



Judicial Recognition of the Right to be Forgotten in India: A Doctrinal and Comparative Analysis

Yash Sharad More

LL.M. (Constitutional Law)

Dr. Ambedkar College of Law,

Chhatrapati Sambhajanagar

+917057170024/ moreyash53@gmail.com

ABSTRACT

Digital info is now permanent and always there, putting the Right to be Forgotten (RTbF) at the heart of today's legal talks. The EU supports this with their GDPR, thanks to the big Google Spain case from 2014. But India? They don't have anything like that yet. This piece looks into whether India's Constitution can support the RTbF. After all, the huge nine-judge panel in the 2017 Puttaswamy case said privacy includes control over your personal info. Without top court guidance though, lower courts are pretty much feeling it out. Plus, there's the Digital Personal Data Protection Act from 2023. Despite its intentions, it falls short in key areas, notably not requiring de-indexing, which is a biggie for RTbF, and its enforcement mechanisms are still super basic.. This paper looks at European, UK, Brazilian, and American legal frameworks to suggest a proportionality-based model for balancing right to forget (RTbF) and freedom of expression as outlined in Article 19 (1) (a). It's a doctrinal study that ends with tailored suggestions for updating laws, shaping court guidelines, and boosting institutions to fit India's needs.

Keywords: *Right to be Forgotten, Informational Privacy, Article 21, DPDPA 2023, Proportionality, De-indexing, Puttaswamy, GDPR, Data Protection, Freedom of Expression*

1. Introduction

The internet doesn't forget. Unlike human memory, which fades, reshapes, and eventually lets go of old stuff, digital systems keep info forever, easily accessible to everyone. Things like old crimes, awkward posts, or private court records stay out there indefinitely, possibly haunting people for life. These details could dramatically impact how employers, loan givers, and random people see you. The contrast between how humans remember and how computers do has created the Right to be Forgotten. It gives individuals the right to ask for removal or de-indexing of personal info that's outdated, out of context, or just irrelevant.

In 2014, the European Court of Justice held in Google Spain SL v. Agencia Española de Protección de Datos that Search engines operate as data controllers and must take legal



responsibility for removing personal info when an individual's privacy is more important than the public's right to see it. Two years after that, Article 17 of the EU's General Data Protection Regulation made this right official across all member states, including detailed criteria, exceptions, and enforcement methods. Since then, the right to be forgotten has drawn a lot of judicial and legislative attention in Brazil, China, the UK, and increasingly in India.

India's involvement with the Right to Forget (RTbF) is seen in its constitutional rulings rather than separate laws. After many years of slowly recognizing it, the Supreme Court's nine-judge panel in *Puttaswamy* (2017) said privacy is a fundamental right under Article 21. They pointed out that controlling personal data is a big part of this privacy right. This set up the legal support needed for the RTbF. Yet, the country's first overall data protection law, the Digital Personal Data Protection Act of 2023, doesn't fully implement an RTbF framework. It offers a limited right to have information erased but doesn't require search engines to remove content. Plus, the group in charge of enforcing this law hasn't even been formed yet.

In this situation, Indian High Courts have dealt with RTbF claims separately. They've granted relief in cases of acquittals and domestic violence but not in other situations, all without a consistent set of guidelines. The Supreme Court is noticeably silent on this too. So, this paper looks at the constitutional, comparative, and legislative aspects of RTbF in India and suggests a practical approach based on principles.

2. Scope and Limitation

This study focuses on the digital aspects of RTbF, looking at search engines, online news archives, social media, and court record databases. It doesn't cover physical archives or government files, nor does it deal with criminal record expungement, except when these come up incidentally in case law analysis. The comparison zeroes in on the EU, UK, US, Brazil, and China—chosen for their direct relevance to the Indian legal framework.

This research follows legislative and judicial developments up to mid-2024 but doesn't include any updates from after that point. Since the DPDPA 2023 was recently enacted and the Data Protection Board of India isn't operational yet, there's no empirical data on enforcement patterns available. So, the study only looks at doctrine-based analysis. It mentions issues specific to minors' data protection, but doesn't go into detail about them. The paper does discuss how the right to fair access to information intersects with artificial intelligence, but it's more about the structure and doesn't analyze AI-specific liability frameworks technically.



3. Objective

The present research is guided by the following objectives:

- I. To examine the constitutional foundations of the RTbF under Articles 19 and 21, tracing the judicial evolution from Kharak Singh (1963) through Maneka Gandhi (1978) to the Puttaswamy nine-judge bench (2017).
- II. To critically survey Indian High Court RTbF judgments—Dharamraj Bhanushankar Dave, Vasunathan, Jorawar Singh Mundy, Zulfiqar Haider, and Nilofar Khan—identifying doctrinal inconsistencies and unresolved questions.
- III. To evaluate the DPDPA 2023 against international benchmarks, particularly the GDPR, identifying legislative gaps requiring reform.
- IV. To conduct a comparative analysis of RTbF frameworks across the EU, UK, US, Brazil, and China, extracting contextually relevant lessons for India.
- V. To develop a structured proportionality framework for resolving conflicts between the RTbF and freedom of expression under Article 19 (1) (a).
- VI. To formulate legislative, judicial, and institutional recommendations for an effective, contextually appropriate RTbF framework in India.

4. Hypothesis

This research proceeds on four working hypotheses:

- H1:** The Right to Be Forgotten is part of the fundamental right to privacy in Article 21, as explained in Puttaswamy. So, it's a constitutional right on its own, not depending on any specific law.
- H2:** The DPDPA 2023 marks some legislative progress but doesn't offer a solid foundation for the RTbF in India. It fails because it lacks a clear de-indexing requirement, has broad exceptions, and its enforcement structure is non-operational.
- H3:** To solve conflicts between the RTbF and freedom of expression, we use a structured proportionality analysis. This looks at how sensitive info is and whether the subject is public or private. It also considers time passed and shown harm, plus if the asked-for remedy fits all these factors proportionately.
- H4:** An Indian RTbF framework should fit the country's constitutional values and real institutional stuff, accounting for issues like caste-based bias and online violence against women, not just copy the European one.



5. Methodology

This research uses a doctrinal legal approach. It looks at primary sources like India's Constitution, rulings from the Supreme Court and High Courts, and key laws—such as the IT Act 2000, IT Rules 2021, and DPDPA 2023. Also included are international standards like the GDPR, ICCPR, and ECHR. For secondary info, it draws on academic law reviews, expert committee reports, particularly the Justice Srikrishna Committee Report from 2018, and government policies. Legal databases used are SCC Online, Manupatra, LexisNexis, Westlaw, and HeinOnline, for both domestic and international stuff..

Comparative legal analysis is used to examine Restriction on Broadcasting and Forwarding (RTbF) frameworks in the EU, UK, US, Brazil, and China. This approach finds common legal principles and warning examples from these places. It looks at how the laws currently stand and suggests needed changes. The study doesn't include empirical methods since there's no systematized enforcement data for RTbF in India. The Data Protection Body of India hasn't put the rules into effect yet. So, this research focuses solely on the legal doctrines, matching the dissertation's needs..

6. Literature Review

The literature on the RTbF spans philosophy, information science, constitutional law, and comparative data protection law. The following five works are foundational to this study.

6.1 Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (Princeton University Press, 2009)

Mayer-Schönberger sets up the thinking for the whole debate on the right to be forgotten. According to him, our ability to forget isn't a glitch in cognition; it's a helpful tool that aids healing, forgiveness, and personal growth. Digital systems, on the other hand, remember every single thing forever. This creates permanent records, or "frozen pasts," which can lock people into outdated moments they've moved beyond. Proposing expiry dates for data, where info gets auto-deleted after a while, has really sparked global legislative discussions. In India, his ideas supply the key dignitarian argument for the right to be forgotten, linking it to Article 21 of the constitution. This shows how preserving memories indefinitely frustrates a person's ability to shape their own life. The core message is that forgetting should be normal, not something needing excuse, because digital immortality messed that up.

6.2 Jeffrey Rosen, 'The Right to Be Forgotten' (Stanford Law Review Online, 2012)

Rosen offers the most influential early critique from an American civil-libertarian viewpoint. He believes that letting private companies like Google make erasure decisions sets up a private censorship regime. The worry here gets worse when public figures try to erase truthful



accounts of their actions. This is especially relevant in the Indian context, where his critique warns against a wide right-to-be-forgotten policy. Such a policy could be used by those in power to quash info in the public interest, like journalism or historical research. Thus, Rosen's work highlights the balance between privacy and accountability, which shapes the proportionality analysis laid out in this paper.

6.3 Usha Ramanathan, 'India, Privacy and the Internet' (Economic and Political Weekly, 2013)

Ramanathan's work is key for this India-focused literature review. She wrote about the Aadhaar biometric system before Puttaswamy came out, arguing that it deepened the privacy issues for regular folks while the law didn't respond much to this. Ramanathan questions whether privacy can truly be protected when there's no solid enforcement, foreshadowing the main flaw in the DPDPA 2023: a formally recognized right that isn't really accessible in practice. She highlights how caste and gender make people more vulnerable in digital spaces, giving a necessary context for designing any Indian right to be forgotten framework. Essentially, Ramanathan suggests that importing rights from European law won't help if they don't fit India's specific socio-political situation.

6.4 Justice B.N. Srikrishna Committee Report on Data Protection Framework for India (MeitY, 2018)

The Srikrishna Committee Report is still the most authoritative policy document on data protection, including RTbf, in India. The committee suggested a qualified right to erasure in their proposed Personal Data Protection Bill but warned against fully adopting the GDPR model. They pointed out conflicts between erasure rights and important public interests like press freedom, academic research, and transparency in court records. Their advice on balancing individual rights with institutional needs influenced both the 2019 Bill and the 2023 DPDPA. For my study, this report is essential, acting as a primary policy source that connects constitutional doctrine with legislative design, especially regarding institutional structure and the roles of regulatory bodies versus courts.

6.5 Paul Bernal, Internet Privacy Rights: Rights to Protect Autonomy (Cambridge University Press, 2014)

Bernal talks about online privacy rights, including the Right to be Forgotten (RTbF), within a bigger idea of personal freedom. He says that the way online data profiles work—being persistent and collected in one place—doesn't just make people embarrassed. It actually limits the choices we make in our everyday lives. We avoid certain behaviors and even refrain from speaking up because we're aware everything could come back to haunt us.



This suppression of autonomy is what ties the RTbF to the Puttaswamy judgment's autonomy part most directly. People change how they act knowing they're being watched all the time. Bernal's thoughts create a link between European data protection rules and India's constitutional views. Essentially, the RTbF isn't just some vague concept of dignity; it's about protecting real-life circumstances where people can live freely and independently, as promised by Article 21..

7. Data Analysis

7.1 Constitutional Foundation: The Puttaswamy Architecture

In India, the constitutional case for the Right to be Forgotten rests on Puttaswamy (2017). The nine-judge bench there nixed earlier rulings by M.P. Sharma (1954) and Kharak Singh (1963), which said no constitutional right to privacy existed. Instead, they declared unanimously that privacy is a key part of Article 21. Chandrachud's main opinion emphasized informational privacy, which is about an individual controlling their personal data's collection, storage, and sharing. This includes the Right to be Forgotten: people can ask for outdated or harmful personal data to be erased or hidden. Also, Nariman's agreement outlined a four-stage test for deciding if fundamental rights restrictions are legit—legality, valid goal, necessity, and strictly proportional means. So, this test guides judges when deciding on Right to be Forgotten cases.

The main conflict is between the right to privacy (Article 21) and the freedom of expression (Article 19(1)(a)) in the constitution. Both can be found in Part III and aren't limitless. To sort out disputes, here's a suggested approach using a balance test:

First, look at what kind of info is involved—things like health records, caste identity, or sexual orientation deserve more privacy. Then consider who owns the data; folks in the public eye shouldn't expect as much privacy for stuff related to their jobs.

Next, think about age: If older info isn't important for any current public reasons, it should lean towards getting erased. Actual damage from something, such as it hurting someone's job, safety, or dignity, makes a privacy case stronger.

Finally, when deciding on a fix, removing just web references (de-indexing) is often better than wiping everything clean.

That sums up the rough guide!.

7.2 Indian High Court Jurisprudence: An Inconsistent Patchwork

Indian High Courts have produced a small but important set of RTbF cases that support the right while pointing out some inconsistencies in the courts' reasoning. In Dharamraj Bhanushankar Dave vs. State of Gujarat in 2017, the Gujarat High Court was the first to look at the RTbF idea. They said it had theoretical validity, based on privacy protections in Article



21, but then refused the request because of proportionality issues. The judgment stayed a public record.

Things took a different turn when the Karnataka High Court looked at an RTbF case. In *Vasunathan vs. Registrar General* in 2017, the court ordered the petitioner's identity to be hidden in the online version of a matrimonial judgment. They saw a distinction between maintaining the physical archive and the potential harm from permanent digital exposure. So, the court took a more claimant-friendly approach in this instance.

The Delhi High Court's decision in *Jorawar Singh Mundy versus Google LLC* (2021) is the biggest right-to-be-forgotten case so far. The court told Google, Indian Kanoon, and the Registry to remove links to the petitioner's acquittal judgment. They said keeping those links available violated the person's privacy and dignity under Article 21. It wasn't justified by any public interest in keeping such records permanently accessible.

In another set of rulings, the Allahabad High Court showed some flexibility. In *Zulfiqar Haider's* case, they denied his request because he didn't prove the news reports damaged him more than the public's right to information. For *Nilofar Khan*, it was different. She got what she asked for, which was to have her info anonymized. The court understood that people who survive domestic violence continue to suffer from past legal proceedings being easily found online.

All together, these rulings show how right-to-be-forgotten laws are starting to be defined in India. But there's still a big need for the Supreme Court to weigh in. They need to set clear rules about what criteria to use, what obligations intermediaries have, and the standards for fixing these issues.

7.3 Legislative Analysis: The DPDPA 2023 and Its Gaps

The Digital Personal Data Protection Act, 2023 marks a big advance for India's data protection. Section 13 lets people fix, finish, update, or remove their personal info once the reason for collecting it is done, except when there are legal reasons to keep it. Also, setting up the Data Protection Board of India (DPBI) as a special judge body is awesome.

The DPDPA 2023 shows four big gaps when you look at what the Puttaswamy mandate says and compare it to the GDPR standards. First off, there's no explicit right to de-indexing in the Act. This means search engines aren't required by law to remove links to personal info when someone requests it. Considering ongoing harm often comes from search visibility more than stored data, this is a major issue.



Secondly, some core terms like 'no longer necessary' and 'legitimate purpose' aren't clearly defined. Because of this vagueness, data fiduciaries and the DPBI can't make consistent decisions.

Third, if a processor has publicly shared personal info, they aren't required to notify others about an erasure request. This makes erasing that info effectively across different platforms nearly impossible.

Lastly, the DPBI isn't up and running. So if someone wants their info removed, they must go to court—which is costly, takes ages, and is totally unsuitable for something that should be a regular administrative task.

7.4 Comparative Insights

The EU's Right to Be Forgotten (RTbF) framework, defined by the Google Spain ruling, GDPR Article 17, and more recent Court of Justice of the European Union (CJEU) rulings like Google v. CNIL and GC v. CNIL (both from 2019), leads the world. This framework, with its set rules for what to erase, clearly stated exceptions for journalists and scholars, orders for search engines to remove info, and needs for notifications, fills in the blanks in India's system perfectly.

In the UK, the NT1 & NT2 v. Google case from 2018 showed how a careful analysis that considers the situation works within a common law setting. We could totally use something similar in Indian courts. Brazil's General Data Protection Law (LGPD) from 2018 and China's Personal Information Protection Law (PIPL) from 2021 both have RTbF rights too, even under their unique systems. But enforcing these rules is way easier in some places than others.

The US gives another example; because of the First Amendment, they don't have an RTbF at all. Yet, India's Constitution does allow for certain limitations on free speech in order to maintain dignity and privacy, giving us room for an RTbF policy the US doesn't have..

Conclusion

This research confirms all four hypotheses. The RTbF is constitutionally embedded in Article 21 via Puttaswamy's informational privacy dimension, making it judicially enforceable. However, no further legislation is needed; we still require a statutory framework to make things work smoothly and consistently. While the DPDPA 2023 represents progress, it doesn't quite provide the solid legal foundation needed. Issues like the lack of de-indexing obligations, vague erasure criteria, missing notification requirements, and the non-operational DPBI office mean that the right's power remains weak in practice.

Here, I've proposed a proportionality framework that weighs factors such as information sensitivity, data subject status, temporal relevance, demonstrable harm, and the idea of a



proportional remedy. This framework can help courts balance the RTbF with freedom of expression in a fair way. Plus, India's approach needs to fit its unique context, which means copying Europe's model wouldn't account for India's specific social issues and digital dynamics.

Based on this analysis, six suggestions are put forward. Firstly, the DPDPA 2023 needs amending to add an explicit right to de-indexing for search engines. This would mimic GDPR Article 17 but fit India's system better.

Secondly, rules on what info is 'no longer necessary' should be set through secondary laws. These criteria must consider how old the info is, the public interest factor, the harm it might cause, and the person it's about.

Third, businesses that spread personal data publicly should warn others involved when someone asks for removal. Fourthly, the DPBI really needs to get set up fast. They should hire tech law experts, define clear review processes for removal requests, and provide ways to temporarily fix issues.

Additionally, the Supreme Court should create thorough guidelines on right-to-be-forgotten cases whenever there's a suitable opportunity.

Lastly, sensitive court docs – especially those linked to matrimonial disagreements, sex crimes, and domestic abuse – need anonymizing. The top judge should lead this project and make sure these files are properly masked for online use in legal databases.

The Right to be Forgotten isn't about rewriting history; it's about making sure the law doesn't define someone forever because of their biggest mistake. India's constitutional tradition, tied to Ambedkar's idea that the Constitution is a moral promise from the state to its people, demands a legal framework that respects dignity, helps with rehabilitation, and recognizes that individuals are more than what their digital footprint shows. The building blocks for this are already in the Puttaswamy judgment. All that's left is for there to be the political will to actually build it.

References

Cases Referred:

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

Google Spain SL, Google Inc. v. AEPD, Mario Costeja González, Case C-131/12 (ECJ, 2014).

Dharamraj Bhanushankar Dave v. State of Gujarat, SCA No. 1854/2015 (Gujarat HC, 2017).

Jorawar Singh Mundy v. Google LLC, CS(OS) 642/2016 (Delhi HC, 2021).

Vasunathan v. Registrar General, Karnataka HC, WP No. 62038/2016 (Karnataka HC, 2017).



Zulfiqar Haider v. Google LLC, WP No. 13063/2016 (Allahabad HC).

Nilofar Khan v. State of U.P., WP No. 47086/2019 (Allahabad HC).

NT1 & NT2 v. Google LLC, [2018] EWHC 799 (QB).

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

Shreya Singhal v. Union of India, (2015) 5 SCC 1.

Legislation:

The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

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

The Information Technology Act, 2000 (Act No. 21 of 2000).

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Books & Reports:

Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009).

Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press, 2014).

MeitY, *Report of the Committee of Experts on a Data Protection Framework for India under the Chairmanship of Justice B.N. Srikrishna* (July 2018).

Articles:

Jeffrey Rosen, 'The Right to Be Forgotten' (2012) 64 *Stanford Law Review Online* 88.

Usha Ramanathan, 'India, Privacy and the Internet' (2013) 48(5) *Economic and Political Weekly* 38.

Prateek Suriseti and Rohan Batra, 'The Right to Be Forgotten in India: An Analysis' (2020) 5 *NUJS Law Review* 55.

Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows' (2011) 8 *SCRIPTed* 229.