
RIGHT TO BE FORGOTTEN IN INDIA: RECONCILING INFORMATIONAL PRIVACY WITH THE RIGHT TO FREEDOM OF SPEECH

Niharika Pathak, B.A. LL.B., Faculty of Law, SMS Law College

ABSTRACT

The right to be forgotten (“RTBF”) has emerged as one of the most contested frontiers of informational privacy in India. Rooted in the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India*, the RTBF seeks to empower an individual to prevent the continued digital circulation of personal information that is outdated, irrelevant, or no longer serves any public purpose. Yet the very architecture of the internet, coupled with India's constitutional commitment to freedom of speech and expression under Article 19(1)(a) and the principle of open justice, resists any straightforward transplantation of this right. This paper traces the doctrinal origins of the RTBF, examines the divergent approach taken by the Gujarat, Karnataka, Kerala and Delhi High Courts, evaluates the limited statutory recognition granted under Section 12 of the Digital Personal Data Protection Act, 2023, and situates the Indian position against the European Union's General Data Protection Regulation. It argues that the absence of a codified, judicially administrable standard has produced inconsistency and unpredictability, and proposes a structured proportionality framework drawing on the legality-necessity proportionality test laid down in *Puttaswamy* through which courts and future legislation may reconcile the dignitarian interest in being forgotten with the public's continuing interest in information, transparency and free expression.

Keywords: Right to be Forgotten, informational privacy, Article 21, Article 19(1)(a), Digital Personal Data Protection Act 2023, open justice, proportionality.

I. INTRODUCTION

The internet does not forget the way human memory does. A conviction later overturned, an FIR later quashed, a divorce long since settled, or a photograph shared in youthful indiscretion continues to surface in a search engine result years even decades, after the underlying event has lost all contemporary relevance. This permanence of digital memory sits uneasily with the constitutional value that Indian courts have, since 2017, treated as central to human dignity: the right to privacy. Out of this tension has grown the idea of a “right to be forgotten” -the claim of an individual to have particular personal information de-indexed, delinked, or erased from public digital circulation once it ceases to serve any legitimate current purpose.

India's engagement with the RTBF has been halting and inconsistent. Unlike the European Union, which has both a judicially articulated right (the Google Spain judgment of the Court of Justice of the European Union) and a codified one (Article 17 of the General Data Protection Regulation, “GDPR”), India has proceeded almost entirely through fragmented High Court orders, several of which point in opposite directions. The Digital Personal Data Protection Act, 2023 (“DPDP Act”) has, for the first time, introduced a statutory right of erasure, but one considerably narrower than its European counterpart. Meanwhile, the constitutional guarantee of free speech and expression under Article 19(1)(a), together with the principle of open justice and the public's right to know, continues to pull in the opposite direction, resisting any right that would allow individuals to sanitise the public record.

This paper examines how Indian law has attempted and largely failed to reconcile these two competing constitutional values. Part II lays out the conceptual distinction between informational privacy and the RTBF. Part III traces the constitutional foundation laid in Puttaswamy. Part IV surveys the divergent judicial trajectory across High Courts. Part V examines the countervailing weight of free expression and open justice. Part VI analyses the statutory response under the DPDP Act and compares it with the GDPR. Part VII proposes a reconciliatory framework, and Part VIII concludes.

II. CONCEPTUAL FOUNDATIONS: INFORMATIONAL PRIVACY AND RIGHT TO BE FORGOTTEN

Informational privacy refers to an individual's ability to control the collection, use, and dissemination of information about themselves. It is broader than the RTBF, which is best

understood as one specific application of informational privacy to the problem of digital permanence the phenomenon by which information, once published online, becomes searchable, indexable, and effectively permanent, regardless of whether it retains any contemporary relevance to the individual it concerns.

The RTBF is conceptually distinct from a right to erasure of unlawfully obtained data (which is uncontroversial) and from a right to rectify inaccurate data (equally uncontroversial). Its more difficult and contested form concerns information that was true and lawfully published at the time, but which the individual argues should nonetheless be delinked or suppressed because of the passage of time and the disproportionate harm its continued visibility now causes. It is this contested form sometimes described as a “right to be let alone” in the digital sphere that has animated the Indian litigation discussed below.

III. CONSTITUTIONAL BASIS: THE PUTTASWAMY FOUNDATION

The constitutional starting point for any discussion of the RTBF in India is the nine judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India. The Supreme Court unanimously held that the right to privacy is a fundamental right protected under Article 21, and is also traceable to the freedoms guaranteed under Article 19 and to the guarantee of equality under Article 14. Overruling the earlier positions taken in *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh*, the Court held that privacy is an intrinsic and inalienable part of human dignity and personal liberty.

Critically for present purposes, the Court held that any state incursion into the right to privacy must satisfy a three-fold test of legality, necessity and proportionality: the restriction must be backed by law, must pursue a legitimate state aim, and the means adopted must be proportionate to that aim. Although Puttaswamy did not itself decide a right-to-be-forgotten claim, several of the concurring opinions expressly recognised informational privacy including control over the dissemination of personal data as falling within the protective umbrella of Article 21. This dictum has since been treated by High Courts, and by the drafters of India's data protection legislation, as the constitutional wellspring from which a right to be forgotten may be said to flow, even though the Court did not lay down its contours.

IV. JUDICIAL TRAJECTORY: A DIVIDED HIGH COURT RESPONSE

In the absence of Supreme Court authority squarely on point, or of a statute occupying the field

until 2023, the task of giving content to the RTBF fell to the High Courts. Their responses have been markedly inconsistent.

a) Dharamraj Bhanushankar Dave v. State of Gujarat (2017) - Refusal

In the first Indian case to squarely raise the issue, the petitioner who had been acquitted of serious charges including murder and kidnapping sought to restrain Google and the legal database Indian Kanoon from continuing to display the judgment recording his trial, arguing that its continued visibility, years after his acquittal, was harming his personal and professional prospects, including an ongoing visa application. The Gujarat High Court dismissed the petition, holding that the publication of a judgment that formed part of the public record did not violate Article 21, and that the High Court Rules in any event permitted third parties to obtain copies of such judgments. The Court declined to recognise a free-standing right to be forgotten in the absence of any statutory foundation for it.

b) Sri Vasunathan v. Registrar General, High Court of Karnataka (2017) - Recognition

Decided only days after Dharamraj Dave, the Karnataka High Court reached the opposite conclusion on markedly different facts. The petitioner sought removal of his daughter's name from the cause title of a criminal case (concerning an annulled marriage and allegations of forgery and extortion) that continued to surface in internet searches. The Court directed the Registry to ensure that no internet search would reveal her name, reasoning that this accorded with the “sensitivity” attached to matters involving women in cases touching upon their modesty and reputation, and treated the RTBF as an emerging facet of the right to privacy, albeit one to be applied narrowly and in appropriate categories of cases such as those involving women and sexual offences.

c) The Kerala High Court Line of Cases - Victim Anonymity

The Kerala High Court has, across a series of orders beginning in 2016 and continuing through subsequent petitions, directed the online legal database Indian Kanoon to remove or redact the names of rape victims and other similarly placed litigants from published judgments, reasoning that the victim's right to privacy and dignity outweighs the public's interest in identifying her, and that the statutory bar on disclosure of a rape victim's identity under the Indian Penal Code

framework reinforces this outcome. In later proceedings, the Kerala High Court also permitted litigants in family and in-camera matters to seek redaction of identifying details from judgments hosted online, while cautioning that the right to be forgotten is not absolute and must be weighed against the public's right to know a balancing exercise the Court suggested was, in the long run, better performed by the legislature than through ad hoc judicial orders.

d) Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd. (Delhi High Court, 2019)

The Delhi High Court went a step further, holding that the right to privacy includes within it a “right to be let alone,” and restraining the republication of articles concerning allegations that had already been removed by the original publisher pursuant to a settlement. While the case did not concern search-engine de-indexing in the manner of the Gujarat and Karnataka disputes, it is frequently cited as affirming that the RTBF and the associated right to be let alone form part of the constitutional privacy guarantee recognised in Puttaswamy.

e) Recent Developments (2025–2026)

The trend toward judicial recognition has continued into 2025 and 2026, with reports of a Delhi trial court directing the de-indexing of online material naming an individual who had been fully exonerated in a money-laundering investigation, on the ground that continued visibility of the material served no legitimate purpose and caused ongoing reputational harm. At the same time, the Supreme Court has, in a separate matter concerning the removal of news reports and judicial records from public databases, stayed a High Court order invoking the RTBF, underscoring the unsettled and evolving character of the doctrine and the institutional discomfort with courts fashioning erasure remedies in the continued absence of clear legislative guidance.

Taken together, this body of case law reveals not a coherent doctrine but a spectrum of outcomes turning heavily on the facts before each court: claims concerning sexual offence victims and minors have tended to succeed, while claims by acquitted persons seeking removal of ordinary criminal judgments from public legal databases have met a more sceptical reception, precisely because such judgments form part of the public record and their transparency serves the administration of justice.

I. THE COUNTERVAILING CONSTITUTIONAL INTEREST: FREE SPEECH, THE PRESS, AND OPEN JUSTICE

Any Indian articulation of the RTBF must contend with the fact that Article 19(1)(a) guarantees freedom of speech and expression, understood by the Supreme Court to encompass both the right of the press to publish and the reader's or listener's right to receive information. Article 19(2) permits only narrowly defined restrictions on this freedom, and courts have historically been reluctant to expand this list through judicial innovation.

Three distinct strands of this countervailing interest recur in the case law and commentary. First, the principle of open justice: judicial proceedings and judgments are, as a rule, matters of public record, and their availability enables public scrutiny of the judicial process, deters arbitrary exercise of power, and allows litigants, researchers and future courts to rely upon precedent. An unqualified right to have inconvenient judgments de-indexed threatens this transparency function directly a concern that animated the Gujarat High Court's refusal in *Dharamraj Dave* and continues to inform the Supreme Court's caution in more recent proceedings.

Second, freedom of the press and of legal publishing: databases such as Indian Kanoon perform a public function by making the corpus of Indian case law freely searchable, a task previously the preserve of expensive private law reports. Treating such platforms as susceptible to erasure orders on a case-by-case basis risks converting them into arbiters of whose past is convenient to display, a role ill-suited to their function as neutral repositories of public record.

Third, the public's right to know, particularly in matters of public interest -the conduct of public officials, matters of financial probity, or information relevant to an individual's fitness for public office or trust which the RTBF cannot be permitted to override merely because the information has become embarrassing or inconvenient to the individual concerned. The European experience under the GDPR similarly excludes information published for journalistic purposes or in the public interest from the ambit of erasure, a qualification that Indian courts have implicitly recognised in distinguishing between cases involving vulnerable individuals and cases involving persons seeking to suppress a matter of continuing public relevance.

II. THE STATUTORY RESPONSE: SECTION 12 OF THE DPDP ACT AND THE COMPARATIVE GDPR POSITION

The Digital Personal Data Protection Act, 2023 represents India's first comprehensive data protection statute, and Section 12 introduces, for the first time, a codified right of correction and erasure. Under Section 12(3), a Data Principal may request a Data Fiduciary to erase personal data, and the Data Fiduciary is obliged to comply unless retention is necessary for the specified purpose for which the data was collected or for compliance with any other law in force.

This statutory right, however, is considerably narrower than the RTBF as litigated before the High Courts, in at least three respects. First, it applies only to personal data that the individual has previously consented to the processing of it does not extend to information published by the press, hosted on public legal databases, or otherwise disseminated without the individual's consent, which is precisely the category of information at issue in *Dharamraj Dave*, *Vasunathan* and the Kerala line of cases. Second, it is triggered only by withdrawal of consent or cessation of purpose, unlike the broader European right, which extends to objections grounded in the data no longer being necessary, unlawful processing, or a simple decision by the individual that continued retention is no longer justified. Third, it operates purely between a Data Principal and a Data Fiduciary in a data-processing relationship, and offers no mechanism at all for addressing search-engine indexing of judicial records or news archives - the very fact pattern that has generated the bulk of Indian RTBF litigation.

By contrast, Article 17 of the GDPR, given judicial content by the Court of Justice of the European Union in *Google Spain SL v. Agencia Española de Protección de Datos*, obliges search engine operators to de-index links to personal data on request where the data is inadequate, irrelevant, excessive, or no longer relevant, subject to an express carve-out where continued availability is justified by the public interest, including the interest in freedom of expression. The European framework thus directly addresses the search-engine de-indexing scenario that dominates Indian litigation, while also building in the free-expression counterweight through an express statutory exception a structural feature that Indian law, whether judicial or statutory, has yet to replicate with comparable precision.

The consequence is a significant lacuna: the category of RTBF claim that Indian litigants most frequently bring de-indexing of judgments, news reports and FIRs from public and quasi-

public databases remains almost entirely unaddressed by the DPDP Act, leaving courts to continue improvising on a case-by-case basis, as the Supreme Court's 2026 stay order illustrates.

III.TOWARDS RECONCILIATION: A PROPORTIONALITY FRAMEWORK

The preceding survey suggests that Indian law currently lacks a stable, principled method for adjudicating RTBF claims, resulting in outcomes that vary more with the identity of the forum than with any articulated legal standard. This paper argues that the legality-necessity-proportionality test articulated in *Puttaswamy* developed originally to govern state incursions into privacy offers a workable template for reconciling the RTBF with Article 19(1)(a), and could usefully structure both future judicial reasoning and any legislative amendment extending Section 12 of the DPDP Act to non-consensual publication.

Four factors, drawn from the comparative experience and from the pattern already visible in Indian case law, merit express incorporation into such a framework. First, the nature of the individual concerned: courts have been considerably more willing to grant relief to victims of sexual offences, minors, and other especially vulnerable claimants, as the Kerala and Karnataka decisions illustrate, than to persons merely embarrassed by a lawfully published record of their own conduct. Second, the public interest in the information: information touching upon the exercise of public power, financial probity, or an ongoing matter of public concern should generally resist erasure, whereas purely private information that has lost all contemporary relevance presents a stronger case for delinking. Third, the passage of time and continued relevance: the longer an event recedes into the past without contemporary bearing on the individual's conduct or public role, the weaker the justification for its continued prominent visibility. Fourth, the nature of the platform and the remedy sought: a targeted order directing search-engine de-indexing, of the kind fashioned by the Karnataka High Court, interferes far less with the underlying public record and with press freedom than an order directing wholesale removal of a judgment from a legal database, a distinction the Gujarat High Court's reasoning implicitly endorses.

A legislative solution remains preferable to continued judicial improvisation. Parliament could usefully amend the DPDP Act, or enact a standalone provision, to extend a structured right of de-indexing to search engines and legal databases in defined categories of case particularly those involving sexual offence complainants, minors and matters of purely private character

while expressly excluding judgments and records bearing on matters of continuing public interest, public office, or ongoing legal proceedings, mirroring the public-interest exception already built into the GDPR. Until such legislative clarity emerges, courts would do well to articulate, in each RTBF decision, an explicit application of the proportionality factors above, so that the resulting body of precedent offers genuine guidance rather than a set of fact-specific outcomes difficult to reconcile with one another.

IV. CONCLUSION

The right to be forgotten sits at the intersection of two constitutional commitments that Indian law values highly and has, until now, struggled to reconcile: the dignitarian promise of privacy recognised in *Puttaswamy*, and the equally foundational guarantee of free expression and open justice under Article 19(1)(a). The High Courts have responded to this tension inconsistently recognising the right readily in cases touching upon sexual offence victims and minors, while resisting it firmly where litigants seek to erase an ordinary, lawfully published judicial record. The DPDP Act's Section 12, while a welcome first step toward codification, does not reach the search engine and legal-database scenarios that dominate Indian RTBF litigation, leaving the field largely to case-by-case judicial development. A structured proportionality framework, attentive to the vulnerability of the claimant, the public interest in the information, the passage of time, and the precision of the remedy sought, offers the most promising route toward a coherent Indian doctrine one that neither permits the internet to become an instrument of permanent digital punishment, nor allows privacy claims to erode the transparency on which public accountability and the rule of law ultimately depend.

REFERENCES

1. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.
2. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
3. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
4. Dharamraj Bhanushankar Dave v. State of Gujarat & Ors., Special Civil Application No. 1854 of 2015 (Guj. HC, judgment dated 19 January 2017).
5. Sri Vasunathan v. The Registrar General, High Court of Karnataka & Ors., Writ Petition No. 62038 of 2016 (Kar. HC, judgment dated 23 January 2017); 2017 SCC OnLine Kar 424.
6. X v. Registrar General, Kerala High Court, Civil Writ Petition No. 9478 of 2016 (interim orders, 2016–2021).
7. Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd. & Ors., CS (OS) 642 of 2018 (Del. HC, order dated 9 May 2019).
8. Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, CJEU (2014).
9. The Digital Personal Data Protection Act, 2023, § 12.
10. General Data Protection Regulation (EU) 2016/679, Article 17.
11. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.