# "The Right to Be Forgotten in the Digital Age: Challenges and Omissions in the Digital Personal Data Protection Act, 2023"

**Dharmendra Kumar**

Research Scholar
School of Law and Governance

**Abstract:**
**The Right to Be Forgotten (RTBF) has emerged as a pivotal privacy right in the digital era, yet India's Digital Personal Data Protection Act, 2023 (DPDPA), lacks explicit provisions for its implementation. This paper examines the DPDPA's approach to data privacy, focusing on its omission of a robust RTBF framework, and identifies associated legal, technical, and enforcement challenges. Employing doctrinal legal research and comparative analysis with the EU's GDPR, the study evaluates gaps in the DPDPA, particularly its vague data erasure provisions (Section 8) and reliance on judicial interpretation. It argues that the absence of clear RTBF mechanisms undermines individual autonomy and fails to address the needs of vulnerable groups seeking data removal. The paper proposes legislative amendments to incorporate explicit RTBF provisions, strengthen the Data Protection Board's role, and enhance public awareness. By addressing these omissions, India can align its data protection framework with global standards, ensuring greater privacy rights in the digital age.**

**Keyboard: Right to Be Forgotten, Digital Personal Data Protection Act, Data Privacy, Informational Autonomy, Judicial Interpretation.**

## 1. INTRODUCTION:

In the digital age, where personal data is incessantly collected, stored, and shared across online platforms, the Right to Be Forgotten (RTBF) has emerged as a critical principle in data privacy.[1] The RTBF empowers individuals to request the deletion of their personal data from digital repositories, enabling greater control over their digital footprints.[2] Originating from European legal frameworks, notably the General Data Protection Regulation (GDPR), the RTBF addresses the challenges posed by persistent digital records that can haunt individuals long after their relevance.[3] In an era of widespread data breaches, profiling, and surveillance, the RTBF is a vital safeguard, ensuring individuals can mitigate risks associated with outdated or harmful personal information. Its global relevance underscores the need for robust data protection laws that balance individual rights with technological advancements.[4]

In India, the Digital Personal Data Protection Act, 2023 (DPDPA), marks a significant milestone as the country's first comprehensive data protection legislation.[5] Enacted to regulate the processing of personal data, the DPDPA aims to establish a framework for accountability, transparency, and user consent in data handling

[1] Geraldine O. Mbah, "Data privacy and the right to be forgotten." *World Journal of Advanced Research and Reviews* 16.2 (2022): 1216-1232.
[2] Sarkar Ghosh, Diya, Prafulla Chandra Mishra, and Tulishree Pradhan. "The conundrum of erasing digital footprints: A regulatory challenge." *Jindal Global Law Review* 15.1 (2024): 25-59.
[3] Politou, Eugenia, et al. *Privacy and data protection challenges in the distributed era*. Vol. 26. Cham: Springer, 2022.
[4] Renuka, Oladri, et al. "Data privacy and protection: Legal and ethical challenges." *Emerging Threats and Countermeasures in Cybersecurity* (2025): 433-465.
[5] Subhajit. Saha and Surjashis Mukhopadhyay. "A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023." *IJLS* 10 (2024): 84.

practices. It introduces obligations for data fiduciaries, rights for data principals, and penalties for non-compliance, aligning India with global data protection standards. However, a critical gap persists: the DPDPA lacks explicit provisions for the RTBF, raising concerns about its efficacy in empowering individuals to control their digital identities.[6]

This paper addresses the research problem of the DPDPA's failure to incorporate clear RTBF mechanisms, which limits its ability to protect individuals from the long-term consequences of data persistence in India's rapidly expanding digital ecosystem.

## 2. RESEARCH QUESTIONS:

1. How is the *Right to Be Forgotten (RTBF)* conceptualized under the Digital Personal Data Protection Act, 2023 compared to global standards (e.g., GDPR)?
2. What are the major challenges in enforcing the RTBF in India's digital ecosystem, particularly in the context of e-commerce, social media, and search engines?
3. What omissions or gaps exist in the DPDP Act, 2023 regarding RTBF, and how might they affect individuals' privacy rights?
4. What balance can be struck between the individual's right to privacy and the public's right to information in the context of RTBF?

## 3. RESEARCH OBJECTIVES:

1. To examine the scope and recognition of the Right to Be Forgotten under the DPDP Act, 2023.
2. To analyze the practical challenges in implementing RTBF in India's digital and technological landscape.
3. To identify legal and structural omissions in the DPDP Act regarding RTBF when compared with international frameworks like the GDPR.
4. To suggest legal and policy reforms that could strengthen the effective enforcement of RTBF in India.

## 4. METHODOLOGY:

This research adopts a doctrinal legal research approach to critically examine the Right to Be Forgotten (RTBF) within the framework of India's Digital Personal Data Protection Act (DPDPA), 2023. The methodology integrates statutory analysis, case law review, and comparative study to evaluate the DPDPA's provisions and their alignment with RTBF principles. Primary sources include the DPDPA, 2023 text, the EU's General Data Protection Regulation (GDPR, specifically Article 17), and relevant Indian court judgments. Secondary sources comprise scholarly articles, legal commentaries, and policy reports accessed through academic databases and reputable online platforms. The qualitative analysis focuses on interpreting the DPDPA's data erasure provisions against global RTBF standards, identifying legislative gaps, and assessing practical challenges through a comparative lens with GDPR. This approach enables a systematic evaluation of legal texts and judicial precedents, ensuring a robust understanding of the DPDPA's omissions and their implications for digital privacy in India. The methodology is well-suited to propose informed reforms for integrating RTBF into India's data protection framework.

## 5. THEORETICAL AND CONCEPTUAL FRAMEWORK OF THE RIGHT TO BE FORGOTTEN:

The Right to Be Forgotten (RTBF) represents a pivotal concept in data privacy law, addressing an individual's ability to request the removal of personal data from digital platforms. This framework explores its origins, jurisprudential foundations, distinctions from data erasure, comparative perspectives, and its role in balancing privacy with free speech, situating it within the context of India's Digital Personal Data Protection Act, 2023 (DPDPA).

[6] Sarkar Ghosh, Diya, Prafulla Chandra Mishra, and Tulishree Pradhan. "The conundrum of erasing digital footprints: A regulatory challenge." *Jindal Global Law Review* 15.1 (2024): 25-59.

**Origins in the European Union**

The RTBF emerged prominently in the European Union through the 2014 *Google Spain v. AEPD and Mario Costeja González* case (C-131/12).[7] In this landmark ruling, the European Court of Justice (ECJ) recognized an individual's right to request search engines to delink personal data that is "inadequate, irrelevant, or no longer relevant," establishing a precedent for RTBF under EU law. This principle was codified in the General Data Protection Regulation (GDPR, 2016), specifically Article 17, which grants data subjects the right to erasure under defined conditions, such as data no longer being necessary for its original purpose.[8] The EU's approach reflects a proactive stance on privacy as a fundamental right, rooted in the Charter of Fundamental Rights of the EU (Article 8).[9] The *Google Spain* case underscored the tension between individual privacy and public access to information, setting a global benchmark for RTBF.[10]

**Jurisprudential Basis: Privacy, Dignity, Autonomy**

The RTBF is grounded in the jurisprudential principles of privacy, dignity, and autonomy.[11] Privacy, as a fundamental right, protects individuals from unwarranted intrusion into their personal lives, a concept reinforced globally through cases like *K.S. Puttaswamy v. Union of India* (2017) in India, which recognized privacy as intrinsic to Article 21 of the Indian Constitution.[12] Dignity, closely tied to privacy, emphasizes an individual's right to control their digital identity, preventing harm from outdated or harmful data.[13] Autonomy underpins RTBF by empowering individuals to shape their personal narratives, particularly in the digital age where data permanence can perpetuate reputational damage.[14] These principles collectively frame RTBF as a mechanism to restore agency over personal information, aligning with human rights frameworks that prioritize individual control in data-driven ecosystems.

**Distinction Between RTBF and Data Erasure**

While often conflated, RTBF and data erasure are distinct. RTBF specifically refers to the right to have personal data delinked or removed from publicly accessible platforms, such as search engine results, without necessarily deleting the data from all databases.[15] For instance, in the *Google Spain* case, the ECJ mandated delinking data from search results, not erasing it from original sources.[16] Data erasure, as outlined in GDPR's Article 17 or DPDPA's Section 8, involves the complete deletion of personal data by data controllers or fiduciaries. RTBF is narrower, focusing on accessibility rather than total erasure, and is often subject to

[7] Sobkow, Beata. "Forget Me, Forget Me Not-Redefining the Boundaries of the Right to Be Forgotten to Address Current Problems and Areas of Criticism." *Annual Privacy Forum*. Cham: Springer International Publishing, 2017.

[8] General Data Protection Regulation (EU) 2016/679, Article. 17.

[9] Brkan, Maja. "The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning." *German Law Journal* 20.6 (2019): 864-883.

[10] Youm, Kyu Ho, and Ahran Park. "The right to be forgotten: google Spain as a benchmark for free speech versus privacy?." *Chi. J. Int'l L.* 24 (2023): 166.

[11] Anujay. Shrivastava, "The origins, jurisprudential fallacies and practical limitations of a 'Right To Be Forgotten'in the European Union." *International Journal of Law and Policy Review* 10.2 (2021): 153-203.

[12] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[13] Whitman, James Q. "The two western cultures of privacy: Dignity versus liberty." *Yale LJ* 113 (2003): 1151.

[14] Blockchains, Permissioned. "Erasing the Trace: Challenges of the Right to Be Forgotten in Healthcare Private." (2025).

[15] Mueller, Milton. *Will the internet fragment?: Sovereignty, globalization and cyberspace*. John Wiley & Sons, 2017.

[16] Sobkow, Beata. "Forget Me, Forget Me Not-Redefining the Boundaries of the Right to Be Forgotten to Address Current Problems and Areas of Criticism." *Annual Privacy Forum*. Cham: Springer International Publishing, 2017.

balancing tests against public interest or free speech.[17] The DPDPA's data erasure provisions lack the specificity of RTBF, creating ambiguity in addressing public-facing data removal requests.

**Comparative Perspective: EU, USA, UK, Canada**

The EU's GDPR provides the most robust RTBF framework, with clear criteria for data deletion and enforcement mechanisms.[18] In contrast, the United States lacks a federal RTBF law, relying on limited state-level regulations (e.g., California's Consumer Privacy Act) and First Amendment protections, which prioritize free speech over data removal.[19] The UK, post-Brexit, retains GDPR-aligned RTBF provisions under its Data Protection Act 2018, though with slight modifications to reflect national priorities. Canada's approach, through the Personal Information Protection and Electronic Documents Act (PIPEDA), implies RTBF-like rights but lacks explicit codification, relying on case-by-case interpretations.[20] These variations highlight the challenge of harmonizing RTBF globally, particularly in jurisdictions like India, where the DPDPA omits explicit RTBF provisions, relying instead on judicial interpretations (e.g., *Zulfiqar Ahman Khan v. Quintillion Business Media*, 2019).[21]

**Balancing Free Speech and Privacy**

The RTBF operates at the inters[22]ection of privacy and free speech, creating a complex balancing act. Privacy advocates argue that RTBF protects individuals from harm caused by outdated or irrelevant data, such as defamatory content or past convictions.[23] Conversely, free speech proponents, particularly in jurisdictions like the US, contend that RTBF risks censorship, limiting access to public information. The *Google Spain* case illustrates this tension, as the ECJ allowed delinking but preserved original source data to uphold journalistic freedom. In India, the DPDPA's exemptions (Section 17) for public interest purposes reflect a similar balancing attempt but lack clarity on RTBF-specific applications.[24] This ambiguity underscores the need for precise legislative guidelines to ensure RTBF respects both individual privacy and societal access to information.

**Relevance to the DPDPA, 2023**

The DPDPA, 2023, represents India's attempt to address data privacy but falls short in explicitly recognizing RTBF.[25] While Section 8 allows data erasure requests, it does not address the public accessibility concerns central to RTBF, leaving individuals reliant on judicial remedies.[26] This framework highlights the DPDPA's limitations in aligning with global standards like GDPR, necessitating reforms to incorporate RTBF and strengthen individual autonomy in India's digital landscape.

---

[17] Geraldine O. Mbah, "Data privacy and the right to be forgotten." *World Journal of Advanced Research and Reviews* 16.2 (2022): 1216-1232.

[18] Mbah, Geraldine O. "Data privacy and the right to be forgotten." *World Journal of Advanced Research and Reviews* 16.2 (2022): 1216-1232.

[19] Buyuksagis, Erdem. "Towards a transatlantic concept of data privacy." *Fordham Intell. Prop. Media & Ent. LJ* 30 (2019): 139.

[20] Mbah, Geraldine O. "Data privacy and the right to be forgotten." *World Journal of Advanced Research and Reviews* 16.2 (2022): 1216-1232.

[21] Panchal, Sumit. "Cross-Border Data Protection Laws in India and European Union: A Critical Analysis of the Complexities and the Legal Challenges." (2024).

[22]

[23] Cofone, Ignacio N. "Online harms and the right to be forgotten." *The Right to be Forgotten*. Routledge, 2020. 1-16.

[24] Sobkow, Beata. "Forget Me, Forget Me Not-Redefining the Boundaries of the Right to Be Forgotten to Address Current Problems and Areas of Criticism." *Annual Privacy Forum*. Cham: Springer International Publishing, 2017.

[25] Sarkar Ghosh, Diya, Prafulla Chandra Mishra, and Tulishree Pradhan. "The conundrum of erasing digital footprints: A regulatory challenge." *Jindal Global Law Review* 15.1 (2024): 25-59.

[26] Blockchains, Permissioned. "Erasing the Trace: Challenges of the Right to Be Forgotten in Healthcare Private." (2025).

## 6. JUDICIAL RECOGNITION OF RTBF IN INDIA:

The Right to Be Forgotten (RTBF) has emerged as a critical facet of digital privacy, enabling individuals to request the removal of personal data from online platforms.[27] In India, while the Digital Personal Data Protection Act (DPDPA), 2023, lacks explicit provisions for RTBF, judicial interventions have played a pivotal role in recognizing this right, albeit inconsistently. This section examines key Indian case law, notably the landmark *K.S. Puttaswamy v. Union of India* (2017) and various High Court judgments, to trace the judiciary's approach to RTBF and highlight gaps in its legal recognition due to the absence of statutory clarity.[28]

The foundational case of *K.S. Puttaswamy (Retd.) v. Union of India* (2017) marked a watershed moment for privacy rights in India. The Supreme Court unanimously recognized the right to privacy as a fundamental right under Article 21 of the Constitution, encompassing informational privacy.[29] The judgment emphasized an individual's autonomy over personal data, laying a conceptual groundwork for RTBF. While the case primarily addressed the Aadhaar scheme, Justice S.K. Kaul's opinion explicitly referenced the RTBF, noting its relevance in controlling one's digital footprint.[30] The Court acknowledged that individuals should have the ability to "erase" personal data no longer necessary or relevant, particularly in the context of pervasive digital platforms.[31] However, *Puttaswamy* stopped short of establishing a clear legal framework for RTBF, leaving its application to future judicial interpretation.

Subsequent High Court judgments have grappled with RTBF requests, reflecting both progress and inconsistency. In *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.* (2019), the Delhi High Court addressed a petitioner's request to remove online articles linking him to a criminal case from which he was acquitted.[32] The Court granted an interim injunction, recognizing the petitioner's right to privacy and the irrelevance of outdated information, effectively endorsing an RTBF-like remedy. Similarly, the Kerala High Court in *Vysakh v. Union of India* (2021) ordered the removal of a petitioner's personal details from a public database, citing privacy concerns post-acquittal.[33] The Gujarat High Court, in *Dharamraj Bhanushankar Dave v. State of Gujarat* (2017), also entertained an RTBF plea, directing the removal of a judgment from online platforms that harmed the petitioner's reputation despite his acquittal.[34] These cases illustrate judicial willingness to protect individuals from perpetual digital stigmatization, particularly in criminal matters.

Despite these developments, significant gaps persist in the judicial recognition of RTBF. Indian courts have approached RTBF on a case-by-case basis, often relying on broader privacy principles rather than a standardized framework.[35] The absence of explicit RTBF provisions in the DPDPA, 2023, exacerbates this inconsistency.[36] Section 8 of the DPDPA allows data principals to request data erasure, but it lacks clear criteria for implementation, such as time limits or public interest exemptions, unlike the EU's GDPR (Article

[27] DIXIT, DR ANIL KUMAR. "Applicability of Right to be Forgotten in Present Times of Digital Age under Indian Legal Environment." (2024).

[28] Khatri, Sonsie, and Tasneem Fatma. "Second Chances and Digital Erasure: Do Former Convicts Have the Right to Be" Forgotten" in India?." *CALJ* 8 (2023): vii.

[29] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[30] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, per Kaul, J., concurring, para 629 (noting that the Right to Be Forgotten allows individuals to control their digital footprint).

[31] Shrivastava, Anujay. "Madras High Court says that there is no'right to be forgotten'against court decisions." *The Daily Guardian* (2021): 1-5.

[32] *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.*, 2019 SCC OnLine Del 8494.

[33] Vysakh K.G. v. Union of India & Anr., 2021 SCC OnLine Ker 5103

[34] Dharamraj Bhanushankar Dave v. State of Gujarat, Special Civil Application No. 1854 of 2015, (Gujarat High Court, Jan. 19, 2017)

[35] Bedi, Shruti. "The Contestation between Right to Be Forgotten and Freedom of Expression: Constitutional Silences and Missed Opportunities." *CALJ* 6 (2021): 1.

[36] JEMIMA, BS. "BALANCING THE GROWTH OF E-COMMERCE WITH DATA SECURITY AND PRIVACY: AN ANALYSIS OF THE INDIAN LEGISLATIVE FRAMEWORK." (2025).

17).[37] Courts have thus been forced to interpret RTBF through constitutional lenses, leading to varied outcomes. For instance, some High Courts have rejected RTBF claims when public interest, such as transparency in judicial records, outweighs individual privacy, as seen in *Orissa High Court v. Madan Mohan* (2020).[38]

The reliance on judicial discretion underscores the DPDPA's critical omission: a statutory framework for RTBF. Without legislative clarity, courts struggle to balance competing rights privacy versus freedom of expression and lack uniform guidelines for enforcement.[39] This gap risks inconsistent protections, particularly for vulnerable groups like victims of online harassment, who face challenges in securing data removal. The judiciary's proactive stance in cases like *Puttaswamy* and *Zulfiqar* signals RTBF's growing relevance, but the DPDPA's silence on this right leaves India's digital privacy framework incomplete, necessitating legislative reform to codify and standardize RTBF protections.[40]

## 7. ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023:

In the digital age, the Right to Be Forgotten (RTBF) empowers individuals to request the removal of personal data from online platforms, balancing privacy with freedom of expression.[41] Originating from EU jurisprudence, RTBF addresses the persistence of digital footprints. India's Digital Personal Data Protection Act, 2023 (DPDPA), enacted on August 11, 2023, marks a significant step toward data privacy regulation.[42] However, it falls short in explicitly incorporating RTBF, revealing omissions and challenges in reconciling individual rights with state interests.

### Key Provisions on Data Deletion, Correction, and Consent Withdrawal

The DPDPA emphasizes consent as a cornerstone for processing digital personal data. Under Section 5, data must be processed for lawful purposes with the Data Principal's (individual's) consent.[43] Section 6 introduces consent managers for managing, reviewing, or withdrawing consent.[44] Withdrawal triggers obligations under Section 8(7): the Data Fiduciary (controller) must cease processing and erase the data, unless retention is legally required. This links consent withdrawal directly to deletion, promoting user control.

For correction and deletion, Section 11(2) grants Data Principals the right to seek correction, completion, updating, or erasure of their data.[45] Fiduciaries must comply reasonably, except where law mandates retention. These provisions aim to ensure data accuracy and obsolescence, but they are reactive, requiring user initiation, and lack proactive mechanisms like automated expiry.

### Section-by-Section Analysis of Data Principal's Rights (Chapter III)

Chapter III outlines Data Principals' rights, focusing on empowerment amid digital vulnerabilities.

- **Section 11(1)**: Provides the right to a summary of processed personal data and activities, enabling transparency and informed decision-making.[46]

---

[37] Kneuper, Ralf. "Data Protection Principles and Their Implementation." *Data Protection for Software Development and IT: A Practical Introduction*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2024. 67-106.

[38] Madan M. Das v. State of Orissa & Ors., W.P.(C) No. 12210 of 2012

[39] Dziyauddin, Haidar. *A comparative study of freedom of expression and right to privacy in relation to the press in Malaysia and the United Kingdom*. Diss. Newcastle University, 2006.

[40] Patel, Kasim. "The Right to Privacy in Digital India: Analyzing the Personal Data Protection Framework." Record of Law, 27 May 2025, recordoflaw.in/the-right-to-privacy-in-digital-india-analyzing-the-personal-data-protection-framework/.

[41] Subiksha, V. Angelin. "Erasing the Past: Examining the Right to Be Forgotten in the Digital Age." *Jus Corpus LJ* 4 (2023): 24.

[42] Digital Personal Data Protection Act, 2023(Act, 22 of 2023).

[43] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 5.

[44] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 6.

[45] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 12(2).

[46] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 11(1).

- **Section 11(2)**: Core to privacy, this section allows requests for correction, completion, update, or erasure. It underscores the fiduciary's duty to act, but limits apply for legal compliance, potentially diluting efficacy in disputes.[47]
- **Section 12**: Introduces the novel right to nominate another individual to exercise rights in cases of death or incapacity, extending protections beyond the principal's lifetime—a forward-thinking but unique provision not mirrored in many global laws.[48]
- **Section 13**: Ensures grievance redressal mechanisms, mandating fiduciaries to provide readily available means for addressing violations or rights exercises.[49]

This chapter prioritizes access and rectification but omits broader rights like data portability or objection to processing, narrowing the scope compared to comprehensive frameworks.

**Omissions: No Explicit Mention of RTBF**

A glaring omission is the absence of explicit RTBF provisions. While Section 11(2) covers erasure, it does not extend to delinking from search results or third-party dissemination, as in true RTBF scenarios.[50] The Act focuses on fiduciary-held data, ignoring the viral nature of online information. This gap leaves individuals vulnerable to perpetual digital traces, especially in defamation or outdated contexts, highlighting a missed opportunity to address modern privacy challenges.[51]

**Role of Exemptions Under Section 17: Tension Between Privacy and State Interests**

Section 17 empowers the Central Government to exempt fiduciaries from provisions for national security, public order, crime prevention, or journalistic purposes.[52] This creates inherent tension: while exemptions facilitate state functions, they risk eroding privacy.[53] For instance, broad exemptions for "prevention of contraventions of law" could justify surveillance without oversight, prioritizing state interests over individual rights. Unlike narrower exemptions in other laws, this discretionary power lacks judicial checks, potentially enabling misuse and undermining the Act's privacy ethos.

**Institutional Framework: Data Protection Board's Powers and Limitations**

Chapter V establishes the Data Protection Board (Section 18), appointed by the Central Government, to inquire into complaints, issue directions, and impose penalties (Sections 19-20).[54] Appeals lie with the Telecom Disputes Settlement and Appellate Tribunal (Section 21). The Board's powers include enforcement and oversight, but limitations abound: it lacks rulemaking authority, vested instead with the government, reducing independence. Government appointments raise impartiality concerns, and without proactive monitoring tools, enforcement may be reactive and under-resourced.[55]

**Comparison with GDPR's Article 17 (Right to Erasure)**

GDPR's Article 17 explicitly enshrines the "right to be forgotten," requiring controllers to erase data and notify third parties,[56] with exceptions for expression or legal claims. DPDPA's erasure right under Section

[47] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 12(2).
[48] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 12.
[49] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 13.
[50] Blockchains, Permissioned. "Erasing the Trace: Challenges of the Right to Be Forgotten in Healthcare Private."
[51] Ok, Emmanuel, James Grace, and Mary John. "Security and Privacy Challenges." (2023).
[52] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 17.
[53] Richards, Neil, and Woodrow Hartzog. "A duty of loyalty for privacy law." *Wash. UL Rev.* 99 (2021): 961.
[54] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), sss. 18, 19, 20.
[55] Hinostroza Fuentes, Vasco Gerardo, et al. "AI with agency: a vision for adaptive, efficient, and ethical healthcare." *Frontiers in Digital Health* 7 (2025): 1600216.
[56] European Union. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)." Official

11(2) is similar but narrower, lacking third-party obligations and explicit RTBF language.[57] GDPR mandates broader compliance, like data portability (absent in DPDPA), and independent supervisory authorities, contrasting DPDPA's government-influenced Board. While both exempt for legal retention, GDPR's framework better balances rights, exposing DPDPA's omissions in addressing digital permanence.

## 8. CHALLENGES IN IMPLEMENTING THE RIGHT TO BE FORGOTTEN IN INDIA:

In the digital era, where personal data proliferates across online platforms, the Right to Be Forgotten (RTBF) emerges as a crucial mechanism for individuals to reclaim control over their information.[58] Originating from the European Union's General Data Protection Regulation (GDPR), RTBF allows data subjects to request the erasure of personal data when it is no longer necessary, irrelevant, or harmful. In India, the Digital Personal Data Protection Act, 2023 (DPDPA) marks a significant step toward data privacy, drawing from the Supreme Court's recognition of privacy as a fundamental right in *K.S. Puttaswamy v. Union of India* (2017).[59] Under Section 12 of the DPDPA, data principals have the right to correction and erasure of personal data, enabling requests for deletion when consent is withdrawn or the purpose is fulfilled.[60] However, the Act refrains from explicitly naming it as RTBF, focusing instead on "erasure" limited to data fiduciaries, omitting broader de-indexing from search engines as in GDPR. This omission, coupled with implementation hurdles, undermines its efficacy in balancing privacy with digital permanence.

Technological challenges pose formidable barriers to enforcing RTBF under the DPDPA. Digital records are inherently permanent, scattered across servers, backups, and third-party storage systems.[61] Once data is shared online, it can be replicated infinitely, making complete erasure nearly impossible. For instance, cached versions, archived backups, and blockchain-based storage resist deletion, complicating compliance for data fiduciaries. In India, with its vast digital ecosystem involving global platforms, ensuring erasure from all nodes including cloud services and decentralized networks—requires advanced tools like AI-driven data mapping, which many entities lack.[62] The DPDPA's omission of specific guidelines for handling distributed data exacerbates this, leaving fiduciaries vulnerable to incomplete deletions and potential breaches.

Legal challenges further complicate RTBF implementation, primarily in balancing it against constitutional rights like freedom of expression (Article 19(1)(a)) and the right to information.[63] The DPDPA provides exemptions for journalistic, artistic, or literary purposes, but lacks clear criteria for adjudication, risking arbitrary decisions.[64] Courts have grappled with this in cases like *Dharamraj Bhanushankar Dave v. State of Gujarat* (2015),[65] where RTBF clashed with public interest. Unlike GDPR's nuanced balancing test, the DPDPA's omissions include no mandatory proportionality assessment, potentially stifling free speech or allowing misuse in suppressing legitimate reporting. Additionally, extraterritorial application to foreign entities raises jurisdictional conflicts, as global platforms may prioritize home-country laws over Indian mandates.

---

Journal of the European Union, vol. L 119, 4 May 2016, Article 17, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[57] ms. Jemima b s, balancing the growth of e-commerce with Data security and privacy: an analysis of the Indian Legislative framework (2025).

[58] Mbah, Geraldine O. "Data privacy and the right to be forgotten." *World Journal of Advanced Research and Reviews* 16.2 (2022): 1216-1232.

[59] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

[60] Digital Personal Data Protection Act, 2023(Act, 22 of 2023), s. 12.

[61] Politou, Eugenia, et al. *Privacy and data protection challenges in the distributed era*. Vol. 26. Cham: Springer, 2022.

[62] Goswami, Amit, Siranjeevi Srinivasa Raghavan, and Karthik Chandrashekar. "SADGURU PUBLICATIONS."

[63] Bedi, Shruti. "The Contestation between Right to Be Forgotten and Freedom of Expression: Constitutional Silences and Missed Opportunities." *CALJ* 6 (2021): 1.

[64] Gupta, Ritu Sen. "Journalistic Exemption from Data Protection Laws: A Critical Appraisal from the Perspective of Bangladesh." *Issue 1 Int'l JL Mgmt. & Human.* 7 (2024): 541.

[65] Dharamraj Bhanushankar Dave v. State of Gujarat. Supreme Court of India, 2015.

Enforcement issues stem from the DPDPA's institutional framework, particularly the Data Protection Board (DPB), which lacks judicial oversight and independence.[66] Appointed by the central government, the DPB may face political influence, weakening its role in handling RTBF complaints. With no appellate tribunal initially outlined (though rules are pending), aggrieved parties rely on overburdened courts, delaying resolutions. Low penalties for non-compliance (up to ₹250 crore) may not deter large tech firms, and the absence of proactive monitoring tools hinders detection of violations.[67] This regulatory vacuum, combined with India's limited digital forensics expertise, renders enforcement reactive and ineffective.

Economic challenges burden intermediaries and e-commerce platforms tasked with DPDPA compliance.[68] Implementing RTBF requires significant investments in data management systems, audit trails, and erasure protocols, escalating costs for small and medium enterprises (SMEs). Platforms like Flipkart or social media giants must retrofit infrastructure to handle erasure requests, including API integrations and staff training, potentially diverting resources from innovation.[69] The Act's omissions, such as no cost-sharing mechanisms or phased rollouts for SMEs, amplify disparities, favoring Big Tech while straining local players in India's burgeoning digital economy.

Social challenges include low public awareness and risks of misuse, undermining RTBF's intent.[70] Many Indians, especially in rural areas, remain unaware of their data rights under the DPDPA, limiting uptake. Misuse risks abound, where influential individuals could exploit RTBF to erase accountability, such as in corruption scandals, clashing with societal transparency needs. Cultural factors, like stigma around past events (e.g., acquitted crimes), may drive genuine requests, but without awareness campaigns, the provision could exacerbate digital divides.[71]

## 9. CRITICAL ANALYSIS AND WAY FORWARD:

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a significant stride in India's data privacy framework,[72] yet it conspicuously omits an explicit provision for the Right to Be Forgotten (RTBF). This right, which empowers individuals to request the deletion or de-indexing of personal data from online platforms when it is outdated, irrelevant, or harmful, is enshrined in frameworks like the EU's GDPR (Article 17).[73] In the DPDP Act, Section 8(7) allows for data erasure once the processing purpose is fulfilled, and Section 12 mandates consent withdrawal leading to erasure.[74] However, these provisions fall short of RTBF's broader scope, which includes balancing privacy against public interest, free speech, and historical records. The omission creates ambiguity, leaving individuals vulnerable in the digital age where data persists indefinitely, exacerbating issues like revenge porn, defamation, or outdated criminal records that hinder rehabilitation.

---

[66] Kaur, Navdeep. "Decoding the Digital Personal Data Protection Bill: Strengths, Weaknesses, and the Road Ahead." *Weaknesses, and the Road Ahead (January 04, 2025)* (2025).

[67] Mathur, Shubh, and Hadiya Khan. "Legal Aperture and Tax Avoidance Strategies in India: An Analysis." *Issue 3 Int'l JL Mgmt. & Human.* 7 (2024): 1253.

[68] Sundara, Karishma, and Nikhil Narendran. "The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection." *Computer Law Review International* 24.5 (2023): 129-141.

[69] Dutta, Sumedha, Asha Thomas, and Puja Khatri. *Disruptive technology in human resource management*. Taylor & Francis, 2025.

[70] Blockchains, Permissioned. "Erasing the Trace: Challenges of the Right to Be Forgotten in Healthcare Private."

[71] Higgins, Noelle, Delia Ferri, and Katie Donnellan. "Enhancing access to digital culture for vulnerable groups: the role of public authorities in breaking down barriers." *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique* 36.5 (2023): 2087-2114.

[72] Mukhija, Khilansha, and Shreyas Jaiswal. "Digital Personal Data Protection Act 2023 in Light of the European Union's GDPR." *Jus Corpus LJ* 4 (2023): 638.

[73] Pancani, Alessandro, and PEI Paulan Korenhof. "SEARCHING TO BE FORGOTTEN."

[74] The Digital Personal Data Protection Act, 2023, (2025), ss. 8(7), 12.

Critically, incorporating RTBF explicitly into the DPDP Act is imperative. The Act's current framework prioritizes data minimization and purpose limitation but neglects the dynamic nature of digital harm.[75] Without RTBF, data fiduciaries (platforms) lack clear guidelines, leading to inconsistent enforcement.[76] Challenges include technological feasibility search engines like Google handle delisting requests variably and jurisdictional conflicts in a borderless internet. Moreover, in a democracy like India, RTBF risks clashing with Article 19(1)(a) of the Constitution (freedom of speech), potentially enabling misuse by powerful entities to suppress information.[77] Judicial precedents, such as the Karnataka High Court's 2020 ruling in *Vinit Kumar v. CBI* recognizing RTBF for acquitted individuals, highlight the legislative gap. Yet, over-reliance on courts burdens the judiciary and results in piecemeal protections, underscoring the need for statutory clarity to prevent privacy erosion amid rising data breaches.

Moving forward, legal reforms should embed a clear statutory right to RTBF in the DPDP Act, modeled on GDPR but adapted to Indian contexts.[78] This could involve amending Section 8 to include RTBF as a distinct right, with criteria for requests: relevance, accuracy, and public interest. Safeguards for free speech are essential exemptions for journalistic, artistic, or legal purposes, akin to GDPR's Article 85.[79] A judicial balancing mechanism, perhaps via specialized data protection tribunals under the Data Protection Board (Section 18), would evaluate requests on a case-by-case basis, weighing privacy against expression rights. This hybrid approach—administrative for routine cases, judicial for contentious ones would ensure proportionality.[80]

The judiciary's role in filling the gap remains pivotal until reforms materialize. Courts have progressively interpreted Article 21 (right to privacy) expansively, as in *Justice K.S. Puttaswamy v. Union of India* (2017), to include informational privacy.[81] High Courts in Gujarat and Orissa have granted RTBF in sensitive cases, setting precedents that could guide interim enforcement. However, this is unsustainable; legislative action is needed to standardize remedies.

Complementing legal measures, awareness and education are crucial support mechanisms. Public campaigns by the Ministry of Electronics and IT could educate citizens on RTBF, akin to GDPR awareness drives, empowering marginalized groups.[82] Technological innovations, such as AI-driven automated delisting tools or blockchain for verifiable erasures, can enhance implementation. Platforms should integrate privacy-by-design features, like expiry dates for data, reducing manual interventions.[83]

## 10. CONCLUSION:

The exploration of the Right to Be Forgotten (RTBF) within the context of India's Digital Personal Data Protection Act, 2023 (DPDP Act), reveals critical insights into the evolving landscape of digital privacy. The analysis underscores that while the DPDP Act introduces significant measures for data protection, it notably lacks explicit provisions for the RTBF. This omission represents a substantial gap in safeguarding individuals' digital dignity, particularly in an era where personal data persists indefinitely online, often beyond an individual's control. The absence of a clear RTBF framework limits the ability of individuals to manage their digital footprints, exposing them to risks such as reputational harm and privacy violations.

---

[75] Kaur, Navdeep. "Decoding the Digital Personal Data Protection Bill: Strengths, Weaknesses, and the Road Ahead." *Weaknesses, and the Road Ahead (January 04, 2025)* (2025).

[76] Ryan, Johnny, and Cristiana Santos. "An unending data breach immune to audit? can the tcf and rtb be reconciled with the gdpr?." *Can the TCF and RTB be reconciled with the GDPR* (2022).

[77] Cofone, Ignacio N. "The Right to be Forgotten." *A Canadian and Comparative Perspective/edited by Ignacio Cofone. 1st ed.(February 7, 2020). Publisher: Routledge* (2020).

[78] ROY, ANANYO, and Dr Aparna SREEKUMAR. "Privacy in the digital era." (2024).

[79] Lambrecht, Maxime. "Free speech by design: algorithmic protection of exceptions and limitations in the copyright DSM directive." *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 11 (2020): 68.

[80] Williams, Stephen F. "Hybrid rulemaking under the administrative procedure act: a legal and empirical analysis." *U. Chi. L. Rev.* 42 (1974): 401.

[81] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

[82] Saeed, Jannat. "Guardians of the Data: Government Use of AI and IoT in the Digital Age." (2024).

[83] Perera, Charith, et al. "Privacy-by-design framework for assessing internet of things applications and platforms." *Proceedings of the 6th International Conference on the Internet of Things*. 2016.

The RTBF, recognized in jurisdictions like the European Union under the GDPR, empowers individuals to request the deletion of personal data that is no longer relevant or necessary. In contrast, the DPDP Act's focus on data minimization and consent does not adequately address the need for mechanisms to erase outdated or harmful digital records. This gap is particularly concerning given India's vast internet user base and the increasing prevalence of data-driven technologies. Explicit recognition of the RTBF would strengthen the legal framework, ensuring individuals have greater control over their personal information.

To align with global standards, India must integrate the RTBF into its data protection regime while balancing constitutional values such as freedom of expression and the right to information. Harmonizing these principles requires a nuanced approach, incorporating clear guidelines for data deletion and judicial oversight to prevent misuse. By addressing this omission, India can enhance digital dignity, foster trust in its digital ecosystem, and affirm its commitment to robust privacy protections in the digital age.