

FROM PERPETUAL DIGITAL MEMORY TO THE JURIDICAL PROMISE OF OBLIVION: A CONSTITUTIONAL EXAMINATION OF THE RIGHT TO BE FORGOTTEN UNDER ARTICLE 21

Prof. Mamta Rana Guleria*
Jigyasa Kumar**

ABSTRACT

Digitalisation has radically transformed the nature of personal. What once faded naturally from public consciousness now outlives its online existence. This paper examines the Right to Be Forgotten (RTBF) as a constitutional response to dangers of technological permanence. Though not expressly codified, RTBF draws its legitimacy from Article 21 of the Indian Constitution, as recognised by the Supreme Court in the Puttaswamy case. However, the procedural infrastructure and institutional structure for its enforcement remain fragmented. The paper undertakes a doctrinal and comparative analysis of RTBF, situating it within India's evolving privacy jurisprudence and relating it to international frameworks—including the GDPR, the UDHR, and the ICCPR—each of which treats informational self-determination as a human right. The paper offers critical scrutiny of the DPDP Act, 2023, and the DPDP Rules, 2025, for failure to recognise RTBF as an independent right undermining constitutional proportionality. Concluding reforms are proposed in areas including algorithmic anonymity, data-expiration norms, posthumous digital dignity, and gendered digital harm. It concludes by articulating the constitutional ethic of the juridical promise of oblivion as a prerequisite against the technological permanence of information.

KEYWORDS: *Right to be Forgotten (RTBF); technological permanence; privacy; constitutional proportionality; digital dignity.*

1. INTRODUCTION—UNDERSTANDING THE EPOCH OF EVERLASTING DIGITAL FOOTPRINTS

There is something philosophically troubling about the permanence of digital memory. The digital infrastructure has changed the way individual identity, reputation, and privacy are seen; information persistently circulates across platforms, and the digital infrastructures and search engines continuously reproduce this data through indirect storage mechanisms, risking stigmatisation and immortalisation of past actions in cyberspace in ways against legitimate public purposes.

The Right to be Forgotten (RTBF) addresses this issue. At its core it is the person's meaningful control over their personal data whose continued availability serves no proportionate purpose. The right received the consequential juridical articulation from the European Court of Justice's (ECJ) in *Google Spain SL and Google Inc. vs. Agencia Española de Protección de*

* Professor & Head, School of Law, SRT Campus, Tehri Garhwal, HNBGU, Uttarakhand.

** LL.M., School of Law, SRT Campus, Tehri Garhwal, HNBGU, Uttarakhand.

In India, the constitutional groundwork of the RTBF gained importance after the case of *Puttaswamy*,² which recognised privacy as a fundamental right under Article 21³, where the informational and decisional privacy were recognised, and which provided a foundation for the right’s evolution. The DPDP Act further institutionalised the discussion by introducing a limited “right to erasure,”⁴ leaving unaddressed certain doctrinal and constitutional questions regarding free expression and the right to be informed. The DPDP Rules, 2025, notified on November 13, 2025, operationalise significant aspects of the act, though significant gaps still persist.⁵

Thus, this paper argues that RTBF represents a legitimate extension of Article 21’s substantive guarantee of dignity and privacy, and that its implementation demands for a principled and proportionality-based framework to balance individual’s informational autonomy against countervailing rights, including free speech, open justice, and the public’s right to know, ensuring that the promise of oblivion does not become an instrument of concealment.

1.1 OBJECTIVES OF STUDY

- To examine the constitutional and judicial basis of RTBF in India.
- To assess legal and technological frameworks, including global models like GDPR, and identify reform pathways for a balanced RTBF enforcement regime.

1.2 RESEARCH METHODOLOGY

The methodology employed is primarily doctrinal in nature, drawing upon constitutional provisions, parliamentary reports, judicial decisions, and scholarly literature on the RTBF in India, with comparative insights from GDPR and the UK Data Protection Act to contextualise India’s evolving position.

¹ *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD)*, (2014) E.C.R.317.

² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

³ INDIA CONST. art. 21.

⁴ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023[hereinafter DPDP Act].

⁵ Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (notified on Nov. 13, 2025) (India) [hereinafter DPDP Rules].

2. CONCEPTUAL FRAMEWORK:

2.1 ORIGINS AND EARLY DEVELOPMENT

The intellectual development of RTBF was found in **France**. The concept of *le droit à l'oubli* —the “right to oblivion”—allows individuals (with past criminal records) to reintegrate into society without being judged by prior actions. While originally based upon offline contexts, the digital proliferation of personal data reinvigorated demands for such a right in the online sphere. Article 12 of the UDHR⁶ and Article 17 of the ICCPR⁷, collectively establish the legal basis for safeguarding individuals against unwarranted intrusion as well as unjust harm to their dignity, reputation, and personal honor, rights foundational to the RTBF across jurisdictions.

2.2 THE EUROPEAN MODEL: GDPR AND THE RIGHT TO ERASURE

The RTBF acquired judicial recognition in the **European Union** through the landmark judgment of the CJEU in the *Google Spain* case, which recognised the search engine providers as data controllers and held that they are obliged for considering requests to de-index search results in cases where personal data has become “inadequate, irrelevant, or no longer relevant⁸.” This judicial articulation culminated in the enactment of Article 17 of the GDPR (2016)⁹, which codifies the Right to Erasure, allowing the requests of the deletion of personal information, with exceptions to journalistic freedom, legal obligations, public interest, and archival value.

The influence of the European regulatory paradigm can be seen worldwide. **Argentina**, (*Rodriguez v. Google Inc.*) recognised intermediary liability for outdated or defamatory content.¹⁰ **Japan**¹¹, and **South Korea**¹² introduced privacy-based delisting guidelines. **New Zealand** allows delisting of outdated and reputation-harming search results.¹³ In contrast, **the United States** remains hesitant to adopt RTBF, prioritising **the First Amendment**¹⁴ and the public’s access to information, though expungement laws serve a similar purpose.

⁶ Universal Declaration of Human Rights (UDHR), G.A. Res. 217 (III) A, U.N. Doc. A/810 (Dec. 10, 1948) art. 12.

⁷ International Covenant on Civil and Political Rights (ICCPR), Dec. 16, 1966, 999 U.N.T.S. 171, art. 17.

⁸ *Google Spain SL*, *supra* note 1.

⁹ Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) art. 17 [hereinafter GDPR].

¹⁰ *Rodriguez v. Google Inc.*, Case No. 99.280/2012 (Sup. Ct. Arg. Oct. 28, 2014).

¹¹ *Google Inc. v. Plaintiff*, Supreme Court of Japan (Jan. 31, 2017).

¹² Korea Communications Commission [KCC], *Guidelines for Requests for Access to or Deletion of Personal Information* (2016) (S. Kor.).

¹³ *A.T. v. Google LLC* [2021] NZHC 1550 (N.Z.).

¹⁴ U.S. CONST. amend. I (“Congress shall make no law...abridging the freedom of speech, or of the press”).

3. ARTICLE 21 AND THE RTBF: EXPANDING THE CONSTITUTIONAL CANVAS

Article 21, guaranteeing *right to life or personal liberty*¹⁵, underwent expansive interpretation to include within its scope the right to *dignity, privacy, bodily integrity, informational autonomy, reputation, and other facets of human personality*, thus naturally accommodating the concept of digital self-determination, which underlies the RTBF.

• JUDICIAL FOUNDATIONS: PRIVACY AND DIGNITY AS KEYSTONES

The earliest judicial concern of protecting personal dignity against perpetual reputational harm appeared in *State of Punjab v. Gurmeet Singh & Ors.*¹⁶, where the Supreme Court mandated confidentiality protections for sexual assault survivors to prevent lifelong stigma and secondary victimisation. This approach later evolved in the case of *K.S. Puttaswamy (Retd.) v. Union of India*¹⁷, which affirmed privacy as an intrinsic facet of Article 21 and clarified that informational privacy, that is, an individual's right to control data generated about them,¹⁸ thus provides ground for the RTBF claims in India.

• JUDICIAL TRENDS SHOWING EVOLUTION AND DEVELOPMENT OF THE RTBF.

The first judicial articulation of RTBF appeared in *Sri Vasunathan v. Registrar General*¹⁹, where the Karnataka High Court directed the removal of a woman's name from publicly accessible online court records to protect the individual's dignity and privacy. This reasoning was extended in *Jorawar Singh Mundy v. Union of India*,²⁰ directing de-indexing of the acquittal order from search engines serving no legitimate purpose and inflicting reputational harm of the acquitted, and in *Subhranshu Rout v. State of Odisha*, which emphasised protection of digital identity against non-consensual content circulation.²¹ The courts even considered the non-consensual publication of private images and deepfake and AI-generated image cases, including *Aishwarya Rai Bachchan v. Unknown & Ors. (2025)* case, illustrating a significant step in applying RTBF to emerging digital threats, acknowledging technologically fabricated violations as cognisable.²²

¹⁵ INDIA CONST., *supra* note 3.

¹⁶ *State of Punjab v. Gurmeet Singh*, (1996) 2 SCC 384.

¹⁷ *Puttaswamy*, *supra* note 2.

¹⁸ *Id.* at paras. 243-254.

¹⁹ *Sri Vasunathan v. Registrar General*, (2017) 7 Kant. L.J. 774.

²⁰ *Jorawar Singh Mundy v. Union of India*, 2021 (2) Del. H.C. 377.

²¹ *Subhranshu Rout v. State of Odisha*, 2020 (II) SLT Orissa H.C. 216 (the Court remarked that "the right of a woman to have her photographs removed from social media is inextricably linked to her right to privacy and dignity under art. 21. ").

²² *Aishwarya Rai Bachchan v. Unknown*, Delhi High Court (2025).

However, there has been consistent emphasis that RTBF is subject to a balancing test and cannot override constitutional values of transparency and free speech protected under Article 19(1)(a) where public interest subsists.

4. LEGISLATIVE AND STATUTORY FRAMEWORKS

While Indian courts defined the contours of the RTBF, statutory recognition evolved progressively from early cyber-governance laws to the latest data privacy statutes, embedding an individual's autonomy over personal data.

4.1 THE INFORMATION TECHNOLOGY ACT, 2000, AND IT RULES, 2011²³

India's data protection journey began with the Information Technology Act, 2000, wherein section 43A²⁴ (implemented through IT Rules) imposed responsibility on corporate bodies to safeguard *sensitive personal data* from negligent disclosure but does not confer a right of erasure.²⁵ Section 79 offers safe harbor to intermediaries on due diligence observance.²⁶ In *Jorawar Singh Mundy v. Union of India*,²⁷ courts creatively applied this provision to compel search engines to de-index content, illustrating the judiciary's willingness to stretch the existing framework to constitutional values. Rule 5 of IT Rules permits individuals to withdraw consent and obligates cessation of data retention,²⁸ applying only to sensitive personal data, without limited enforcement mechanisms.

4.2 THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The DPDP Act is the most ambitious legislative engagement with personal data governance. It allows data principals to rectify, update, and request deletion of their personal data.²⁹ Section 12 allows erasure once the data processing purposes are fulfilled or the consent is withdrawn,³⁰ subject to exemptions for legal compliance, national security, and judicial purposes.³¹ Section 44 of the Act creates important statutory spillover: it repeals Section 43A of the IT Act and amends Section 8(1)(j) of the Right to Information Act, 2005, with the phrase 'information which relates to personal information,' creating tension

²³ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Information Technology (Intermediaries Guidelines) Rules, 2011, Gazette of India (Apr. 11, 2011).

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.* s.79.

²⁷ *Jorawar Singh Mundy*, *supra* note 20.

²⁸ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 5 (India).

²⁹ DPDP Act, *supra* note 4, s. 11.

³⁰ *Id.* s. 12.

³¹ *Id.* s. 17.

between data privacy and RTI-based transparency.³² However, enforcement is discretionary of data fiduciaries, with limited scrutiny by the Data Protection Board.³³ However, clarity on online de-indexing and removal of third-party content is limited.

4.3 POLICY RECOMMENDATIONS AND EMERGING DIMENSIONS

At the policy level, the Justice Srikrishna Committee Report (2018) recognised RTBF as central to informational privacy³⁴, while the Expert Committee (2020) stressed individual control over data, including the right of erasure and portability.³⁵ Thus, policy reports strengthened this progress.

4.4 RECENT DEVELOPMENT: DPDP RULES, 2025

The MeitY's notification of the DPDP Rules, 2025,³⁶ marks a significant milestone in India's privacy regime, aiming to transition from fragmented digital regulation to a more reliable system of data governance.³⁷

The rules introduced a mandatory data-erasure requirement and mandated specified entities (like social media platforms and e-commerce intermediaries) by Rule 8 to delete personal data after three years of user "inactivity," with at least forty-eight hours' notice (representing India's first statutory time-bound data retention framework). Significant Data Fiduciaries (SDFs) face stricter obligations, including compulsory Data Protection Impact Assessments, audits, and record maintenance, relevant to addressing algorithmic permanence, automated profiling, and inferential data retention. Additional protective measures—encryption mandates, structured access controls, and verifiable parental consent for children—are also introduced, strengthening individuals' autonomy.³⁸ The creation of the Digital Data Protection Board (DPB) provides for a formal compliance mechanism.

The gap, however, remains substantial. The three-year deletion mandate does not extend to platforms processing sensitive data, legacy archives, and AI-trained datasets. Derived or inferential data and the de-indexing norms for search engines remain out of the rule's scope. A recent controversy regarding the mandatory pre-installation of the Sanchar Sathi application illustrated the

³² *Id.* s. 44.

³³ *Id.* ch. VI (outlines limited oversight by the Data Protection Board).

³⁴ JUSTICE B.N. SRIKRISHNA COMM., DATA PROTECTION COMM. REPORT: A FREE AND FAIR DIGITAL ECONOMY (2018).

³⁵ EXPERT COMM. ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK, REPORT (2020).

³⁶ DPP Rules, *supra* note 5.

³⁷ *Digital Personal Data Protection Rules, 2025 Notified*, SCC ONLINE (2025).

³⁸ *DPP Rules 2025: Key Security Requirements*, TIMES OF INDIA (2025).

risks of disproportionate data collection in the absence of clear sunset clauses.³⁹ These highlight the need to update the Rules and to expressly mention the explicit retention limits, independent oversight, and enforceable erasure mechanisms.

5 INTERSECTING RIGHTS AND THE CONSTITUTIONAL STATUS

5.1 SURVEILLANCE CAPITALISM AND MEMORY AS POWER

In the contemporary digital era, personal data has acquired the character of being the most valuable instruments of institutional power, transforming human experience: such as movement, preference, and identity—into a commercial resource that is harvested, stored, and monetised by both corporate and state entities for profit-making, raising foundational concerns under Article 21 regarding erosion of dignity and the ability to exist beyond the permanent institutional memory.⁴⁰

India's DPDP Act, 2023, offers limited rights of correction and erasure as an acknowledgement of the problem. Yet, these problems are undermined by broad exemptions granted to government agencies for "legitimate purposes," allowing mass data retention and surveillance-based profiling.⁴¹ The DPDP Rules, 2025, reinforce this framework by sanctioning prolonged data retention for government databases—particularly for law enforcement, welfare delivery platforms, and identity repositories.⁴²

This further becomes troubling not by legislation but by what it enables on the ground. Facial recognition technologies used across the 2023 Kumbh Mela,⁴³ Digilocker facilities, UPI, the Aadhar-linked data leaks, and geo-tagging of offenders in Nagpur (August 2025),⁴⁴ all signal the same reality: that surveillance is no longer peripheral to governance but rather has become structural and difficult to contest, undermining privacy concerns.

5.2 ARTICLE 21 AND THE HUMAN RIGHT TO DIGITAL DIGNITY

The jurisprudence around Article 21 has been expanded beyond literal interpretation to provide constitutional grounding for the RTBF. As technology

³⁹ *Sanchar Saathi Mandatory Preloading Raises Privacy Concerns*, INDIAN EXPRESS (2025), <https://indianexpress.com/article/opinion/columns/sanchar-saathi-mandatory-preloading-cyber-security-privacy-10397920/>.

⁴⁰ *Puttaswamy*, *supra* note 2, at 66-72.

⁴¹ DPDP Act, *supra* note 4, s. 17(2)(a).

⁴² DPDP Rules, *supra* note 5, rr. 4-7.

⁴³ INTERNET FREEDOM FOUNDATION (IFF), "FACIAL RECOGNITION IN INDIA: 2023 REPORT (2023)", <https://internetfreedom.in/facial-recognition-in-india-2023>.

⁴⁴ *Geo-tagging of Criminals Launched in Nagpur to Enhance Surveillance*, TIMES OF INDIA (Aug. 2025), <https://timesofindia.indiatimes.com/city/nagpur/geo-tagging-of-criminals-launched-in-nagpur-to-enhance-surveillance/articleshow/123150286.cms>.

mediates with identity, the concept of *digital dignity* extends privacy into the realms of storage and reputation. The RTBF thus becomes crucial in allowing individuals seeking erasure or delinking of obsolete, stigmatic, or harmful data, thereby enabling control over how they are seen, remembered, or searched in the information society.

Even after acquittal or social reintegration, individuals are haunted by their outdated digital records, which shape public perception and deny them the possibility of redemption.⁴⁵ Like in 2025, several former undertrial prisoners sought delinking of their names from archived media reports and repositories, citing psychological distress and social ostracism as direct consequences of persistent digital exposure.⁴⁶ Likewise, in April 2025, an NGO representing survivors of sexual assault filed PIL, seeking the removal of media content revealing victims' identities, leading to a "second assault" on dignity.⁴⁷

Thus, India must move beyond fragmented judicial remedies and legislate a clear framework balancing RTBF with free speech and public interest. The DPDP Rules, 2025, attempt to sharpen the scope of erasure rights by mandating verification procedures, processing timelines, and appeal mechanism.⁴⁸ However, it does not expressly impose erasure obligations on search engines, creating ambiguity regarding whether they qualify as "data fiduciaries," which weakens the operationalisation for RTBF in India.

5.3 RTBF VS. FREEDOM OF INFORMATION: CONFLICT WITH RTI AND PUBLIC INTEREST

The RTBF safeguards an individual's autonomy over personal information and guards against perpetual digital exposure, whereas on the other side, India's constitutional design upholds robust guarantees for transparency and free speech under Article 19(1)(a) of the Constitution, while the RTI Act, 2005,⁴⁹ institutionalises access to government-held sensitive data as a tool of accountability.⁵⁰ However, on the other side, the RTI Act exempts the disclosure of personal information in cases involving "unwarranted invasion of privacy," unless outweighed by public interest.⁵¹ Hence, the right of being

⁴⁵ LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 127-33 (2d ed. 2020).

⁴⁶ *Delhi High Court Mulls Right to Be Forgotten for Acquitted Persons*, TIMES OF INDIA (Feb. 5, 2025), <https://timesofindia.indiatimes.com/city/delhi/delhi-high-court-orders-name-masking-for-acquitted-individuals-online/articleshow/115540091.cms>.

⁴⁷ *Petition Seeks Removal of Online Content Disclosing Rape Survivors' Identities*, INDIAN EXPRESS (2025), <https://indianexpress.com/article/india/supreme-court-bars-media-from-revealing-identities-of-rape-survivors-5489192/>.

⁴⁸ DPDP Rules, *supra* note 5, rr. 5-8.

⁴⁹ The Right to Information Act, 2005, No. 22, Acts of Parliament, 2005 (India) [hereinafter RTI Act].

⁵⁰ INDIA CONST. art. 19(1)(a); RTI Act, *supra* note 49.

⁵¹ RTI Act, *supra* note 49, s. 8(1)(j).

forgotten may conflict with the collective interest in transparency, open justice, and historical memory.

However, in *Vysakh K.G. v. Union of India*,⁵² blanket erasure of judicial records from the online database was refused, citing open-justice principles and the absence of a legislative framework necessitating caution and case-by-case balancing.

Administrative and quasi-judicial bodies apply similar proportional balancing under the RTI framework. Like, the Karnataka Information Commission directed publication of marks of selected candidates as accountability outweighed the individual's privacy claims.⁵³ Thus, these developments confirm that RTBF in India cannot be absolute but must coexist with the constitutional ethos realised through a proportionality-based approach.

5.4 ROLE OF INTERMEDIARIES: GOOGLE, META, AND INDIAN OBLIGATION

The IT Act, 2000⁵⁴, provides intermediaries (such as Google, Meta, Twitter/X, hosting sites, and search engines) a conditional “safe harbor” from liability for the third-party data as long as they satisfy the legislative conditions and respond to “actual knowledge” or to the government and judicial orders.⁵⁵ This places intermediaries not as neutral carriers or fully autonomous publishers, but as the gatekeepers of the digital public sphere.⁵⁶

In the case of *Mrs. X v. Union of India*⁵⁷, the petitioner sought delisting of her name from an old sexual harassment proceeding, arguing that public indexing of such material violated her right under Article 21. The court observed that while intermediaries possess technically sophisticated tools for automated identification, the absence of a standardised legally-mandated de-indexing protocol leaves judicial discretion as the only operative safeguard for the right enforcement.⁵⁸

⁵² *Vysakh K.G. v. Union of India*, 2022 SCC Online Ker 6975.

⁵³ *Disclosure of Marks in Recruitment Process*, TIMES OF INDIA (Feb. 15 2025), <https://timesofindia.indiatimes.com/city/bengaluru/marks-of-selected-candidates-should-be-made-public-karnataka-information-commission/articleshow/121605778.cms>.

⁵⁴ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

⁵⁵ *Id.* s. 79.

⁵⁶ See *Shreya Singhal v. Union of India*, (2015) 5SCC 1, where the Supreme Court read down s.79(3)(b) to protect intermediaries from arbitrary takedown requests not backed by judicial orders.

⁵⁷ *Mrs. X v. Union of India*, W.P.(C) 10880/2022(Del. H.C., 26 Apr 2023).

⁵⁸ *Id.* at interim order 12.

The IT Rules 2021⁵⁹, as amended in 2022 and 2024, address intermediary responsibility but lack provisions governing RTBF requests. Similarly, *X Corp. (formerly Twitter) v. Union of India*⁶⁰ exposed the unresolved tension between state-directed takedowns and intermediary autonomy regarding blanket removal orders under Section 69A of the IT Act, arguing arbitrary directions compromise both safe harbor protections and freedom of expression.⁶¹ Thus, we need a clear legislative framework to balance the compliance and the discretion.

5.5 ETHICAL AND INCLUSIVE PERSPECTIVES: A DIGITAL TRAUMA

Digital perpetuity has created a unique form of gendered vulnerability. Non-consensual intimate image (NCII) circulation, commonly known as *revenge porn*, and a threat of AI-generated deepfake content disproportionately harms both men and women and also LGBTQ+ individuals, converting private violations into perpetual public humiliation.

Feminist scholarship extends this notion beyond privacy as an issue of informational justice, enabling individuals to detach themselves from harmful digital associations and restore control over their self-representation.⁶² Thus, RTBF extends beyond mere deletion, enabling narrative control, aligning with the constitutional triad of dignity, equality, and autonomy under Articles 14, 19, and 21.⁶³

5.6 ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND THE PROBLEM OF TIMELESS DATA

Informational permanence has emerged as a newly redefined challenge before the governance, commerce, and public administration begotten by the increased rise of AI technologies. The AI models learn and create predictive profiles that continue to operate even after the original has been deleted.⁶⁴ These algorithmic structures store *derived, residual, and inferential data*, transforming “forgetting” from a mere act of deletion to a more complicated process of *unlearning and de-circulation* of the information.

The “*inferential persistence*” allows the algorithmic systems to continue reproduction of biases (whether on browsing habits, gender, sexual orientation, caste, economic indicator, etc.), indirectly profiling the individuals. Similar to

⁵⁹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 G.S.R. 139(E)(India).

⁶⁰ *X Corp. v. Union of India*, W.P. No. 23470/2023 (Karn. H.C.).

⁶¹ *Id.* (Court filings).

⁶² CATHARINE A. MACKINNON, *TOWARD A FEMINIST THEORY OF THE STATE* 212 (1989).

⁶³ INDIA CONST. arts. 14, 19 & 21.

⁶⁴ S. Narain, *Artificial Intelligence and the Challenge of Forgetting: Rethinking Privacy in the Age of Algorithms*, 8 INDIAN J.L. & TECH 102 (2023).

Puttaswamy case, in *Internet Freedom Foundation v. Union of India*⁶⁵, the Delhi High Court expressed apprehension over facial recognition and predictive policing systems deployed without transparent data retention policies, recognising the threat that such systems pose to the dignity of the individual.

The DPDP Act, 2023, does not address *derived or inferred data* within AI frameworks, creating a legal vacuum that immunises algorithmic memory from erasure, thus undermining RTBF. Though the DPDP Rules, 2025, mandate data retention limits and audits for significant data fiduciaries, they do not require models to “unlearn” or purge inferential data.

5.7 DIGITAL AFTERLIFE: PRIVACY RIGHTS OF DECEASED INDIVIDUALS

The Indian Constitution progressively interprets Article 21 extending beyond the physical lifespan of the individual, recognising posthumous identity encompassing treatment of the dead body, last rites, and preservation of digital identity.

The Supreme Court observed that the right to dignity extends even beyond physical lifespan also to the body after death, establishing posthumous identity as a *constitutional value*,⁶⁶ underscored during public sensationalisation, following the deaths of Sushant Singh Rajput and Jiah Khan.

The National Human Rights Commission’s 2021, *Advisory on Dignity on Rights of the Dead*, amidst the pandemic, directed that all states and UTs must ensure respectful handling of bodies and that hospitals do not detain bodies due to unpaid bills, thus promoting the notion of respecting the humanity of the deceased.

With the recognition of the *digital afterlife*, a new dimension has emerged—the right of the deceased over their digital legacy. In *re: RG Kar Medical College & Hospital* (Kolkata Rape Case 2024), the Supreme Court issued an injunctive order directing the removal of all material identifying the deceased victim from media platforms, holding that her dignity remains protected under Article 21 notwithstanding her death.⁶⁷ In response, MeitY passed instructions strengthening the emerging foundation for a post-mortem variant of the RTBF. Thus, the rights to be forgotten and to die with dignity are constitutionally intertwined.

⁶⁵ *Internet Freedom Found. v. Union of India*, W.P. (C) No. 452 of 2022 (India).

⁶⁶ *Pt. Parmananda Katara v. Union of India*, (1989) 4 SCC 286.

⁶⁷ *In re: Alleged Raped and Murder Incident of a Trainee Doctor in R.G. Kar Medical College and Hospital*, SMW (Crl) No. 2 of 2024 (India).

5.8 CONSTITUTIONAL PRIVACY OR POLITICAL CONCEALMENT: THE DEMOCRATIC ACCOUNTABILITY

The right, however, raises concerns of a threat to democratic accountability. If left unchecked, it may allow political figures to remove records of past misconduct, corruption allegations, or criminal activities from the public domain under the guise of privacy, thus transforming the right of informational autonomy into an instrument of concealment, obstructing an individual's right to know.⁶⁸ This weakens institutional transparency, distorting historical records and impeding journalistic scrutiny.

The DPDP Rules, 2025, address the risk by granting categorical exemptions for data in the public interest, including political transparency. However, there is a need for a constitutionally sound approach to distinguish between private informational rights and public interest obligations, to ensure the democratic principle of informed citizenry.

6. DATA COLONIALISM: GLOBAL GOVERNANCE AND DIGITAL DEPENDENCY

The twenty-first century has witnessed the rise of *data colonialism*: i.e. commodification of the human experience as raw material by the global digital corporations, converting users into perpetual data sources. This causes a digital dependency, especially in the Global South, where platforms headquartered in the Global North continue to dominate digital infrastructures and rule-making processes.

Governance Vacuum and Normative Asymmetry. Besides data's centrality, there exists no binding international treaty governing cross-border data transfers or digital sovereignty. The UN's Global Digital Compact 2024 reaffirmed equitable digital governance but lacked enforceable mechanisms.⁶⁹ Meanwhile, regimes such as the GDPR (2018) and California's CCPA (2020) continue to influence countries like India without giving them a voice in setting standards.⁷⁰

Digital Dependency and Developmental Sovereignty. India's DPDP Act, 2023, permits cross-border data transfers to "notified countries," raising concern over foreign technological dependency. The 2025 initiative to establish AI cloud centers with US and UAE tech firms raised debates on data sovereignty and citizen autonomy.

Algorithmic Imperialism and Cognitive Control. The Indian Parliament's Standing Committee on IT (Report No. 331, 2025) described this as "algorithmic imperialism," warning opaque digital curation undermining

⁶⁸ INDIA CONST. art. 19(1)(a).

⁶⁹ U.N. Secretary-General, *Global Digital Compact*, U.N. Doc. A/79/1 (2024).

⁷⁰ GDPR, *supra* note 9.

democratic participation,⁷¹ a concern reflected in decisions of various High Courts.

Towards Decolonising Digital Governance. The UN OCHR Report on Digital Sovereignty treats data as a collective resource demanding equitable participation and benefit sharing.⁷² Thus, the right to be forgotten becomes part of a decolonial constitutional vision.

7. BEYOND ERASURE: TOWARDS A CONSTITUTIONAL FRAMEWORK OF DIGITAL FORGETTING IN INDIA

In the evolving digital republic, the RTBF goes beyond mere deletion toward recognising dignity that endures over time.

The DPDP Act, 2023,⁷³ marks India's first legislative move toward informational control but remains silent on defining the scope of RTBF. The DPDP Rules, 2025⁷⁴, notified under Section 40 of the DPDP Act, partially fill this gap by introducing Data Storage Limitation Registers, mandatory Data Expiry Schedules, and Oblivion-Compliance Audits for significant data fiduciaries, thereby operationalising a system in which data retention becomes the exception rather than the norm.⁷⁵ Meanwhile, the Supreme Court's e-Committee (2025) has initiated anonymisation of digital court records- a constitutionally significant step toward institutionalised forgetting.⁷⁶ The debate now extends to digital afterlife, which has been dealt with and addressed by the NHRC rules and the Delhi High Court. Worldwide, the UNESCO 2024 Report on Digital Ethics calls for *right to algorithmic oblivion* and reinforces that forgetting is essential to freedom in the age of machine memory.

8. COMPARATIVE ANALYSIS: GLOBAL APPROACH

The notion of the RTBF has developed unevenly across legal systems, reflecting divergent constitutional priorities and cultural understandings of privacy and free speech.

In the European Union, Article 17 of the GDPR⁷⁷, allows individuals to request deletion of personal data that is irrelevant or serves no purpose.⁷⁸ The

⁷¹ PARLIAMENT OF INDIA, STANDING COMM. ON INFORMATION TECHNOLOGY, REPORT NO. 331, para 42 (2025).

⁷² U.N. High Commissioner for Human Rights, *Report on Digital Sovereignty and Human Rights*, U.N. Doc. A/HRC/59/42 (June 2025).

⁷³ DPDP Act, *supra* note 4.

⁷⁴ DPDP Rules, *supra* note 5.

⁷⁵ Ministry of Electronics & Information Technology, *Draft Digital Personal Data Protection Rules*, rr. 7-12, 18, 21 (2025) (India).

⁷⁶ SUPREME COURT E-COMMITTEE, JUDICIAL DATA GOVERNANCE FRAMEWORK (2025), <https://cdnbbsr.s3waas.gov.in/s388ef51f0bf911e452e8dbb1d807a81ab/uploads/2025/05/20250530524370674.pdf>.

⁷⁷ GDPR, *supra* note 9.

⁷⁸ *Id.* art. 17.

FROM PERPETUAL DIGITAL MEMORY TO THE JURIDICAL PROMISE OF OBLIVION: A
CONSTITUTIONAL EXAMINATION OF THE RIGHT TO BE FORGOTTEN UNDER ARTICLE 21 305
CJEU in *Google Spain* case⁷⁹ treated search engines as “data controllers,”
mandating them to delist outdated content upon legitimate request, balancing
personal dignity with the collective interest in information access.

The United Kingdom, post-Brexit, has maintained an analogous framework
under the UK GDPR read alongside the Data Protection Act, 2018.⁸⁰ Though
British courts bend towards balancing individual privacy claims against
demands of journalism and historical record.

The United States is grounded in the First Amendment jurisprudence and
the commitment to public record transparency over any statutory or
constitutional right to be forgotten. In *Florida Star v. B.J.F.*,⁸¹ the court held
that truthful information lawfully obtained cannot be suppressed, regardless of
the harm that its publication inflicts, thus prioritising free expression over
digital oblivion.

India’s position is, however, somewhere in between. The *Puttaswamy*
case,⁸² laid the constitutional foundation for informational privacy within
Article 21; the DPDP Act provides partial statutory recognition, leaving scope
for future judicial development; even subsequent decisions in *the Dharamraj*
*Bhanushankar*⁸³ and *the Jorawar Singh Mundy*,⁸⁴ recognised selective digital
erasure where no legitimate public interest survives. But India has not fully
developed an infrastructure that would make RTBF operationally effective.
Overall, the EU and UK models institutionalise the right through data
protection systems; the U.S. subordinates it to expressive liberty; while India
attempts to balance privacy, reputation, and transparency through judicial
creativity in the absence of legislative direction, thus requiring urgent
legislation.

9. CONCLUSION: REIMAGINING ARTICLE 21 IN THE AGE OF PERPETUITY

Indian constitutional jurisprudence has always grown in responding to the
pressures of its time. Evolution from *Maneka Gandhi*⁸⁵ to *Puttaswamy*,⁸⁶
reflects how Article 21 has expanded from a procedural straitjacket into a
substantive protector of liberty, dignity, and privacy. Today, the digital reality
presents an urgent challenge. As personal data becomes a tool of control,

⁷⁹ *Google Spain*, *supra* note 1.

⁸⁰ Data Protection Act 2018, c. 12 (UK).

⁸¹ *Florida Star v. B.J.F.*, 491 U.S. 524 (1989).

⁸² *Puttaswamy*, *supra* note 2.

⁸³ *Dharamraj Bhanushankar Dave v. State of Gujarat*, SCA No. 1854 of 2015 (Guj. H.C.).

⁸⁴ *Jorawar Singh Mundy*, *supra* note 20.

⁸⁵ *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.

⁸⁶ *Puttaswamy*, *supra* note 2.

stigmatisation, and structural inequality, the right to be forgotten must be recognised as a constitutional necessity and not as a judicial concession.

The RTBF in India remains fragmented and procedurally fragile. Although the DPDP Act, 2023, constitutes a significant statutory milestone, its scope of circumscribed erasure is limited by wide exemptions under national security, legal obligations, and public interests.⁸⁷ The Act's silence on algorithmic inferential data, intermediary responsibility, and posthumous privacy creates a regulatory vacuum in the governance of “digital immortality” and highlights the essentiality of “forgetting.”

The DPDP Rules, 2025, partially address these gaps through *Data Expiry Schedules*, *Storage Limitation Registers*, and *Oblivion-Compliance Audits*, mandating periodic destruction of non-essential personal data, notifications prior to expiry, and auditable records of deletion—laying the groundwork for an ethical restraint in data retention.

Thus, the judiciary carefully balances personal dignity against transparency, open justice, and free speech, even extending Article 21 posthumously to protect privacy and memory, highlighting that human personhood is taken seriously. However, principled reasoning is itself not sufficient; the real challenge lies in translating this evolving jurisprudence into a proper legislative structure—one that ensures that the right to be forgotten receives a institutional grounding than just leaving it as a doctrinal desire.

10. SUGGESTIONS AND WAY FORWARD

The constitutional evolution of RTBF demands convergence between judicial creativity, legislative clarity, and ethical governance. There is thus the need to expand Article 21's ambit to address digital dignity, algorithmic privacy, and protection of posthumous identity in the digital era. Pending codification, the Supreme Court may exercise its extraordinary jurisdiction by issuing interim guidelines under Article 142⁸⁸ to balance privacy with free expression.

In order to protect individuals from targeted manipulation, the DPDP Act, 2023⁸⁹ should be strengthened by expressly defining RTBF with time frames, independent review mechanisms, and public-interest exemptions. Introducing a chapter on algorithmic privacy and mandating ‘data expiry by design’ would ensure automatic deletion once data expires.⁹⁰ Institutional strengthening is equally important: the Data Protection Board must be given limited suo moto erasing powers, and bodies such as Public Memory Ombudsman and National Digital Memory Authority should also be established to monitor ethical

⁸⁷ DPDP Act, *supra* note 4, s. 12.

⁸⁸ INDIA CONST. art. 142.

⁸⁹ DPDP Act, *supra* note 4, ss. 14-18.

⁹⁰ OECD, DIGITAL POLICY REPORT (2024).

archiving, deletion of posthumous data and platform accountability. Media organisations and AI developers must observe the ethical protocols for digital likenesses, which ensure permission, sensitivity, and contextual integrity.⁹¹

India's framework should be aligned with GDPR Article 17⁹², while ensuring constitutional proportionality. A National Digital Dignity Charter and Index may serve as tools for assessing ethical data practices, and universities may establish Digital Rehabilitation Clinics to assist in digital redressal.⁹³ The right must also seek to address significant gaps that are unaddressed—the Right to Digital Silence, Community Data Sovereignty, and a humane Right to Data Mercy—offering pathways to address coerced visibility, distorted cultural narratives, and unjust digital stigma.⁹⁴ In long run, Digital Forgetting Architecture—combining anonymisation of APIs, expiration mechanisms, and real-time erasure models into search engines and state databases—must be engineered as a legal obligation rather than as a technical afterthought.

Ultimately, in an algorithmically governed world, Article 21 must serve as a constitutional bridge between technological capability and human dignity. Forgetfulness, when carefully calibrated, is not a threat to history but a precondition for fairness.

As the closing reflection rightly captures, “*The dignity of life depends not only on what we choose to remember, but also on what we allow to be forgotten.*”

BIBLIOGRAPHY

Case Laws

- *Aishwarya Rai Bachchan v. State of Madras*, AIR 1950 SC 27.
- *Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*, Case C-131/12, Court of Justice European Union (2014).
- *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.
- *K.S. Puttaswamy v. Union of India (Aadhaar)*, (2019) 1 SCC 1.
- *Sourav Das v. Union of India*, 2023 SCC OnLine SC 677.
- *State of Punjab v. Gurmeet Singh & Ors.* (1996) 2 SCC 384.
- *Subhranshu Rout v. State of Odisha*, BLAPL No. 4592/2020, High Court of Orissa (2020).
- *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221.
- *Vasu Vasanthan v. Registrar General*, W.P. No. 62038/2016, High Court of Karnataka (2017).
- *Vysakh K.G. v. Union of India*, W.P. (C) No. 26500/2020, Kerala High Court (2021).

⁹¹ SUPREME COURT E-COMMITTEE, *supra* note 83.

⁹² GDPR, *supra* note 9, art. 17.

⁹³ NITI AAYOG, AI ETHICS FOR BHARAT (2025).

⁹⁴ *X v. Registrar General*, 2022 SCC OnLine Mad 1764.

- *Zulfikar Ahmad Khan v. Quint Digital Media Ltd.*, 2019 SCC OnLine Del 8494.

Statutes, Conventions, and Reports

- Constitution of India, 1950.
- Information Technology Act, 2000.
- Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
- European Union General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
- Justice B.N. Srikrishna Committee, *Report of the Committee of Experts on Data Protection Framework for India*, Ministry of Electronics and Information Technology (2018).
- *United Nations Human Rights Council Resolution on the Right to Privacy in the Digital Age*, A/HRC/RES/68/167 (2013).
- Internet Freedom Foundation, *Analysis of the Digital Personal Data Protection Act 2023* (Policy Report).

Online Sources

- Ministry of Electronics and Information Technology (MeitY), “*Digital Personal Data Protection Act, 2023*” – available at: <https://www.meity.gov.in/>
- Supreme Court of India e-Committee, “*Policy on Judicial Data and Anonymisation*” (2023) - <https://ecommitteesci.gov.in/>
- United Nations Human Rights Office, “*The Right to Privacy in the Digital Age*” (OHCHR Report, 2021) - https://www.ohchr.org/en/ohchr_homepage
- Anjani Agarwal & Aman Singh, “*The right to be forgotten under the digital personal data protection act, 2023 : A missed opportunity in India’s data privacy regime*”, *International Journal of Law*, Vol. 11 (2025).
- Prashant Mali., “*Privacy Law: Right to Be Forgotten in India*” *NLUI Law Review*, Vol. VII (2018).
- Internet Freedom Foundation, *RTBF and Indian Jurisprudence: Challenges in Implementation*, Policy Brief (2022).