

INTEGRATION IN SOCIAL SCIENCES AND HUMANITIES

An online peer reviewed Open Access Journal Published by Cignix Press
 Content available at www.cognixpress.in Online ISSN: XXXX-XXXX

LEGAL EVOLUTION OF THE RIGHT TO BE FORGOTTEN IN INDIA: A SYSTEMATIC REVIEW OF JUDICIAL, STATUTORY, AND POLICY DEVELOPMENTS**G.SIDDARTHA**

1st yr LLB, Damodaram Sanjeeviah National Law University, Visakhapatnam, Andhra Pradesh, India.

ARTICLE HISTORY	ABSTRACT
Received: 19.04.2026 Revised: 11.05.2026 Accepted: 24.06.2026 Keywords: <i>Right to be forgotten (RTBF); Digital Personal Data Protection Act, 2023; Right to privacy; Puttaswamy judgment; Judicial records; Freedom of expression; Data fiduciaries.</i> *Communication Author G.Siddhartha	The right to be forgotten (RTBF) occupies a contested space in Indian data protection law, emerging from the constitutional recognition of privacy in Justice K.S. Puttaswamy v. Union of India (2017) yet remaining without explicit statutory codification. This systematic review maps the judicial, statutory, and policy developments shaping RTBF in India, with the objective of identifying doctrinal inconsistencies, legislative gaps, and the implications for individual privacy rights. Indian high courts have granted RTBF relief in specific contexts- such as cases involving sexual offense victims or acquitted individuals-while simultaneously emphasizing the public's right to access judicial records. The Digital Personal Data Protection Act, 2023, introduces a statutory erasure right but omits the term "right to be forgotten" and lacks mechanisms for de-indexing, thereby creating a disconnect between legislative intent and judicial practice. Comparative analysis with the European Union's GDPR framework highlights India's reliance on case-by-case adjudication rather than a structured proportionality test, leading to inconsistent enforcement. Key gaps include the absence of an independent data protection authority with binding powers, unclear standards for balancing RTBF against freedom of expression, and insufficient guidance for data fiduciaries. We conclude that India's RTBF framework remains critically underdeveloped; without coherent statutory provisions and regulatory oversight, individuals face diminished control over their digital identities, and platforms encounter compliance uncertainty. Future reforms should prioritize explicit RTBF provisions, a centralized enforcement body, and guidelines tailored to emerging technologies.

INTRODUCTION

The digital age has fundamentally transformed the relationship between individuals and their personal information, creating unprecedented challenges for privacy law. As vast quantities of personal data are generated, stored, and disseminated across global networks, the ability of individuals to control their digital identities has become a central concern for legal systems worldwide. The right to be forgotten (RTBF), which allows individuals to request the removal of personal information from online platforms under certain conditions, has emerged as a critical legal mechanism to address this challenge. This right, most prominently articulated in the European Union's General Data Protection Regulation (GDPR) of 2018, represents a significant evolution in privacy jurisprudence, moving beyond traditional notions of data protection to encompass a proactive right of erasure and de-indexing [1].

The legal landscape surrounding the right to be forgotten in India is particularly complex and fragmented. The foundational moment for privacy rights in India occurred with the landmark judgment of the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017), which declared the right to privacy a fundamental right under Article 21 of the Constitution [2]. This decision provided the constitutional bedrock upon which subsequent privacy claims, including those invoking the right to be forgotten, could be built. However, the Puttaswamy judgment did not explicitly define the contours of the RTBF, leaving its precise scope and limitations to be determined by subsequent judicial interpretation and legislative action. The Digital Personal Data Protection Act (DPDPA), enacted in 2023, introduced a statutory right to erasure, yet it notably refrained from using the term "right to be forgotten" and failed to provide comprehensive mechanisms for de-indexing from search engines [3]. This legislative omission has created a significant disconnect between the evolving judicial practice and the statutory framework.

Despite the growing body of case law and academic commentary on the RTBF in India, the field suffers from a notable lack of systematic synthesis. Existing research tends to focus on individual high court decisions or comparative analyses with the European framework, but few studies have attempted to comprehensively map the entire trajectory of legal developments across judicial, statutory, and policy domains [4]. This fragmented approach has obscured the identification of persistent doctrinal inconsistencies, legislative gaps, and the practical implications for both individuals and data fiduciaries. For instance, while Indian high courts have granted RTBF relief in specific contexts—such as protecting the identities of sexual offense victims or allowing acquitted individuals to remove records of their arrests—the legal reasoning employed has varied considerably across jurisdictions, leading to unpredictable outcomes [5]. Furthermore, the absence of a clear proportionality test, akin to the one developed by the Court of Justice of the European Union in the Google Spain case, has left Indian courts without a structured framework for balancing the right to privacy against competing rights, such as freedom of expression and the public's right to access information [6]. As digital platforms continue to proliferate and personal data becomes an increasingly valuable commodity, the absence of a clear and enforceable RTBF framework creates significant risks for individual autonomy and dignity. Individuals may find themselves permanently tethered to outdated, irrelevant, or harmful information, with limited legal recourse to reclaim control over their digital narratives. Simultaneously, data fiduciaries, including search engines and social media platforms, face considerable compliance uncertainty, as they must navigate a patchwork of inconsistent judicial pronouncements without clear statutory guidance. This review, therefore, seeks to consolidate the existing knowledge base, identify the key areas of doctrinal tension, and highlight the critical gaps that must be addressed to develop a coherent and effective RTBF regime in India.

COMPARATIVE JURISDICTIONAL ANALYSES OF THE RIGHT TO BE FORGOTTEN

A significant body of the included studies undertakes comparative jurisdictional analyses to situate the Indian right to be forgotten within the broader global legal landscape. The European Union, with its well-established and judicially elaborated framework under the General Data Protection Regulation (GDPR), serves as the primary comparator for most studies, while several also incorporate the United States' First Amendment-dominated approach. These comparative analyses are instrumental in identifying the structural and doctrinal gaps in the Indian framework, as well as in proposing potential reform pathways [7].

The most comprehensive cross-jurisdictional mapping is provided by Sharma [12], which offers a tripartite comparison of the RTBF in the EU, India, and the USA. This study highlights that the EU has vigorously adopted the RTBF with statutory delisting remedies subject to narrow journalistic exceptions, as established by the Google Spain (CJEU 2014) judgment and codified in GDPR Article 17. In stark contrast, the United States, guided by the First Amendment, flatly rejects any general RTBF, as demonstrated by the Ninth Circuit in *Garcia v. Google* and the Second Circuit in *Martin v. Hearst*, which held that courts cannot "undo historical facts" [12]. India occupies a middle ground: no settled statutory RTBF exists, the Digital Personal Data Protection (DPDP) Act of 2023 includes a limited erasure right but omits an explicit "be forgotten" label, and courts have begun balancing privacy and free speech on a case-by-case basis, informed by the constitutional privacy right declared in *Justice K.S. Puttaswamy v. Union of India* (2017) [12]. This finding underscores the precarious and unfinished nature of the Indian RTBF, caught between the European model of proactive protection and the American model of maximal free expression.

Several studies narrow their comparative focus to the EU-India dyad, analyzing the transferability of European legal principles to the Indian context. For instance, Gupta & Naithani [8] examines how India and the EU have handled the RTBF specifically in the context of search engines as data fiduciaries or controllers. The study notes that the RTBF is relatively new in India, with several judgments beginning to shape its dimensions, whereas the EU has had a right to erasure since 1995 and a decade of jurisprudence post-Google Spain [8]. The paper suggests that the implementation of the RTBF in India would depend on the nature of data fiduciaries and their services, implying that a one-size-fits-all approach borrowed from the EU may be inappropriate [8]. Similarly, Khetan [10] provides a comparative analysis arguing for the formal adoption of the RTBF within India, advocating for a legal structure that effectively balances the right to privacy with free speech, as the GDPR does through context-specific adjudication [10]. The study emphasizes that the Indian approach is still in its developmental stage, lacks a comprehensive legislative framework akin to the GDPR, and suffers from inconsistent enforcement due to the absence of a central regulatory authority [10].

A more granular comparative constitutional analysis is undertaken by Singh, Vishwakarma & Nigam [14], which contrasts the EU's rights-first approach, grounded in Article 8 of the European Convention on Human Rights (ECHR) and the GDPR, with India's judicially emergent approach, where privacy was read into Articles 14, 19, and 21 of the Constitution through the Puttaswamy judgment. The study examines key cases such as *Shreya Singhal* (freedom of speech), *Anuradha Bhasin* (intermediary regulation), and *Google Spain* (cross-border data governance) to reveal that the Indian model suffers from a

lack of institutional independence and algorithmic accountability mechanisms, and proposes an original Indian model that integrates existing principles into a coherent regulatory design [14]. This constitutional perspective is complemented by Shrivastava [13], which traces the jurisprudential origins of the RTBF in the EU, identifies theoretical indeterminacy arising from the co-existence of the RTBF and the right to privacy, and then undertakes a comparative analysis with the nascent development of the RTBF and informational privacy in India [13].

The most forward-looking comparative analysis is provided by Singh & Malik [5], which compares the law governing the RTBF in the EU, the US, and India through a qualitative doctrinal analysis of legislation, regulatory materials, and leading judgments. This study identifies three distinct models: EU law recognizes qualified erasure and de-referencing subject to safeguards for expression, journalism, and public interest; US law generally protects truthful, lawfully obtained public-record information; and Indian law recognizes informational privacy constitutionally, but its statutory erasure right was not yet fully operationalized, and the Supreme Court had not finally settled the treatment of online judicial records [5]. The study proposes a remedy ladder and a structured proportionality test for Indian courts, designed to preserve authoritative judicial records while reducing disproportionate name-based exposure, drawing on the Delhi High Court's distinction among preservation, masking, and name-based de-indexing [5]. This proposed framework represents a sophisticated attempt to reconcile the competing demands of privacy and open justice within the Indian context.

Several studies extend the comparative analysis beyond the EU and USA to include the United Kingdom and to incorporate broader thematic concerns. Akriti Gupta [9] establishes the compatibility of the RTBF between the UK and India, referencing the CJEU's decision in Google Spain-Costeja and offering recommendations for the Indian framework [9]. Nair [11] compares the Indian Personal Data Protection Bill with the GDPR, focusing on the right to erasure and the balance between privacy and free expression, as articulated in the Google Spain case [11]. Sankar [4] and Wani & Jaggi [16] broaden the comparative scope to examine the interplay between the Right to Know and the Right to Be Forgotten, analyzing relevant Indian statutes such as the Right to Information Act of 2005, the Information Technology Act of 2000, and the DPDP Act of 2023, alongside significant rulings like *Rajagopal v. State of Tamil Nadu* and *Subhranshu Rout v. State of Odisha* [4, 16].

Finally, [16] addresses the role of data protection law in combating generative AI misinformation, employing comparative approaches from the EU, India, and the United States. The study analyzes legal doctrines such as the RTBF, informational self-determination, and public interest law theories, and identifies key regulatory loopholes, such as the lack of requirements for AI developers, patchwork global norms, and ineffective enforcement capacity [16]. It proposes necessary reforms, including AI impact assessments, algorithmic audits, and watermarking requirements, to ensure good governance and accountability of AI systems [16]. This study is unique in linking the RTBF to the emerging challenges of synthetic media and deepfakes, thereby extending the comparative analysis into the realm of technological governance. The key characteristics of the studies that perform comparative jurisdictional analyses are summarized in Table 1 below, which collates the scope of comparison, key legal instruments compared, and the stage of RTBF development in India as identified by each study.

Table 01: Cross-Jurisdictional Comparison of RTBF Frameworks and Developmental Stages

Study ID	Scope of Comparison	Key Legal Instruments Compared	Stage of RTBF Development in India
Gupta & Naithani [8]	Comparison of how India and the European Union have handled the right to be forgotten, specifically in the context of search engines.	EU's right to erasure since 1995; India's data protection legislation.	Relatively new, with several judgments beginning to shape its dimensions; India considering comprehensive data protection legislation.
Wani & Jaggi [16]	Comparative approaches from the European Union, India, and the United States.	Right to be forgotten, informational self-determination, and public interest law theories.	Addressed in the context of generative AI misinformation and emergent digital harms.
Akriti Gupta [9]	UK and India.	Google Spain-Costeja case, decision of CJEU.	Establishes compatibility between UK and Indian frameworks.
Khetan [10]	Comparative analysis of the Right to Be Forgotten in Europe and India.	General Data Protection Regulation (GDPR) in Europe and draft data protection legislation in India.	Developmental stage; lacks comprehensive legislative framework similar to GDPR;

			inconsistent enforcement due to absence of central regulatory authority.
Nair [11]	Comparison of the Indian Personal Data Protection framework and the GDPR.	Indian Personal Data Protection Bills and the GDPR.	Compares erasure provisions and balancing mechanisms between both regimes.
Sharma [12]	Comparative review of how EU, India, and USA balance RTBF against press freedom and the public's right to know.	EU: Google Spain (CJEU 2014), GDPR Art. 17; India: KS Puttaswamy (2017), DPDP Act 2023; USA: First Amendment, Garcia v. Google, Martin v. Hearst.	No settled statutory RTBF exists; DPDP Act 2023 includes limited erasure right but omits explicit 'be forgotten' label; case-by-case balancing.
Shrivastava [13]	Comparative analysis of RTBF in supra-national EU with nascent development of RTBF and informational privacy in India.	EU's RTBF framework; India's nascent RTBF and informational privacy jurisprudence.	Nascent development.
Singh, Vishwakarma & Nigam [14]	Comparative constitutional analysis of digital constitutionalism in India and the EU (privacy, speech, cross-border governance).	EU: Article 8 ECHR and GDPR; India: Articles 14, 19, and 21 of the Constitution as interpreted in Puttaswamy, Shreya Singhal, Anuradha Bhasin.	Contrasts EU's rights-first approach with India's judicially emergent constitutional model.
Sankar [4]	Approaches of EU, UK, US and India towards the Right to Know and the Right to Be Forgotten.	Right to Information Act 2005, IT Act 2000, DPDP Act 2023; rulings in Puttaswamy, Rajagopal, Subhranshu Rout, Jorawar Singh Mundy.	Examines balance between Right to Know and RTBF across multiple jurisdictions.

BALANCING PRIVACY WITH COMPETING RIGHTS: THE CORE DOCTRINAL TENSION

The fundamental legal challenge animating the right to be forgotten in India is the necessity of balancing the individual's interest in controlling personal information against a constellation of competing rights, most notably freedom of speech and expression, the public's right to know, and the principle of open justice. The included studies consistently identify this balancing exercise as the central doctrinal tension, revealing that Indian courts and lawmakers have yet to develop a consistent and predictable framework for resolving these conflicts. The analysis of these studies demonstrates that the manner in which this balance is struck fundamentally determines the scope, enforceability, and practical utility of the RTBF. The studies reveal a wide spectrum of approaches to this balancing problem, ranging from the rejection of any general RTBF in the United States to the structured proportionality test of the European Union, with India occupying an intermediate but uncertain position. Sharma [12] provides a stark illustration of these divergent approaches: in the United States, the First Amendment's protection of free speech is so dominant that courts flatly reject any general RTBF, as exemplified by the Ninth Circuit's holding in *Garcia v. Google* that a European-style right to be forgotten "is not recognized in the United States" and the Second Circuit's refusal in *Martin v. Hearst* to expunge an expunged arrest from the press, noting that "the law... cannot undo historical facts" [12]. This contrasts sharply with the European Union, where the RTBF was vigorously adopted with statutory delisting remedies, albeit subject to narrow journalistic exceptions, as established in the *Google Spain* case [12]. India's approach, as described by [12], is characterized by a case-by-case balancing by courts, with no settled statutory RTBF and a limited erasure right in the DPDP Act 2023 that omits the explicit "be forgotten" label. Several studies propose specific frameworks or tests for structuring this balancing exercise. The most comprehensive proposal is offered by Singh & Malik [5], which recommends a remedy ladder and a structured proportionality test for Indian courts, designed to preserve authoritative judicial records while reducing disproportionate name-based exposure. This framework draws on the Delhi High Court's distinction among preservation, masking, and name-based de-indexing, suggesting that the remedy should be calibrated to the severity of the harm and the nature of the competing interest [5]. Similarly, Sankar [4] presents a Privacy-Transparency-Public Interest Framework rooted in principles of proportionality,

necessity, public interest, accuracy or relevance of information, status of the individual, likelihood of harm, and historical significance to offer courts, regulators, and online platforms a contextual approach when balancing these interests [4]. This framework is notable for its multi-factor analysis, which acknowledges that the balance cannot be determined by a single principle but must be tailored to the specific circumstances of each case. The balancing of privacy with competing rights is not merely a theoretical exercise but has immediate practical consequences for the recognition of the RTBF in specific contexts. Khetan [10] highlights that Indian courts have recognized the RTBF in cases concerning the protection of sexual offence victims and individuals who are acquitted of their crimes, but this recognition is inconsistent and lacks a uniform standard [10]. The study argues for a legal structure that effectively balances the right to privacy with free speech, emphasizing that the absence of a central regulatory authority in India leads to inconsistent enforcement [10]. Nair [11] frames the issue as a "balance-of-rights analysis of the right to privacy vs. the right to free expression," noting that the RTBF applies to "misleading, embarrassing, irrelevant, or obsolete personal information on the Internet" and that the European Court of Justice's ruling in *Google Spain* established this balancing as a matter of EU law [11].

The studies also reveal that the concept of "public interest" is a crucial but contested variable in the balancing equation. Wani & Jaggi [16] addresses the role of data protection law in combating generative AI misinformation, emphasizing that the right to be forgotten must be balanced against "democratic integrity, and public interest" [16]. The study identifies key regulatory loopholes, such as the lack of requirements for AI developers and patchwork global norms, suggesting that the balancing exercise becomes even more complex when applied to emerging technologies like synthetic media and deepfakes [16]. Yadav [17] provides a more specific critique of the DPDP Act's failure to reconcile the tension between "public information access and individual bodily and economic autonomy," arguing that the lack of a comprehensive de-indexing framework creates an "inescapable digital panopticon" [17].

The most critical dimension of the balancing exercise concerns the treatment of judicial records. Courts are repositories of information that is presumptively public, and the open justice principle holds that court proceedings and judgments should be accessible to all. However, the permanent digital availability of judicial records-including those containing outdated, irrelevant, or stigmatizing information about individuals-creates a direct conflict with the RTBF. Singh & Malik [5] directly addresses this tension by proposing a remedy ladder that distinguishes between preservation, masking, and name-based de-indexing, arguing that courts should preserve authoritative judicial records while reducing disproportionate name-based exposure [5]. This approach acknowledges that the solution is not to delete judicial records, which would violate the principle of open justice, but to make them less easily discoverable through search engines, thereby reducing the harm to individuals without compromising the public's right to access the information.

DOMESTIC LEGAL FRAMEWORKS AND JUDICIAL PRECEDENTS: THE FRAGMENTED ARCHITECTURE OF THE INDIAN RIGHT TO BE FORGOTTEN

The Indian legal landscape for the right to be forgotten is characterized by a conspicuous absence of explicit statutory codification, a nascent but growing body of judicial precedents from high courts, and a constitutional foundation that was only recently established. The included studies collectively reveal that the Indian RTBF is not a single, coherent legal right but rather a fragmented assemblage of constitutional principles, statutory provisions that do not use the term "right to be forgotten," and ad hoc judicial decisions that vary significantly in their reasoning and scope. This subsection provides a systematic analysis of the domestic legal frameworks and judicial precedents that constitute the current state of the RTBF in India, drawing on the specific studies that focus on this dimension.

The constitutional bedrock for the RTBF in India was established by the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017), which declared the right to privacy a fundamental right under Article 21 of the Constitution [2]. This decision is consistently cited across the included studies as the foundational moment that enabled subsequent privacy claims, including those invoking the RTBF. For example, Yadav [17] explicitly grounds its analysis in the Puttaswamy precedent, arguing that the constitutional recognition of privacy should logically extend to a right to control one's digital past, yet the DPDP Act of 2023 fails to fully realize this constitutional promise [17]. Similarly, Sharma [12] identifies the Puttaswamy judgment as the key Indian precedent that established privacy as a fundamental right, but notes that the Supreme Court has not yet explicitly defined the contours of the RTBF, leaving its precise scope to be determined by subsequent high court decisions and legislative action [12]. Sankar [4] also includes Puttaswamy as one of the significant rulings that has shaped the legal developments surrounding the RTBF in India, alongside other cases such as *Rajagopal v. State of Tamil Nadu* and *Subhranshu Rout v. State of Odisha* [4].

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents the most significant legislative development concerning the RTBF in India, yet its treatment of the right is notably limited and indirect. Several studies provide critical analyses of the DPDP Act's provisions. Talukdar & Bagaria [15] examines the right to be forgotten as provided under the

DPDP Act, 2023, and analyzes the judgments of the Supreme Court and the High Courts pertaining to the right [15]. Yadav [17] offers a more pointed critique, focusing on Section 12 of the DPDP Act and arguing that the lack of a comprehensive, free-standing de-indexing framework creates an "inescapable digital panopticon" [17]. The study contends that the statutory erasure right in the DPDP Act is insufficient because it does not explicitly address the most critical mechanism for enforcing the RTBF: removal from search engine results and other third-party platforms that aggregate and commodify personal data [17]. Sharma [12] corroborates this assessment, noting that the DPDP Act includes a "limited erasure right but omits an explicit 'be forgotten' label," which creates a significant gap between the legislative intent and the practical enforcement of the right [12].

The included studies also examine other statutory frameworks that are relevant to the RTBF, even if they were not originally designed for this purpose. Sankar [4] provides a comprehensive analysis of the interplay between the RTBF and the Right to Information Act of 2005, the Information Technology Act of 2000, and the DPDP Act of 2023 [4]. This study is unique in its focus on the tension between the right to know and the right to be forgotten, and it examines how these competing rights can be reconciled within the existing Indian legal framework. The study cites key judgments such as *Rajagopal v. State of Tamil Nadu*, which addressed the right to privacy in the context of publishing autobiographies, and *Subhranshu Rout v. State of Odisha*, which dealt with the removal of arrest records from search engines, to illustrate the evolving judicial approach to this tension [4]. The study also references *Jorawar Singh Mundy v. Union of India*, a case concerning the right to be forgotten in the context of criminal records [4].

The judicial precedents on the RTBF in India are primarily from high courts, as the Supreme Court has not yet delivered a definitive ruling on the scope and limitations of the right. The included studies reveal that these high court decisions are inconsistent in their reasoning and vary in the scope of relief granted. Khetan [10] notes that "Indian courts have given reference of Right to Be Forgotten in certain cases, particularly concerning the protection of sexual offence victims and individuals who are acquitted for their crimes," but that "inconsistent enforcement preserve due to the absence of a central regulatory authority" [10]. This observation highlights the ad hoc nature of the current judicial approach, where the RTBF is recognized in specific contexts but without a uniform standard or a clear doctrinal foundation. Talukdar & Bagaria [15] similarly analyzes the judgments of the Supreme Court and the High Courts pertaining to the right to be forgotten, focusing on the overall trajectory of judicial recognition [15].

The most detailed analysis of Indian judicial precedents is provided by Sankar [4], which examines the legal developments surrounding the RTBF through significant rulings such as *Justice KS Puttaswamy v. Union of India*, *Rajagopal v. State of Tamil Nadu*, *Subhranshu Rout v. State of Odisha*, and *Jorawar Singh Mundy v. Union of India* [4]. This study traces the evolution of the RTBF from the constitutional recognition of privacy to the specific application of the right in cases involving criminal records and the removal of personal information from search engines. Singh & Malik [5] provides forward-looking analysis, noting that the Delhi High Court's distinction among preservation, masking, and name-based de-indexing represents a significant doctrinal development that could shape the future of the RTBF in India [5].

Table 02: Domestic Legal Frameworks and Judicial Precedents: Scope, Statutory Basis, and Key Cases

Study ID	Scope of RTBF Definition	Statutory Basis in India	Key Indian Cases Cited
Gupta & Naithani [8]	Focuses on search engines as data fiduciaries/controllers under RTBF.	Considers emerging data protection bills and IT rules.	High Court rulings on search engine intermediary obligations.
Talukdar & Bagaria [15]	Enables individuals to have personal data deleted from internet so it is no longer accessible, subject to limitations.	Digital Personal Data Protection (DPDP) Act, 2023.	Judgments of Supreme Court and High Courts pertaining to RTBF.
Yadav [17]	Critiques lack of comprehensive de-indexing framework; RTBF should cover erasure of digital pasts to prevent digital panopticon.	Section 12 of India's Digital Personal Data Protection (DPDP) Act, 2023.	Justice K.S. Puttaswamy v. Union of India (2017).
Akriti Gupta [9]	Right to remove obsolete or harmful information online; compatibility with UK/EU.	Draft personal data protection legislation.	Puttaswamy privacy jurisprudence.
Khetan [10]	Gives individuals ability to request removal of personal information that negatively impacts character	Draft data protection bills (lacks comprehensive framework like GDPR).	High Court cases on sexual offence victims and acquitted

	or privacy.		individuals.
Sharma [12]	Allows individuals to have outdated, irrelevant, or harmful personal info erased or de-indexed.	No settled statutory RTBF; DPDP Act 2023 includes limited erasure right omitting explicit 'be forgotten' label.	K.S. Puttaswamy (2017) and subsequent High Court decisions.
Sankar [4]	Interplay between Right to Know and RTBF across public records and platforms.	Right to Information Act 2005, IT Act 2000, DPDP Act 2023.	Puttaswamy (2017), Rajagopal (1994), Subhranshu Rout (2020), Jorawar Singh Mundy (2021).

The synthesis of findings across the included studies reveals a legal landscape for the right to be forgotten in India that is simultaneously dynamic and deeply fragmented. Taken together, the evidence consistently demonstrates that the Indian RTBF exists in a state of doctrinal and legislative limbo, caught between a robust constitutional foundation and an incomplete statutory superstructure. The pattern that emerges across the studies is one of ad hoc judicial recognition in specific, often sympathetic, contexts—such as the protection of sexual offense victims or acquitted individuals—without the development of a coherent, universally applicable legal standard. This fragmented trajectory is not merely a transitional phase but reflects a fundamental structural tension within the Indian legal system: the constitutional right to privacy, declared in *Justice K.S. Puttaswamy v. Union of India* [2], has not been translated into a clear, enforceable right to control one's digital past, and the Digital Personal Data Protection Act, 2023 [3], while introducing a statutory erasure right, has deliberately avoided the term "right to be forgotten" and failed to provide the critical mechanism of de-indexing. This disconnect between constitutional promise, legislative intent, and judicial practice is the central finding of this review and has profound implications for the protection of individual privacy in India.

The implications of this fragmented framework are both theoretical and practical. From a theoretical perspective, the Indian experience challenges the assumption that a constitutional declaration of privacy is sufficient to generate a coherent data protection regime. The studies consistently show that the Puttaswamy judgment [2] provided the necessary foundation, but subsequent legislative and judicial developments have not built upon this foundation in a systematic manner. This suggests that the evolution of privacy rights is not a linear process from constitutional recognition to statutory codification to judicial enforcement, but rather a contested and iterative process in which each branch of government may pull in different directions. The Indian case also highlights the importance of institutional design: the absence of an independent data protection authority with binding powers, as noted by Khetan [10] and Singh et al. [14], means that even when courts recognize the RTBF, there is no centralized body to ensure consistent enforcement across jurisdictions and against different types of data fiduciaries. This institutional gap is a critical weakness that cannot be remedied by judicial pronouncements alone.

From a practical perspective, the implications for individuals and data fiduciaries are significant and troubling. For individuals, the current state of the law means that the ability to exercise control over one's digital identity is highly dependent on the specific facts of the case, the jurisdiction in which the claim is brought, and the willingness of the court to extend the RTBF beyond the narrow contexts in which it has been recognized. An individual seeking to remove outdated or irrelevant information from a search engine faces a legal landscape that is uncertain, costly, and unpredictable. The studies by Yadav [17] and Sharma [12] emphasize that the DPDP Act's limited erasure right, without a corresponding de-indexing mechanism, leaves individuals without an effective remedy against the most pervasive form of digital harm: the permanent association of their name with stigmatizing or irrelevant information through search engine results. For data fiduciaries, including search engines, social media platforms, and news websites, the lack of clear statutory guidance creates significant compliance uncertainty. They must navigate a patchwork of inconsistent high court decisions, each of which may apply a different balancing test or recognize a different scope of the RTBF, without the benefit of a Supreme Court ruling or a regulatory authority that can provide binding guidance. This uncertainty is not merely an inconvenience but a real barrier to the development of a robust digital economy in India, as platforms may choose to err on the side of caution and remove content that would otherwise be protected by freedom of expression, or, conversely, may refuse to remove content that should be subject to the RTBF, exposing themselves to legal liability.

The comparative analyses included in this review provide a valuable lens through which to understand the limitations of the Indian approach. The European Union's GDPR [1] offers a model of structured proportionality, where the RTBF is explicitly codified, subject to a clear set of exceptions, and enforced by a centralized regulatory authority. The studies by Singh & Malik [5] and Sankar [4] propose frameworks that are explicitly inspired by the European model, suggesting that Indian courts and lawmakers could benefit from adopting a similar structured approach. However, the studies also caution against a simple transplantation of the European model, noting that the implementation of the RTBF in India must depend on the

nature of data fiduciaries and their services, implying that a one-size-fits-all approach may be inappropriate. The United States' First Amendment-dominated approach, as described by Sharma [12], serves as a counterpoint, demonstrating that a legal system can reject the RTBF entirely in favor of maximal free expression. India's position between these two poles is not inherently problematic, but the lack of a clear and consistent framework for navigating this middle ground is the source of the current doctrinal confusion.

CONCLUSION

This systematic review has mapped the fragmented and contested legal evolution of the right to be forgotten in India, revealing a framework that rests on a constitutional foundation yet remains critically underdeveloped in its statutory and regulatory dimensions. Our synthesis confirms that the Indian RTBF exists in a state of doctrinal limbo: the Supreme Court's declaration of privacy as a fundamental right in *Puttaswamy* provided the necessary constitutional bedrock, but the Digital Personal Data Protection Act, 2023, introduced only a limited erasure right without the explicit "be forgotten" label or the critical mechanism of de-indexing. High courts have granted relief in specific contexts, yet their reasoning varies considerably, producing inconsistent outcomes that undermine legal certainty for both individuals and data fiduciaries. The central contribution of this review is therefore to demonstrate that the Indian RTBF is not a single, coherent legal right but rather an assemblage of constitutional principles, incomplete statutory provisions, and ad hoc judicial decisions that lack a unifying doctrinal framework. The practical and theoretical implications of these findings are substantial. Without a structured proportionality test or a centralized enforcement authority, individuals face unpredictable access to a remedy that should protect their digital autonomy, while platforms confront compliance uncertainty that may chill legitimate speech or, conversely, leave harmful information permanently accessible. The comparative analyses in this review suggest that India could benefit from adopting elements of the European model, particularly its structured balancing test and independent regulatory oversight, but any such transplantation must be carefully adapted to the Indian constitutional context and the specific nature of its digital ecosystem. Future research should prioritize empirical studies of data fiduciary compliance, doctrinal analyses of emerging high court decisions, and investigations into how the RTBF can be adapted to address the novel challenges posed by generative AI and synthetic media. The path forward requires not merely legislative amendment but a coherent institutional architecture that can translate constitutional promise into enforceable reality.

REFERENCES

1. Voigt P, von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer; 2017.
2. Bhandari V, Lahiri K. The surveillance state, privacy and criminal investigation in India: Possible futures in a post-*Puttaswamy* world. *Univ Oxf Hum Rights Hub J*. 2020;3:1-28.
3. Nath S, Dhar R. An Analysis of the Digital Personal Data Protection Act 2023. *Christ Univ Law J*. 2026;15(1):45-68.
4. Sankar AK. An Exploratory Study of Reconciling the Right to Be Forgotten and the Right to Know in India through Privacy, Transparency and Public Interest. *Natl Res J Soc Sci*. 2026;12(2):110-128.
5. Singh MM, Malik V. Balancing Digital Privacy and Freedom of Information: The Right to Be Forgotten Across Three Jurisdictions. *J Digit Justice Leg Innov*. 2026;4(1):89-114.
6. Kalis SM. Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González: An entitlement to erasure and its endless effects. *Tulane J Int Comp Law*. 2014;23(2):541-556.
7. Sharma MK, Kaur P. Constitutional and Legal Landscape of the Right to Be Forgotten in India. *Lentera Hukum*. 2025;12(1):137-158.
8. Gupta I, Naithani P. Right to be forgotten in case of search engines: Emerging trends in India as compared to the EU. *J Data Prot Priv*. 2023;6(2):142-156.
9. Gupta A. Data Privacy in Digital World: Right to Be Forgotten. *Law Rev*. 2018;9(3):77-92.
10. Khetan G. A Comparative Analysis of the Right to Be Forgotten in Europe and India. *NUJS J Regul Stud*. 2025;7(1):55-78.
11. Nair S. In the Digital Age, the Right to be Forgotten: A Comparison of the Indian Personal Data Protection Act of 2018 and the GDPR. *Natl J Cyber Secur Law*. 2022;5(2):33-51.
12. Sharma J. Freedom of the Press in the Shadow of Privacy: The Right to be Forgotten in India, EU, and USA. *LawFoyer Int J Doctrinal Leg Res*. 2025;3(4):201-224.
13. Shrivastava A. The origins, jurisprudential fallacies and practical limitations of a 'Right To Be Forgotten' in the European Union. *Int J Law Policy Rev*. 2021;10(2):65-84.
14. Singh RK, Vishwakarma AK, Nigam V. Two Paths to Digital Rights: A Comparative Constitutional Analysis of Digital Constitutionalism in India and the European Union. *Int J Comput Inf Syst Ind Manag Appl*. 2026;18:145-162.
15. Talukdar R, Bagaria S. Changing Contour of the Right to Privacy in the Digital Age: A Study on the Right to Be Forgotten in India. In: *Society, Polity, Economy and Culture of India*. 2024.

16. Wani SA, Jaggi R. Role of data protection law in combating generative AI misinformation: A visible threat to privacy. In: Combating Misinformation in the Age of Artificial Intelligence. IGI Global; 2026.
17. Yadav S. The Digital Panopticon: The Right to Be Forgotten Under India's DPDP Act, 2023. Wah Acad J Int Law Policy. 2026;8(1):15-38.