International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 09-05-2025, Accepted: 08-06-2025, Published: 23-06-2025
Volume 11, Issue 6, 2025, Page No. 57-62

The right to be forgotten under the digital personal data protection act, 2023: A missed opportunity in India's data privacy regime

Anjani Agarwal[1], Aman Singh[2]
[1] Department of Law Dr. Bhimrao Ambedkar Law University, Jaipur, Rajasthan, India
[2] Research Scholar, Department of Law, Banaras Hindu University, Varanasi, Uttar Pradesh, India

Abstract
With reference to India's Digital Personal Data Protection (DPDP) Act, 2023, this article seeks to critically analyze the idea of the Right to Be Forgotten. It assesses the Act's omission of this right, investigates its effects on personal privacy and digital dignity, and contrasts India's strategy with international norms like Article 17 of the EU's General Data Protection Regulation, 2017. The article also analyses judicial trends in India and suggests potential legal reforms by giving particular emphasis on landmark decision such as K.S. Puttaswamy v. Union of India. By doing thus, it draws attention to the increasing demand for a well-balanced framework that protects freedom of speech and information access while preserving the right to informational autonomy. The article also addresses the difficulties in putting Right to be Forgotten into practice in a digital environment characterized by cross-border data flows, technological constraints, and a lack of thorough enforcement procedures.

Keywords: Data principal, data fiduciary, data controller, blockchain, judicial overreach

Introduction

Individual privacy has emerged as a key topic in conversations about data governance in an age where personal data is continuously gathered, processed, and shared across digital platforms. Control over personal information has become a major problem as a result of people's growing digital footprints, whether via social media interactions, online transactions, or data provided with service providers. Countries all around the globe have begun implementing extensive data protection laws that are intended to protect people's rights in response to these worries. With the passage of the Digital Personal Data Protection Act (DPDP Act), 2023, India has also started down this path, taking a big step in guaranteeing its citizens' digital privacy and autonomy. The Right to be Forgotten, or Section 12(3) of the DPDP Act, 2023, is one of the fundamental rights under the law. A greater understanding of a person's desire and ability to control the story of their digital identity is reflected in this right. It gives data principals—the people to whom personal data pertains—the authority to ask for the removal or delisting of personal data that is no longer required, has fulfilled its function, or for which consent has been revoked. The Indian setting presents distinct issues in terms of its social, legal, and technical fabric, even if it is influenced by international precedents, particularly the General Data Protection Regulation (EU's-GDPR). The DPDP Act, 2023's inclusion of the Right to be Forgotten represents a cultural and ethical advancement in addition to a legal one. It shows a change in the power dynamics between people and data fiduciaries, who decide how and why to process personal information. In the past, people had little control over the persistence or distribution of data after it was posted online or input into digital systems. This relationship frequently resulted in enduring digital traces that may have an impact on a person's reputation, future prospects, and mental health. The goal of the Right to be Forgotten is to give people back some degree of control by enabling them to distance themselves from records of data that are out-of-date, unnecessary, or possibly dangerous.

Understanding the Right to be Forgotten

Fundamentally, the DPDP Act's Right to be Forgotten gives a data principal the ability to ask a data fiduciary to stop disclosing their personal information. The necessity and proportionality principles govern the circumstances in which this privilege may be used. The data principal must, for instance, show that the information is no longer required for the original purpose for which it was gathered, that permission has been revoked, or that there are no compelling reasons to keep or use the information.
The DPDP Act defines the responsibilities of data fiduciaries and the rights of persons in an organized manner. The Indian Constitution states that the right to be forgotten is not absolute; rather, it is subject to a balancing test that considers the public interest, freedom of speech, and the legal duties of the data trustee. This equilibrium makes sure that the right fulfills its intended function of preserving privacy and individuality rather than turning into a weapon for censorship or historical revisionism.

Background

The Right to Privacy was declared a fundamental right in India under the K.S. Puttaswamy v. Union of India [1] judgment**.** The Supreme Court's majority decision, delivered by a nine-judge panel, affirmed that the right to privacy is a fundamental right that is safeguarded by the Indian Constitution. The issue was related to the Aadhaar scheme, which is a government program that assigns residents a unique identity number based on their demographic and biometric information. There have been worries expressed about possible abuse and illegal access to personal data. This prompted a broader constitutional question *Does the Indian Constitution guarantee a fundamental right to privacy?* Until this ruling, the Indian judiciary had not definitively recognized privacy as a fundamental right.

Earlier decisions, notably M.P. Sharma v. Satish Chandra [2] and Kharak Singh v. State of Uttar Pradesh [3], had either rejected or offered a narrow interpretation of privacy protections.

In the Puttaswamy case, the Supreme Court overturned previous judgments, concluding that privacy is guaranteed under Article 21 (Right to Life and Personal Liberty) since it is fundamental to life and liberty. The Court further pointed out that privacy is a multifaceted right as it is related to the freedoms protected by Articles 14 (Right to Equality) and 19 (Freedom of Expression, Movement, etc.). Body integrity, personal autonomy, protection of personal data, and decisional autonomy with regard to intimate personal choices (such as sexuality, relationships, and beliefs) are all included in privacy, the ruling stressed. The Court made it clear that the right to privacy is not unqualified, which is significant.

The state may impose reasonable restrictions on it, but these must meet three requirements: necessity (the restriction must be required to accomplish a valid state goal), legality (the action must be authorized by law), and proportionality (the extent of the restriction must be commensurate with the goal being pursued). The *Puttaswamy* judgment laid the foundation for India's modern digital privacy regime. It had far-reaching implications beyond Aadhaar—impacting data protection laws, surveillance reforms, sexual and reproductive rights, and individual autonomy. The Digital Personal Data Protection Act, 2023, was greatly influenced by this ruling, which also cleared the path for the recognition of other derivative rights, such as the Right to be Forgotten, which is today a crucial component of informational privacy.

The right to be forgotten is acknowledged everywhere, especially in the EU under Article 17 of the General Data Protection Regulation (GDPR). One important privacy protection is the protection to Be Forgotten, which enables people to ask for their personal information to be deleted when it is no longer required or pertinent for the reasons it was gathered. When the European Union (EU) implemented the GDPR in May 2018, this right became well known. Article 17 of the GDPR codifies the Right to Be Forgotten, which is officially referred to as the "Right to Erasure." Under certain conditions, it gives people—known as data subjects—the ability to ask for the erasure of their personal information that is stored by data controllers and processors. Data subjects are entitled to have their data deleted without undue delay under GDPR Article 17(1) if:

- The information is no longer required for the reason it was gathered.
- The person revokes the permission that underlies the processing.
- There are no compelling legal reasons, and the person opposes to the processing.
- The data was processed illegally.
- In order to fulfil a legal need, the data must be deleted.
- The information was gathered in connection with a child's offer of information society services.

However, the Right to be Forgotten is not an absolute right. Article 17(3) outlines exceptions where the right does not apply, such as:

- exercising the freedom of information and speech.
- Fulfilling a duty in the public interest or adhering to a legal requirement.
- For historical, scientific, or archival study.
- The creation, use, or defense of legal claims.

By striking a balance between privacy and other essential rights, the Right to be Forgotten is protected from being used as a means of censorship or historical distortion.

The concept gained public attention following the 2014 ruling of the Court of Justice of the European Union in the Google Spain v. AEPD and Mario Costeja González **[4]**. According to the court, search engines like Google are "data controllers" and are obligated to abide by legitimate requests to have their data erased, especially where such data is erroneous, irrelevant, or out-of-date. The GDPR and its Right to be Forgotten clause have had a huge worldwide impact. Brazil, South Korea, Canada, and India are just a few of the nations and territories that have researched or included such rights in their data protection legislation. For example, the Right to Be Forgotten is included by India's Digital Personal Data Protection Act, 2023, which takes conceptual cues from the GDPR framework.

Relevance in the Indian Context

India's demographic and technological diversity adds layers of complexity to the application of the Right to be Forgotten. On the one hand, the nation's digital economy is expanding quickly, as seen by rising internet usage, mobile connection, and the uptake of digital services. On the other hand, a large number of citizens might not be completely aware of their rights or the ramifications of data sharing. Given this, the definition of such a right is especially crucial since it encourages data fiduciaries to handle data in a more responsible manner while simultaneously empowering individuals.

Through programs like Digital India and the use of digital platforms for service delivery, the Indian government has also placed a greater emphasis on digital governance. Although these programs have increased accessibility and efficiency, they also need for strong privacy safeguards to stop abuse or illegal access to private information. In this context, the Right to be Forgotten is essential because it guarantees that people are not permanently confined to digital representations of their history that do not accurately reflect their present situation.

Key Issues Explored

The DPDP Act of 2023 defines the right to be forgotten. The processing of digital personal data is governed by the DPDP Act, 2023, which acknowledges both the necessity of processing such data for legitimate reasons and the right of individuals to safeguard their personal data. Although the Act does not use the phrase "Right to Be Forgotten" [5] explicitly, the right is implicitly embedded within the broader rights conferred to individuals, known as Data Principals [6].

Key Provision

Under Section 12(3) of the DPDP Act, a Data Principal has the right to "correction, completion, updating and erasure" [7] of their personal data that is either**:**

- Inaccurate or misleading,
- No longer required for the reason it was handled,
- Or where consent has been withdrawn and no legal basis for retention exists.

Therefore, the DPDP Act's Right to be Forgotten is mostly applied through the right to erasure, which allows a person to ask for the removal of personal information that has been processed illegally, is outdated, or is irrelevant. From this framework, the Right to be Forgotten under Indian law can be understood as: "A right vested in the Data Principal to request the erasure of their personal data from a data fiduciary's records, particularly where the data is no longer necessary, consent has been withdrawn, or its continued processing infringes upon the individual's privacy." [8] This right is not absolute, and it is subject to several reasonable restrictions based on public interest, legal obligation, journalistic freedom, and other competing rights.

Scope of the Right to Be Forgotten

The scope of the Right to be Forgotten under the DPDP Act involves a multifaceted understanding of how and where it can be exercised, who can request it, and what its limitations are-

1. **Eligible Persons:** Only Data Principals [9], defined as individuals to whom the personal data relates, may exercise this right. They may also do so through a consent manager or legally appointed representative in specific situations, such as minors or incapacitated persons.

2. **Entities Bound by the Right:** The right is enforceable against **Data Fiduciaries** [10], which include companies, organizations, or even government bodies that collect, store, or process personal data digitally. These fiduciaries are responsible for honoring erasure requests, subject to applicable conditions and exceptions.

3. **Conditions for Exercising the Right:** A Data Principal may request the erasure of their data if:

- The data is no longer required in connection with the purposes for which it was gathered or processed, and the purpose for which it was obtained has been satisfied.
- Consent is withdrawn by the data principal.
- There has been illegal processing of the data.

However, the data cannot be erased if it is:

- Required to adhere to any legal requirements,
- Essential for pursuing legal claims,
- Or in the public interest (for instance, for journalistic reasons, statistical analysis, or historical study).

Global Theories Supporting Privacy Based Right to be Forgotten

Legal and ethical theories across jurisdictions provide further validation for Right to be Forgotten as part of informational privacy. Alan Westin's theory of privacy as control suggests individuals should determine the extent of their personal data exposure. Helen Nissenbaum's contextual integrity theory proposes that privacy violations occur when data flows out of its original social context—in this case, when outdated information continues to circulate indefinitely online. Legal philosopher Charles Fried theory argued that privacy is necessary for maintaining human relationships and self-development.

Judicial Recognition in India

In K.S. Puttaswamy v. Union of India [11], By recognizing an individual's right to manage their digital identity and personal data, the Supreme Court established the constitutional basis for the Right to be Forgotten and ruled that the right to privacy is a basic right under Article 21.

In Dharmaraj Bhanushankar Dave v. State of Gujarat [12], Petitioner after acquittal, sought removal of online case records. However, the High Court denied it due to absence of legal backing at the time. As a result, this becomes the First Indian case to raise Right to be Forgotten, highlighted the need for a statutory framework.

In Sri Vasunathan v. Registrar General [13], Petitioner sought removal of daughter's name from an online judgment. *Karnataka High Court* allowed anonymization. As court recognized Right to be Forgotten to protect reputation and privacy in sensitive personal matters.

In Jorawar Singh Mundy v. Union of India [14], U.S. citizen acquitted of criminal charges in India sought removal of judgment from online portals. Delhi HC directed the judgment to be anonymized on Indian Kanoon. As court recognized Strongest affirmation of Right to be Forgotten; acknowledged need to protect dignity post-acquittal.

Global Perspective on Right to be Forgotten

The European Union: A Robust Framework- The General Data Protection Regulation (GDPR) of the European Union, which went into force in 2018, offers a methodical and transparent approach to the Right to be Forgotten. Under some circumstances, such as when the data is no longer required for the purposes for which it was gathered or when the individual withdraws consent that underpins the processing, Article 17 of the GDPR gives people the right to seek the erasure of personal data.

Key features of the EU's Right to be Forgotten include:

- **Scope of Application:** Regardless of the controller's location, the right is applicable to all data controllers that process the personal data of EU citizens.

- **Conditions for Erasure:** When data is erroneous, unnecessary, or handled illegally, data subjects have the right to request that it be erased.

- **Exceptions:** When processing is required to fulfill a legal requirement, exercise the right to free speech, or serve the public interest, the right is not applicable.

The EU's approach emphasizes a balanced consideration of privacy rights and other fundamental rights, ensuring that Right to be Forgotten is not exercised at the expense of public interest or freedom of expression.

Brazil

Legislative Developments and Judicial Interpretations: The right to be forgotten is not specifically acknowledged by Brazil's General Data Protection Law (LGPD), which was passed in 2018 and goes into effect in 2020. Nonetheless, the legislation gives people the ability to see, update, remove, or anonymize their personal information. These clauses provide a basis for demands similar to the Right to be Forgotten.

Notably, the Brazilian Federal Supreme Court highlighted the conflict between freedom of expression and privacy

when it decided that the Constitution does not protect a general right to be forgotten. Nevertheless, the LGPD's provisions, which are consistent with the Right to be Forgotten principles, allow people to request the deletion of personal data in specific situations.

South Korea

Cyber Defamation Laws and Data Protection: South Korea's strict online defamation laws have an impact on its Right to be Forgotten policy. Both genuine and false defamatory utterances are punishable by harsh penalties under the Information and Communications Network Act, which makes defamation over telecommunications networks illegal. The safeguarding of people's online reputations is given top priority in this framework. South Korea's cyber defamation laws allow people to seek compensation for harm they have experienced online, even if the country does not have a statutory Right to be Forgotten statute. The nation's focus on reputation protection highlights how crucial it is to protect people from online danger.

Table 1: Comparative Analysis

Jurisdiction	Recognition	Legal Basis	Key Provisions
EU	Explicit	GDPR	Under certain circumstances, people have the right to seek the deletion of their personal data under Article 17.
Brazil	Implicit	LGPD	Provides rights to access, correct, and delete personal data; Right to be Forgotten -like provisions inferred.
South Korea	Implicit	Cyber Defamation Laws	Emphasizes protection against online defamation; no formal Right to be Forgotten law.
India	Unclear	DPDP Act, 2023	Rights to access, correct, and delete personal data; Right to be Forgotten not explicitly mentioned.

Challenges and Concerns

People can ask for the removal or de-indexing of personal information that is no longer accurate, relevant, or required under the legally recognized Right to be Forgotten. Although this right is essential for safeguarding personal privacy in the digital age, there are a number of intricate issues and worries regarding its use from a legal, moral, technological, and pragmatic standpoint. However, there are difficulties in putting this right into practice. The following difficulties may arise when this right is put into practice:

1. **Conceptual Ambiguity and Legal Interpretation:** Ambiguity results from the DPDP Act's imprecise language and unclear boundaries around the Right to be Forgotten. According to Section 12(3), the data principle has the right to have personal data updated, corrected, completed, and erased, particularly where permission has been revoked or the objective has been achieved. Nevertheless, neither the right to be forgotten nor the circumstances under which it may be granted nor refused are specifically stated. This lack of detail raises important queries:
   - What qualifies as a legitimate erase request?
   - Does it apply to data that was made public prior to the law's enactment?
   - Is it possible to apply this to publicly available material like news reports or court documents?

If these issues are not resolved, there might be uneven application, ambiguity in the law, and a possible restriction on the right to free speech.

2. **Conflict with Freedom of Speech and Public Interest:** Right to be Forgotten's possible conflict with the freedom of speech and expression protected by Article 19(1)(a) of the Indian Constitution is one of the most divisive topics surrounding it. Erasing legally published personal information (such as in a news story) might undermine press freedom, restrict public access to historical documents, or impede judicial openness, particularly when public rulings include reference to personal information. Demands to remove criminal records or court rulings, even when they have repercussions for the public good, are a prime example. Such a removal may impact legal studies, skew public memory, and impair media responsibility. As a result, putting Right to be Forgotten into practice requires striking a balance between people's right to privacy and the public's right to knowledge.

3. **Absence of a Robust Adjudication Mechanism:** While the DPDP Act provides for a Data Protection Board of India [15] (DPBI), it is still an emerging institution with limited powers and undefined procedures. It remains unclear:
   - Whether the Board will have quasi-judicial authority to interpret the Right to be Forgotten and adjudicate disputes?
   - How appeals against its decisions will be managed?
   - What legal remedies will be available if a data fiduciary (entity holding the data) refuses to act on a deletion request?

4. **Technological Constraints and Practical Challenges:** The implementation of Right to be Forgotten faces several technical limitations, especially in the digital ecosystem, where data replication, caching, and archival are common. Key concerns include:

   - **Data persistence:** Data once shared may reside in multiple servers, including third-party backups and cloud systems, making complete deletion almost impossible.
   - **Indexing by search engines:** Even if content is removed from a source, it may still be accessible via search engine caches unless actively deindexed.
   - **Blockchain-based systems:** In decentralized networks, the very architecture of immutability makes it technically incompatible with data erasure.

Moreover, ensuring compliance across cross-border data flows adds another layer of complexity, especially where foreign entities are not subject to Indian law.

5. **Lack of Awareness and Digital Literacy:** The lack of knowledge among Indian users regarding their digital rights, such as the Right to be Forgotten, is another significant issue. Many people might not be aware of the procedures involved in submitting a request for data deletion, the legal foundation for their rights, or the deadlines and restrictions that go along with it. This can result in the right being underutilized or in intermediaries and data brokers abusing it. To close this gap, user-centric grievance procedures and digital literacy initiatives are crucial.

6. **Judicial Overreach and Subjective Interpretation:** Courts may be asked to interpret and uphold the Right to be Forgotten in the absence of explicit statutory instructions. Nevertheless, this may result in subjective rulings or judicial overreach. Courts may, for example, allow erasure petitions based on personal sensitivity rather than the general welfare, which can result in the suppression of reasonable criticism, the censorship of historical records, and inconsistent precedents that erode the rule of law. This also raises questions about privacy not being a basic right but rather a tool for reputation management.

7. **Global Precedents and Lack of Harmonization:** India's right to be forgotten is still in its infancy and is not in line with international standards, in contrast to the EU's GDPR, which provides a clearly defined right to be forgotten (Article 17). Cross-border data transfers, reciprocal erase request recognition, and compliance with global privacy standards are all hampered by this. This legislative heterogeneity causes regulatory uncertainty and compliance fatigue for multinational tech businesses doing business in India.

8. **Scope of Exceptions under the Law:** The DPDP Act specifies several acceptable uses of personal information, including national security, journalism, and judicial procedures. These exclusions, however, are ambiguous and wide-ranging, allowing for the capricious rejection of claims for the Right to be Forgotten. the absence of specific guidelines about what constitutes "public interest." Which information qualifies as "necessary"? And after consent, how long may data be kept? renders the application of Section 12(3) vulnerable to abuse or overuse.

Conclusion

An important turning point in India's transition to a more organized and citizen-centric data governance approach is the Digital Personal Data Protection Act, 2023. However, the Act's failure to clearly express the Right to Be Forgotten points to a serious weakness in giving people complete control over their online selves. Although the Act establishes significant procedures for data deletion upon consent withdrawal or purpose completion, these clauses fall short of establishing the Right to be Forgotten as a stand-alone right, which could serve as a crucial defense in an increasingly intrusive digital world.

With precise definitions, legal guidelines, and appeal procedures, a formal Right to be Forgotten would provide people the ability to really exercise control over personal data that is out-of-date, unnecessary, or possibly dangerous. Furthermore, the government might guarantee that petitions for erasure are fairly assessed by enshrining this right inside an open adjudicatory system, striking a balance between conflicting public interests like the right to information and freedom of speech and individual privacy.

Formally acknowledging Right to be Forgotten will also demonstrate India's adherence to international best practices, especially those delineated in the General Data Protection Regulation (GDPR) of the European Union, which has emerged as a global standard for digital rights laws. Legal harmonization becomes not only desirable but also essential for efficient enforcement and international collaboration as data moves across borders more often and global platforms operate under Indian jurisdiction.

However, India needs a context-sensitive model of Right to be Forgotten that is based on its sociopolitical realities, cultural quirks, and constitutional principles. For example, care must be taken to prevent the possible abuse of the Right to be Forgotten by influential people or organizations in order to conceal historical wrongdoings or censor public documents. This emphasizes the importance of a case-by-case strategy in which each erasure demand is examined by a judge or quasi-judiciary, taking into consideration the necessity and proportionality of data retention vs deletion.

Institutional support and regulatory clarity will be crucial going ahead. The DPDP Act's proposed Data Protection Board has to have the legal and technological know-how to decide on intricate Right to be Forgotten cases. A balanced framework that preserves democratic ideals while bolstering privacy rights may be developed concurrently with the aid of public awareness campaigns and stakeholder interaction, which includes civil society, business, and legal professionals.

In conclusion, the lack of an expressly stated Right to Be Forgotten is still a lost chance, even if the DPDP Act significantly advances the development of a rights-based approach to data protection in India. To make sure that people are not always plagued by their digital pasts, it will be crucial to close this gap through judicial development, interpretive advice, and legislative improvement. In addition to bolstering India's digital rights framework, a statutory, appropriately calibrated Right to be Forgotten will uphold the core idea that privacy is a right rather than a luxury.

Lessons for India

1. **Explicit Recognition of Right to be Forgotten:** In its data protection laws, India should think about expressly acknowledging the Right to be Forgotten and outlining precise rules for its use and restrictions.

2. **Balancing Privacy and Freedom of Expression:** India should, like the EU, make sure that the Right to be Forgotten is balanced with other essential rights, including the freedom of speech.

3. **Judicial Clarity:** To provide people and data controllers clarity, Indian courts should interpret the Right to be Forgotten consistently. Use a balancing strategy, assessing the right to information, legal openness, and the public interest versus privacy.

4. **Public Awareness:** Raising public knowledge of the right to be forgotten and data rights can enable people to successfully utilize their rights.

References

1. K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
2. K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
3. M.P. Sharma v. Satish Chandra (1954) SCR 1077.
4. Kharak Singh v. State of Uttar Pradesh (1964) SCR 332.
5. Case C-131/12 Google Spain v. AEPD and Mario Costeja González [2014] EU 317.
6. Digital Personal Data Protection Act 2023, s 12(3).
7. Digital Personal Data Protection Act 2023, s 2(j).
8. Digital Personal Data Protection Act 2023, s 12(3).
9. Digital Personal Data Protection Act 2023, s 12(3).
10. ibid.
11. Digital Personal Data Protection Act 2023, s 2(i).
12. supra
13. Dharmaraj Bhanushankar Dave v. State of Gujarat (2015) SCC Guj 223.
14. Sri Vasunathan v. Registrar General (2017) SCC Kar 424.
15. Jorawar Singh Mundy v. Union of India (2021) SCC Del 2306.
16. Digital Personal Data Protection Act 2023, s 18.