trial) A Writ filed under Article 32 by prominent RTI activists and media bodies (including *The Reporters Collective*), this petition directly challenges the constitutionality of multiple rules and provisions of DPDP Act. This petition specifically targets Sections 17(1)(c) and 17(2)—

¹¹ RBI, "Master Direction on Know Your Customer (KYC) Direction", 2016

¹² Google Spain vs. AEPD, Case C-131/12

¹³ Venkatesh Nayak vs. Union of India, W.P. (C) No. 178/2026

the expansive state exemptions that allow government agencies to bypass data obligations—arguing they create an unchecked state surveillance framework. It also challenges Section 44(3), which amended the RTI Act to enforce a blanket ban on disclosing "personal information," setting up a direct constitutional battleground between data erasure and data privacy with the public's right to know.

Dharamraj B. Dave vs. State of Gujarat¹⁴ (2015) – This case is considered as one of the earliest Indian case which dealt with issues related to Right to Erasure under on De-indexing and Judicial Erasure. The petitioner had already been acquitted in the case, he was seeking to remove his name from legal databases on the internet which were detrimentally affecting his reputation. This plea was not accepted as the judgments of the courts are public records which are essential for maintaining transparency and legal accountability. .

Laksh Vir Yadav vs. Union of India¹⁵ (June 2026) (Delhi High Court)-The Ruling: In a monumental 144-page judgment addressing a batch of 35+ privacy petitions, the Delhi High Court established a calibrated framework for the Right to Erasure. Justice Sachin Datta held that acquitted persons, victims of matrimonial disputes, and sexual offense survivors have a constitutionally protected right to seek the global de-indexing or masking of their personal identifiers from name-based search engine results. The Court observed that because the DPDP Act, 2023 focuses heavily on commercial fiduciaries and does not fully clarify historical court records or public archives, the broader constitutional umbrella of Article 21 must step in to fill the gaps for true erasure.

COMPARATIVE ANALYSIS- INDIA vs EUROPEAN UNION- Indian Legislators took huge inspiration from their European counterparts while enacting DPDP Act. Although the they took the liberty to not make the enactment very rigid and much less direct, behind the red tape and focusing more on the interests of the authority of the state and lesser on the people, on the other hand, GDPR considers data privacy as fundamental right which is completely absolute in nature while focusing on maintaining human dignity and autonomy. In India, the onus to begin any proceeding for modification or erasure is on the concerned person himself while in EU it is mandatory to delete or remove any data post the timeline for

¹⁴ Dharamaraj B. Dave vs. State of Gujarat, 2017 SCC Gujarat 2019

¹⁵ LakshVir Yadav vs. Union of India, 2026 Delhi High Court:4892

retention is over. Some of the key differences between DPDP and GDPR¹⁶ i.e. Right to Erasure v/s Right to be Forgotten are-

On the basis of Philosophy- DPDP Act puts emphasis on data protection while keeping the economic and business aspect in mind, it also give huge importance to national security while GDPR tries to keep the human dignity and right to autonomy at the forefront.

On the basis of catalyst behind erasure- DPDP Act allows the right to erasure when a person begins the process post withdrawing his consent or after the purpose for which the data was given has been fulfilled, under GDPR, the process of erasure triggers on its own once the time for which the data was given comes to an end.

On the basis of Exemptions- DPDP Act as per Section 17 allows the Central Government to provide exemptions to authorities which are much broader in effect if it in any way poses danger to state security, sovereignty, or public law and order, while under GDPR it is very difficult to refuse the right to erasure. The state can only deny it if its of utmost importance for example- If it affecting health services provided to the public, defence of the country or for evidence in court of law.

On the basis of Nature of Data Protected- DPDP Act only allows protection to that data which is on the internet i.e. which is collected from online or which was in physical form but later was put on the internet after digitalization, while GDPR protects all kinds of personal data which is available online of which is in physical form in the offices of the company.

On the basis of Punishment- DPDP Act does not provide any provision for compensation if an individual person sue directly in court and will have to go to the Data Protection Board while the board can inflict fines up-to two hundred fifty crores which will be given to the Consolidated Fund of India, while GDPR, the individual person can sue in court directly, also the maximum fine to be inflicted is twenty million Euros or four percent of the yearly revenue generated globally, whichever is more.

CRITICAL ANALYSIS OF THE LEGAL AND PRATICAL GAP UNDER DPDP ACT-

Judgment of Puttaswamy vs. Section 17 Exemptions- The greatest legal vulnerability of the DPDP Act lies in its compatibility with the 2017 judgment of K. Puttaswamy. The Apex Court held that “the Right to Privacy comes under the purview of fundamental right under Article 21 of the Constitution”. The court also introduced a “Proportionality Test” which

¹⁶ DPDP Consultants, "GDPR vs DPDP Act: Key Differences Explained," DPDP Consultants Blogs, available at: <https://www.dpdpc consultants.com/blog.php?id=70&title=comprehensive-comparative-analysis-of-gdpr-and-dpdp>

allowed the state to infringe with privacy as long as it satisfied the test which includes: legitimacy of aim, suitability, necessity (least intrusive means), and proportionality. But Section 17(2)(a) has overreached the test by allowing the Centre to exempt any governmental body from the breach of the provisions (ex- right to erasure) which are essential for the “sovereignty, security of the State, or public law and order”. By allowing blanket state exemptions without statutory procedural safeguards, Section 17 creates a parallel, unreviewable state database ecosystem. This structural loophole fails the *Puttaswamy* proportionality test, as it allows indefinite data retention and state profiling without providing citizens a judicial remedy for deletion.

Regulatory Conflicts and Jurisdictional Clashes-

Section 12 creates an impediment as the data stored cannot be erased if its retention is required by any other law. For Example- Reserve Bank of India (RBI) / SEBI requires the financial institutions to retain Know-Your-Customer (KYC) information and transaction logs for minimum five to ten years. A user who wants to withdraw his consent can't compel a bank to erase his personal data because it is in conflict with the financial laws. Income Tax Act, 1961 “requires corporate and individual tax records to be preserved for up to six to eight years”. Other legislations like- Prevention of Money Laundering Act (PMLA), 2002 mandates absolute data logs for banking transactions to track financial crimes. In short, the laws which prevent crime pre-emptively take down the request for erasure.

Inadequacy of Data Protection Board- This Act mandates formation of a Data Protection Board of India. However, the key leadership and members have not yet been formally appointed. The government initiated the process to fill leadership roles and invited applications for the Chairperson and board member in mid-2026. The Data Protection Board is considered as the primary quasi-judicial body which adjudicates the cases and which is conferred with the powers to conduct inquiry into any alleged breach or violations, provide any remedies, conflict befitting penalties. In the erasure context, the Data Protection Board will handle the cases where the Data Fiduciaries have failed to perform erasure duties as ordered by the board, after internal redressal and will determine whether the data is necessary to be retained or not. There is a need of specialized and technical training and legal expertise in order to meet these goals and demands and for effective functioning of the Board will require.

Right to Erasure vs Right to Freedom of Speech and Expression- The statute lacks a clear mechanism to resolve conflicts with competing constitutional rights, specifically when it is in conflict with the “Right to Freedom of Speech and Expression” under Article 19(1)(a) of the

Constitution and with the Right to Information Act, 2005. In the historic 2014 European case *Google Spain v. Agencias*, the EU Court held that privacy rights generally outweigh the financial and economic interests of the search engines when in conflict with the interest of the general public, unless the individual in question is a well-known personality and widely recognised in society. The High Courts, however, have dealt with 'Right to Erasure' on case-to-case basis, resulting in contradictory rulings:

In **Zulfiqar A. Khan vs. Quintillions Business Media**¹⁷ (2019), the High Court of Delhi in this case recognized 'Right to Erasure' as an essential element of privacy, while ordering the media company to remove the damaging articles. Conversely, in **Gujrat High Court vs. Dharamraj Bhanushali**¹⁸ (2021), the court refused to remove a public judgment from the web, ruling that judicial records are public documents and erasing them would damage archives. In **Karthik Theodore vs. Registrar General**¹⁹ (2024)- the High Court of Madras ordered that third-party legal search engines and digital databases like Indian Kanoon must remove an individual's name from the acquittal judgment. This case highlights the practical conflict between individual reputation and public records. It established that permanent digital searchability can act as a lifelong "sentence" even after legal vindication, supporting the core concept that outdated data must face extraction. Further, the DPDP Act does not codify a "public interest" or "historical archive" exception to Section 12. Consequently, the judiciary is left without a statutory balancing test to decide when personal deletion requests turn into digital censorship.

Right to Erasure vs Artificial Intelligence- DPDP Act does not provide any provisions which could guide the concerned in the situation when details of the personal data have been incorporated or fed to any model of Artificial Intelligence while training it or during daily operations. This Act doesn't bifurcate between data stored in the servers or data used to machine train the AI. The High Court of Orissa held in *Subharanshu Raut vs. State of Odisha* (2020) that it is not possible to erase the data which has been entered in the public domain, raising concerns about privacy rights, also two legal questions emerge from this problem, firstly, does erasure require only the removal of the data record from the storage systems of the entity, or does it also require the removal of the data's influence from trained models that were built using that data and secondly, what would amount to sufficient proof that an erasure request has been complied when the data has already been put in or processed

¹⁷ Zulfiqar A. Khan vs. Quintillions Business Media Ltd., 2019 SCC Del 8495

¹⁸ Dharamraj B. Dave vs. State of Gujarat, 2017 SCC Gujarat 2019

¹⁹ Karthik Theodore vs. Registrar General, W.A. (MD) No. 1911 of 2021

through a model of Artificial Intelligence.²⁰ Rather the companies should be forced to introduce Machine Unlearning which focuses on erasing specific data from a trained model without retraining the entire AI from scratch. It uses algorithmic updates to suppress or "forget" specific data points or patterns associated with an individual.

FINDINGS AND SUGGESTIONS-

1. Some kind of proportionality should be introduced to the State Exemptions under Section 17 which gives the state sweeping, arbitrary powers to avoid erasing citizen data while hiding behind vague terminologies like- "public order" or "national security" without any check and balance by the courts. The government should recommend that any authority under it which is looking to use the exemption must pass a proportionality test which was given in the Puttaswamy judgment.
2. Since the Data Protection Board has been constituted by the Union Government, it causes suspicion as to how much independent and autonomous the board would be of. The Executive should constitute the board with fixed tenure for its members and a transparent system for selection and for fixing the eligibility with no meddling from the Centre. In turn, there is a requirement of a Data Protection Authority which is both judicially independent and answerable only before the parliament.
3. There are so many vague, unclear and ambiguous words in the statute like; Reasonable Security Safeguards, Public Interest, harm, etc. There should be inclusion of certain clear and definite statutory definitions like the General Clauses Act, 1897, a statement of explanatory notes should be used to attain internationally harmonisation.
4. The private individuals are not allowed to sue companies or other entities who breach and violate their personal data under this Act. They should be conferred with right to bring civil proceedings against the violators when a significant data breach has happened or the request for erasure or modification has not been complied with even after the directions of the Board.
5. Authorities like RBI should map out the overlaps like KYC beforehand and if an erasure request comes in, the system secure the financial/KYC data until the statutory retention period expires and wipe out the rest.

CONCLUSION

The provisions regarding Data Protection and Data Privacy including the "Right to Erasure" under DPDP Act, 2023 represents a monumental leap forward for digital privacy in India, yet

²⁰ Subharanshu Raut vs. State of Odisha, 2020 SCC Ori 878

it remains a work in progress when measured against mature global benchmarks like the EU's GDPR²¹.

By the act of mixing erasure to the consent and purpose for an infinite time, the Indian law has successfully achieved a corporate-friendly, economically stable act which effectively tackles the challenges of the digital system in modern times. But, its state-centric exemptions and the refusal to include the of physical information and data while not giving an individual any chance to sue privately in a court to get compensation leave some significant room for improvement and for growth. The government and the statutory bodies like the Data Protection Board have to look into the loopholes. There is a need of maintaining legal balance between the right to privacy of an individual and the right to speak of the general public as given by the Constitution. And inclusion of essential guidelines in order to interpret confusing and ambiguous terminologies like necessary for the particular purpose which will help us to make a law which is balanced and make both the consumers and corporates happy while taking our economy to new highs.

REFERENCES/BIBLIOGRAPHY-

Books

1. D.P. Mittal, Commentary on The Digital Personal Data Protection Act, 2023 (Commercial Law Publishers, Delhi, 2024)
2. Upendra Baxi, The Future of Human Rights (Oxford University Press, New Delhi, 3rd ed., 2008)
3. K.K. Khandelwal, Apoorva K. Singh and Anu Singh, A Treatise and Commentary on Digital Personal Data Protection Act, 2023 (OakBridge Publishing, New Delhi, 2026)

Journal Articles

1. University of Greater Manchester, "The Cambridge Analytica Scandal and What It Teaches Us," available at: <https://greatermanchester.ac.uk/blogs/the-cambridge-analytica-scandal-and-what-it-teaches-us>
2. Data Secure, "Why the “Right to be Forgotten” is still hard to implement?," DPO India Blogs, April 6, 2026, available at: <https://www.dpo-india.com/Blogs/why-right-forgotten/>

²¹ Regulation (EU) 2016/678 of the European Parliament on the “protection of the natural persons with regard to processing of the personal” (General Data Protection Regulation), [2016] OJ L 129/1.

3. DPDP Consultants, "GDPR vs DPDP Act: Key Differences Explained," DPDP Consultants Blogs, available at:
<https://www.dpdpc consultants.com/blog.php?id=70&title=comprehensive-comparative-analysis-of-gdpr-and-dpdp>

Case Laws

1. Justice K Puttaswamy vs. Union of India (2017)
2. Google Spain vs. Agencia Española de Protección de Datos (2014)
3. Venkatesh Nayak vs. Union of India (February 2026)
4. Dharamaraj B. Dave vs. State of Gujarat (2015)
5. LakshVir Yadav vs. Union of India (June 2026)
6. Zulfiqar Khan vs. Quintillion Business Media (2019)
7. Gujrat High Court vs. Dharamraj Bhanushali (2021)
8. Karthick Theodore vs. Registrar General (2024)
9. Subhranshu Rout vs. State of Odissa (2020)

Statutes

1. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) [DPDP Act,2023]
2. The Digital Personal Data Protection Rules, 2025
3. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1 (GDPR)
4. The Constitution of India, 1950
5. Information Technology Act, 2000
6. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules)
7. Right to Information (RTI) Act, 2005
8. EU General Data Protection Regulation (GDPR)
9. Income Tax Act, 1961
10. Prevention of Money Laundering Act (PMLA), 2002
11. General Clauses Act, 1897

Institutional and Committee Reports-

1. Justice B.N. Srikrishna Committee
2. Ministry of Electronics and Information Technology, "Report of the Committee of Experts on a Data Protection Framework for India: A Free and Fair Digital Economy" (2018)
3. Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Notified on November 13, 2025)
4. Reserve Bank of India, Master Direction - Know Your Customer (KYC) Direction, 2016 (Issued on February 25, 2016)
5. Ministry of Electronics and Information Technology, "Invitation for Appointment to the post of Chairperson and Other Members in the Data Protection Board of India (DPBI)" (May,2026)
6. 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 (General Data Protection Regulation), [2016] OJ L 119/1.