



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

RIGHT TO BE FORGOTTEN IN INDIA

Anshu Meena

1. INTRODUCTION

The fundamental principle of human memory is naturally imperfect, it is built to gradually forget, filter and heal. However, this natural human tendency has been superseded by absolute permanent data retention due to rise of the digital age. Individual achievements, structural errors and private moments are today captured indefinitely in the global internet. This transition from physical solitude to permanent digital records has completely changed the traditional concept of personal liberty.

In the era of data that outlives its context, The Right to be Forgotten (RTBF) has emerged from being just a statutory mechanism to a core element of digital dignity. The RTBF ensures individual are not permanently chained to a static digital history by allowing them to evolve, rehabilitate and reclaim their public identity.

2. RIGHT TO BE FORGOTTEN

At its core, the Right to be Forgotten is an individual's right to request the removal, de-indexing, or erasure of their personal data from public internet searches and commercial databases once that information is no longer accurate, necessary, or legally relevant. Legally, it is crucial to distinguish between complete source erasure and search engine de-indexing. While source erasure destroys the underlying data from the host website, de-indexing—popularized by early search engine litigation—leaves the source intact but severs the search link. This ensures the data cannot be surfaced by a simple search of the individual's name.

The jurisprudential roots of this concept trace back to the foundational right to "informational privacy," an extension of the classic "right to be let alone" articulated by Samuel Warren and Louis Brandeis. In a modern context, this right addresses the asymmetrical power dynamics between individual citizens and corporate data processors. It recognizes that personal identity

is dynamic, and that individuals suffer distinct psychological and economic harm when an unchangeable digital profile permanently dictates their public standing.

3. THE FACETS OF DIGITAL DATA

For a better understanding personal data can be classified into three categories based on how it entered into the public domain. Each category has its own way of balancing individual privacy and competing public interests.

I: Voluntarily Uploaded Data

This encompasses all kinds personal information such as images, thoughts and profiles, etc. that a person directly and voluntarily uploads to internet platforms. Here the legal concern rests entirely on the autonomy of consent. The user has a fundamental right to revoke their consent as long as there isn't a conflicting legal requirement to keep data. When the user withdraws their consent, the platform is bound to erase it.

II: Reported Data

This category contains information published by journalists, news portals and digital media houses that is non voluntary and third party originated. When first published this information may have been true, but overtime it can become deceptive, outdated or irrelevant. The legal analysis here shifts from pure consent to evaluating Accuracy vs. Relevance, requiring courts to determine when truthful historical reporting turns into unjust, persistent public bias. For example, an archive news article on an initial arrest can cause irreversible harm if the person later found not guilty of any charges, but the original article still appears at the top of search engine results. The legal analysis here shifts from pure consent to evaluating Accuracy vs. Relevance, requiring courts to determine when truthful historical reporting turns into unjust, persistent public bias.

III: Institutional and Legal Data

This category comprises formal records produced by state machinery, namely court rulings, orders, police registries and official gazette notification. The obligation for public, verifiable legal documents and the open court concept protect this data. This is the category that contains conflict between state interest in preserving legal records and individual's right to personal rehabilitation. This conflict is deeply structural because an individual acquitted of a

crime or any legal dispute who seeks to remove their name from online judgement repositories to escape social stigma and preserve their employment opportunities is unable to do so.

4. ORIGIN OF RTBF

The modern legal framework for the RTBF was established by the Court of Justice of the European Union (CJEU) in the foundational case of *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)* (2014).¹ The CJEU ruled that search engine operators are data controllers and must, upon request, remove links to web pages containing personal data if that information is inadequate, irrelevant, or excessive in relation to the purposes for which it was processed. This landmark judicial rule was formally codified in Article 17 of the General Data Protection Regulation (GDPR) as the "Right to Erasure," creating a clear statutory path for citizens to manage their digital footprints.

5. THE INDIAN LEGAL REVOLUTION

The RTBF was included in the existing framework of fundamental rights before the introduction of explicit data protection laws. The historic nine-judge bench decision in *Justice K.S. Puttaswamy v. Union of India* (2017), which unanimously declared the Right to Privacy an intrinsic part of the Right to Life and Personal Liberty under Article 21 of the Constitution marked a turning point. The Supreme Court in this judgement recognized informational privacy as an essential component of this right. The court also acknowledged that an individual should have control over their digital narrative and that the right to protect one's reputation includes a qualified right to be forgotten.

Following *Puttaswamy*, various High Courts began addressing practical applications of the RTBF, particularly in cases like *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.*², the Delhi High Court recognized the need to grant interim relief by directing the removal of damaging articles while a case was being resolved, establishing that a clean professional reputation is an essential element of Article 21.

The High Courts in India have increasingly faced petitions from individuals cleared of criminal charges. These petitioners contend that the permanent online availability of their

¹ *Google Spain SL v. Agencia Española de Protección de Datos*, Case C-131/12, [2014] E.C.R. 317.

past legal struggles ruins their employment and personal prospects. Courts have constantly adopted a balancing approach by directing legal platforms to conceal names or de-index judgments when the public interest in the record is minimal when compared to the personal harm caused.

For instance, in the writ petition *Sri vasunathan v The Resistrar-General*³ before the Karnataka High Court, the court observed that “This would be in line with the trend in western countries of the 'right to be forgotten' in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned.” Therefore, the court instructed its registry that the name of the petitioner’s daughter should not appear in the criminal petition body or case title.

Contrary to the aforementioned ruling, The Gujarat Hight court noted in *Dharamraj Dave v. State of Gujarat* that the petitioner lacks sufficient evidence to demonstrate that "uploading judgment on the Internet is a violation of Article 21 of the Constitution" and that there is no applicable law to remove judgments from Google searches or Indian Kanoon. These examples highlight the judiciary's incapacity to interpret the right to be forgotten and the absence of a legal framework. Therefore, in order to safeguard the right to be forgotten, India needs particular data protection laws.

The petitioner lacks sufficient evidence to demonstrate that “uploading judgement on the internet is a violation of Article 21 of the Constitution” and that there is no applicable law to remove judgements from Google searches or Indian kanoon. Cases like these highlighted the need for particular legal framework for the safeguarding right to be forgotten.

THE DPDP ACT, 2023

The legislative landscape shifted fundamentally with the enactment of the Digital Personal Data Protection (DPDP) Act, 2023. This statute provides India's first dedicated framework for digital personal data.

The RTBF is explicitly provided in Section 12 of the DPDP Act, 2023, which establishes the *Right to Correction, Completion, and Erasure* of personal data. Under this provision, a Data Principal (the individual) has the right to request that a Data Fiduciary (the data collector or platform) erase personal data that is no longer necessary for the specific purpose for which it was collected, or data for which consent has been withdrawn.

³ *Sri Vasunathan v. The Registrar General*, 2017 SCC OnLine Kar 424.

The DPDP Act also provides some limitations. Obligations of section 12 do not apply if such data is necessary for enforcing a legal right, fulfilling a statutory obligation, or serving specific state-mandated exemptions. The enforcement of these rights is supervised by the Data Protection Board of India (DPBI), which acts as the adjudicating body for data disputes.

6. THE CONSTITUTIONAL TUG OF WAR

As much as this right is required in this digital age, its enforcement creates a direct, structural conflict between two fundamental rights within the Indian Constitution that are the Right to Privacy (Article 21) and the Right to Freedom of Speech and Expression (Article 19(1)(a)), which includes the public's right to information and the freedom of the press. The right of public to seek, receive and impart information, as well as the freedom of media to report and archive events holds great importance for a transparent society and open access to justice.

To resolve this conflict, Indian courts use a strict Proportionality and Balancing Test. The RTBF is never treated as an absolute right instead; it must be balanced against the social utility of the information in question.

When determining whether data should be forgotten, the judiciary evaluates several core criteria such as the nature of the Information, Information regarding heinous crimes, systematic financial fraud, or deeply impactful historical events is preserved to protect public safety and history. Conversely, details of minor infractions, settled family disputes, or unproven allegations lean heavily toward erasure. And the Context of Time, Courts assess whether the information continues to serve a valid public purpose or has become purely punitive, serving no purpose other than to damage an individual's reputation.

7. CHALLENGES

Implementation of the RTBF faces severe technical and systemic hurdles. Such as-

- **The Streisand Effect:** A digital phenomenon where an individual's formal legal attempt to suppress, delete, or hide a piece of information inadvertently draws widespread public attention to it, causing it to be mirrored and shared across multiple alternative platforms.
- **Web Archives and Scraping:** Even if a primary publisher removes an article or Google de-indexes a link, the information often remains perfectly preserved on web

archives (such as the Wayback Machine) or stored within independent data-scraping networks that operate outside conventional jurisdictions.

- **Intermediary Burden:** Forcing search engines to act as the primary adjudicators of removal requests create a dangerous operational dynamic. If platforms face steep penalties under the DPDP Act for failing to erase data, they may choose to over-comply. These risks turning private corporations into automated digital censors, quietly deleting valid public information to protect themselves from legal liability.

8. CONCLUSION

The Right to be forgotten is a necessary legal response to the challenges of permanent digital storage. India's transition from the landmark declarations of *Puttaswamy* to the structured statutory provisions of Section 12 of the DPDP Act, 2023, shows a clear national commitment to preserving individual dignity within the digital economy.

The future of this right in India relies on the regulatory precision of the Data Protection Board and the balanced judgment of its courts. The RTBF must never be permitted to become a tool used by public to alter inconvenient truths or rewrite historical records. Rather, it has to be maintained as a targeted equitable remedy. India can create a digital environment that respects both historical transparency and the fundamental right to a second chance.