

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

THE RIGHT TO BE FORGOTTEN IN INDIA: BALANCING THE RIGHT TO PRIVACY WITH THE RIGHT TO INFORMATION

AUTHORED BY - SOWMYA.A

School of law, Vellore Institute of Technology (VIT) University Chennai campus,
Vandalur road Kelambakkam 1Chennai- 600127, India

1.0 Abstract

The permanence of digital information has produced one of the most significant contemporary conflicts in Indian constitutional law: the tension between the right to privacy and the right to information. Search engines, judicial repositories such as Indian Kanoon, and online news archives ensure that personal data — including matrimonial disputes, criminal accusations, and even judicially confirmed acquittals — remains perpetually retrievable long after the underlying dispute has been resolved. This paper undertakes a doctrinal and comparative examination of the Right to Be Forgotten ("RTBF") in India, situating it within the constitutional framework established by Article 21 of the Constitution, as interpreted in Justice K.S. Puttaswamy v. Union of India, and against the countervailing guarantee of free speech and information under Article 19(1)(a) read with the Right to Information Act, 2005.

Using a doctrinal approach, this research paper identifies judicial pronouncements by Karnataka, Delhi, Kerala, Madras and Bombay High Courts between 2016 – 2024, then analyses the statutory right to erasure in Section 12 of the Digital Personal Data Protection Act, 2023 ('DPDP Act') in a critical manner. A comparative element is incorporated through a study of the European Union General Data Protection Regulation, 2018 ('GDPR'), along with case law of the Court of Justice of the European Union – namely Google Spain SL v. AEPD, Google LLC v. CNIL - against Cox Broadcasting Corp. v. Cohn from the United States, which represents an information broadening, speech-enhancing standpoint.

I find that Indian courts, without legislative motivation, have arrived at a very cautious, fact-specific proportionality framework – allowing erasure where the concept of 'intimate dignity' is concerned, while denying it where accountability to the public is concerned. I conclude that

the DPDP Act, 2023 is actually a significant legislative intervention, but the right to erasure it prescribes is skeletal, under-detailed and does not specify timelines, codified public-interest exceptions or institutional independence. The paper concludes by proposing a distinctly Indian balancing framework — rooted in the Puttaswamy proportionality standard, informed by the procedural clarity of the GDPR, and tempered by the free-expression vigilance of the American model.

Keywords

Constitutional Law; Data Protection; Digital Personal Data Protection Act, 2023; GDPR; Judicial Developments; Right to Be Forgotten; Right to Information; Right to Privacy.

2.0 Introduction

The Right to Be Forgotten has, over the last decade, evolved from an obscure academic proposition into one of the most litigated questions at the intersection of privacy and technology law in India. In the pre-digital era, the natural erosion of memory and the practical inaccessibility of court records allowed individuals whose disputes had concluded to move on largely unburdened by their past. The proliferation of search engines, digital case-law repositories, and archived news reporting has fundamentally altered this equilibrium. A matrimonial dispute settled a decade earlier, or a criminal charge that concluded in acquittal, continues to surface instantaneously upon a simple search of an individual's name, often causing disproportionate and continuing reputational harm.

This phenomenon gives rise to two questions of constitutional significance. First, does an individual possess a right, as an incident of the right to live with dignity guaranteed under Article 21, to seek the removal or de-indexing of personal information that has lost contemporary relevance? Second, to what extent does the recognition of such a right encroach upon the constitutionally protected right of the citizenry to information and free expression under Article 19(1)(a), and upon the institutional value of open justice that underlies the publication of judicial records?

The passing of the Digital Personal Data Protection Act, 2023 can be considered the first complete data protection law in India and also provides for a statutory right to correction and erasure of personal data under Section 12.¹ However, the Act does not employ the phrase "Right

¹[The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), s. 12.]

to Be Forgotten," nor does it articulate the constitutional lineage of the right, the standard by which courts or the Data Protection Board ought to adjudicate competing claims, or the lessons available from more mature regimes such as the European Union's GDPR. This paper seeks to address that gap by tracing the constitutional foundations of RTBF in India, mapping its uneven judicial development, critically examining its fledgling statutory expression, and proposing a workable balancing framework.

3.0 Objectives of the Study

This paper is directed towards the following five objectives:

1. To uncover the constitutionality of the Right to Be Forgotten in India having regard to Article 21 and the Supreme Court case, Justice K.S. Puttaswamy v. Union of India.
2. To examine the Indian High Courts' sometimes divergent and variable case law on RTBF claims.
3. To analyze thoroughly the right to erasure contained in section 12 of the DPDP Act, 2023 and to explore its structural shortcomings.
4. To attempt a comparative analysis of the Indian position, vis-à-vis, the GDPR in the European Union; and the approach taken by the United States, centered around the First Amendment.
5. To propose a practicable, India-specific framework for balancing individual dignity with public accountability and free expression.

4.0 Scope and Limitations

This study is confined to a doctrinal and socio-legal inquiry. It examines the constitutional text, the DPDP Act, 2023, the Right to Information Act, 2005, the GDPR, and judicial decisions rendered between 2016 and 2024 by the Supreme Court and the High Courts of Karnataka, Delhi, Kerala, Madras, Bombay and Gujarat. The comparative analysis is restricted to the European Union and the United States, and does not extend to other jurisdictions such as Argentina or Japan that have also developed erasure-related jurisprudence. The study does not undertake an empirical or survey-based assessment of public awareness, nor does it examine the technical architecture of search-engine de-indexing. It is further confined to online and digital manifestations of the right, and does not address offline defamation or reputational torts.

5.0 Research Methodology

The study adopts a doctrinal, analytical and comparative methodology. Primary sources include the Constitution of India, the DPDP Act, 2023, the RTI Act, 2005, the GDPR, and case law drawn from official law reports, SCC Online and Indian Kanoon. Secondary sources include peer-reviewed journal articles, Law Commission reports, and commentary from recognised legal databases. The comparative segment draws upon judgments of the Court of Justice of the European Union and the Supreme Court of the United States. A significant limitation of the study is that several Rules under the DPDP Act, 2023 remain in the process of phased notification; the analysis therefore proceeds principally on the text of the Act itself, supplemented by the notified Rules where available.

6.0 Constitutional Foundations of the Right to be Forgotten.

The right to be forgotten has no explicit textual basis in a specific Indian legislation, but its constitutional basis lies in the broad reading and interpretation given to Article 21 of the Indian Constitution. Article 21 is and was once again highly misconstrued by the nine-member bench of the Supreme Court; the justices partially construed Article 21, in a series of decisions, to become a broad article-encompassing right to life that subsumed other 'unenumerated freedoms' such as the right to livelihood, right to health, the environment and the right of personal choice.

The right to privacy took a definitive constitutional turn in the *Union of India* case, with a nine-judge (Full Court) convention of the Supreme Court on 24 August 2017.² The court, which was unanimous, held that the right to privacy is part of the fundamental right to life and personal liberty guaranteed by Art.21, and is also protected as one of the freedoms and personal guarantees of equality stated in articles 19 and 14 of the Constitution respectively. It also overruled the earlier incidences of *M. P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh*, which precluded privacy from attaining the status of a constitutional right.

What is singularly relevant is the finding, by the concurring opinion of Justice S. K. Kaul that the right of an individual to determine over her information and to determine over her existence and self-presentation on the internet - is itself an incident of informational privacy. While this

²Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1; AIR 2017 SC 4161.

acknowledgement was in the specific context of the Aadhaar biometric identification scheme, this has since been used by High Courts to establish a separate Right to Be Forgotten, which allows an individual to approach and regain control over her personal information which is no longer relevant, accurate or necessary.

The Puttaswamy Bench, but the Court was equally categorical in its affirmation that “privacy is not an absolute right”. The Court introduced a three-tier line of proportionality scrutiny which any encroachment of privacy (and any simultaneous attempt to trump competing public interests by recourse to privacy) has to pass through first in order to survive: that “the measure be prescribed by law”; that the measure seek “a legitimate state aim”; and that “the means be proportionate to the end ... and no more restrictive than necessary to achieve the aim” The structure of proportionality has therefore since become the Court’s core approach for determining the scales of the perennial tug-of-war between RTBF assertions and competing rights to information.

7.0 Right to Information and the Value of Transparency

The countervailing constitutional value in this discourse is transparency, which the Supreme Court has long located within the guarantee of free speech and expression under Article 19(1)(a). The Court has reasoned that the right to receive and disseminate information is a necessary corollary of free speech, since meaningful public discourse and democratic participation are impossible without access to information concerning matters of public concern. This judicial recognition found statutory expression in the Right to Information Act, 2005, which conferred upon citizens an enforceable right to seek information from public authorities and has since become an important instrument of governmental accountability and anti-corruption enforcement.

The publication of judicial proceedings occupies a related but distinct position within this transparency framework. The principle of open justice that judicial proceedings and decisions must ordinarily be conducted and recorded in public view is regarded as a structural safeguard against arbitrary or biased adjudication and as a mechanism of accountability for the judiciary itself. It is precisely at the intersection of these two values the citizen's interest in accessing judicial and governmental records, and the individual's interest in not being permanently defined by a resolved dispute that the Right to Be Forgotten operates. The central inquiry, as the following section demonstrates, is not whether one value should categorically prevail over

the other, but at what point continued public availability of personal information ceases to serve any transparency function and becomes solely a source of enduring stigma.

8.0 Judicial Developments in India

8.1 The Karnataka High Court: Sri Vasunathan v. Registrar General

The Karnataka High Court was the first Indian court to explicitly engage with the Right to Be Forgotten. In *Sri Vasunathan v. The Registrar General*, High Court of Karnataka, decided on 23 January 2017³, the petitioner sought a direction that his daughter's name, which appeared in the cause-title and body of a criminal proceeding that had culminated in an out-of-court compromise, be prevented from surfacing in internet search results. Justice Anand Byrareddy directed the Registry to ensure that the daughter's name would not be reflected in any internet search of the order, while clarifying that certified copies of the order obtained through ordinary channels would continue to bear her name in full.

The Court expressly grounded its direction in the emerging international trend recognising a right to be forgotten in sensitive matters involving women, and particularly cases touching upon modesty, marital status, or sexual offences. This decision, though narrow in its operative direction it concerned only search-engine visibility rather than deletion of the judicial record itself established the template that subsequent High Courts would follow: relief calibrated to the sensitivity of the subject matter, granted through selective redaction or de-indexing rather than wholesale erasure, and justified by reference to the diminishing public interest in a matter long since resolved by compromise.

8.2 The Delhi and Kerala High Courts

The Delhi High Court has since received the largest volume of RTBF petitions in the country. Its most cited pronouncement is *Jorawer Singh Mundy v. Union of India*, decided in April 2021⁴. The petitioner, an American citizen of Indian origin, had been tried under the Narcotic Drugs and Psychotropic Substances Act, 1985 and was acquitted by the trial court in 2011, with the acquittal subsequently affirmed by the Delhi High Court itself in 2013.

Upon returning to the United States to practise law, the petitioner discovered that the judgment recording his acquittal continued to appear prominently in search results on Google, Indian

³ *Sri Vasunathan v. The Registrar General*, High Court of Karnataka and Ors., Writ Petition No. 62038 of 2016 (GM-RES), order dated 23 January 2017; reported at 2017 SCC OnLine Kar 424.

Kanoon and vLex.in, materially prejudicing his professional prospects despite his complete exoneration. Justice Pratibha M. Singh, relying upon the privacy holding in Puttaswamy and upon the Court's own earlier order in Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd., granted interim protection directing the removal of the judgment from search-engine indexing, while leaving the substantive question of a general Right to Be Forgotten to be finally determined in the batch of connected writ petitions.

The Kerala High Court, in a comparable line of decisions concerning victims of sexual offences and litigants in matrimonial proceedings, has similarly recognised a privacy-based interest in the removal of identifying details from judgments hosted on platforms such as Indian Kanoon, while cautioning that judicial records perform an independent public function in ensuring the transparency and accountability of the justice-delivery system⁵. Kerala 's Court has thus rejected any broad-net orders of removal, and by adopting a nuanced, fact- specific criteria, requiring the case- specific balancing of interests, with incidental personal information being subject to removal orders, with incidental personal information being subject to removal orders, while important judicial reasoning not to be obscured. Other High Courts have charted a broadly similar middle path. The Madras and Bombay High Courts have permitted the masking of names and identifying particulars in proceedings involving sexual offences, matrimonial disputes, and juvenile matters, while declining analogous relief in cases involving corruption, financial fraud, or offences against the State, on the ground that continued public visibility of such matters serves a demonstrable accountability function. The Gujarat High Court, by contrast, has on at least one occasion declined to recognise a general Right to Be Forgotten in the absence of specific legislative authorisation, illustrating the continuing absence of doctrinal uniformity across jurisdictions.

8.3 Emerging Jurisprudential Trends

A synthesized view of these decisions reveals two clear trends. One, that there has never been a High Court in the country which viewed the Right to Be Forgotten as an unconditional and unconditional right that could be immediately enforced on the mere existence of the right. Second, that doctrinal language moved from ground up, where the majority of the early decisions were concerned only with constitutional morality and the privacy judgment in Puttaswamy, to top down, where more recent decisions were openly grounded on the provisions of the DPDP Act, even as the erasure provisions of the DPDP Act remain in phased implementation.

However, despite doctrinal developments, the lack of binding Supreme Court guidance or a

statutory guide has led to continuing plurality of outcomes across coordinate High Courts in the country thus highlighting the need for legislative clarity.

9.0 Comparative Perspective: The European Union and the United States

9.1 The European Union

In contrast to India, the Right to Be Forgotten in the European Union evolved through adjudication, not legislation. The foundational decision is *Google Spain SL v. Agencia Española de Protección de Datos*, decided by the Court of Justice of the European Union in May 2014.⁶ The complainant, Mario Costeja González, objected to the continued appearance, in Google's search results for his name, of a 1998 newspaper notice concerning the forced auction of his property for recovery of social security debts a matter that had been fully resolved years earlier. The Court held that a search engine operator, by indexing and making available third-party content, itself qualifies as a "data controller" under European data protection law, and is therefore obliged, upon request, to remove links to information that is inadequate, irrelevant, or no longer relevant, even where the underlying publication itself remains lawful. This points the creation of what is more accurately called a right to de-referencing than deletion of underlying content was the doctrinal basis subsequently enacted as that under Article 17, GDPR.

The territorial scope of this right was tested in *Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL)*, decided in September 2019.⁷ The French data protection authority had directed Google to apply de-referencing orders globally, across all versions of its search engine, rather than merely within the European Union. The Court of Justice rejected this position, holding that while EU law does not prohibit a Member State from ordering worldwide de-referencing, it does not presently require it; a search engine operator satisfies its obligations under EU law by de-referencing the relevant results across the versions of its search engine corresponding to the Member States, coupled with measures effectively preventing EU-based users from otherwise accessing the delisted links through non-EU domains. This decision has proved influential well beyond Europe, as it establishes a workable model for reconciling domestic erasure orders with the inherently borderless architecture of the internet. A related decision, *GC and Others v. CNIL*, delivered on the same day, addressed the heightened

⁶*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, Judgment of the Court of Justice of the European Union, 13 May 2014.

⁷*Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL)*, Case C-507/17, Judgment of the Court of Justice of the European Union, 24 September 2019.

protection owed to "special categories" of sensitive personal data including data revealing criminal proceedings, political opinion, or sex life.⁸ The Court held that although search engine operators are not, strictly speaking, prohibited from processing such sensitive data, they must apply a particularly rigorous proportionality assessment before declining a de-referencing request, according significant weight to the data subject's fundamental rights. Read together, these three decisions illustrate an incremental judicial method: the right was first recognised, its territorial scope was then delimited, and the intensity of the balancing exercise was calibrated according to the sensitivity of the data in question a sequencing from which Indian courts, operating without comparable legislative guidance, may usefully draw.

9.2 The United States

The United States has, by contrast, consistently declined to recognise a general Right to Be Forgotten, a position rooted in the primacy accorded to the First Amendment guarantee of freedom of speech and of the press.

American constitutional doctrine treats the publication of truthful information lawfully obtained from public records as deserving of the highest degree of protection, largely irrespective of the passage of time or the reputational consequences to the subject. This principle finds its clearest articulation in *Cox Broadcasting Corp. v. Cohn*, decided by the United States Supreme Court in 1975,⁹ where the Court held that a State could not impose civil liability upon a broadcaster for publishing the name of a deceased rape victim lawfully obtained from public judicial records, reasoning that the interest in privacy necessarily yields when the government itself has placed information in the public domain through its own records.

In the absence of an omnibus federal privacy statute, American regulation of personal data proceeds sectorally: the Children's Online Privacy Protection Act governs data relating to minors; the Health Insurance Portability and Accountability Act governs health information; and, at the State level, the California Consumer Privacy Act confers a qualified right to deletion that is expressly subordinated to countervailing free-speech, journalistic, and public-record exceptions. American commentators and technology companies have consistently expressed concern that a broadly framed Right to Be Forgotten risks functioning as an instrument of censorship, enabling powerful or well-resourced individuals to suppress accurate and matters of public record — a concern that assumes particular significance for a paper examining India,

⁸GC, AF, BH, ED v. Commission Nationale de l'Informatique et des Libertés (CNIL), Case C-136/17, Judgment of the Court of Justice of the European Union, 24 September 2019.

⁹*Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975).

where litigants of means have at times sought to deploy RTBF claims to obscure legitimate matters of public interest such as pending litigation or regulatory action

9.3 Lessons for India

The comparative survey suggests that India's own model ought not to replicate either the European Union or the United States wholesale, but must instead be tailored to India's distinct constitutional structure. From the European experience, three lessons are particularly instructive.

First, a codified procedural framework comparable to the time-bound response mechanism contemplated under Article 17 of the GDPR is necessary to render the right meaningfully enforceable, rather than dependent upon protracted writ litigation before High Courts.

Second, explicit statutory exceptions for journalism, legal proceedings, historical archiving and research are indispensable if the right is not to encroach impermissibly upon free expression and institutional memory.

Third, the independence of the adjudicating authority the Data Protection Board in India's case is a structural precondition for the right's credible enforcement, particularly in disputes involving powerful private or governmental data fiduciaries.

From the American experience, India should draw a corresponding institutional caution: the Right to Be Forgotten must not be permitted to function as a vehicle for suppressing accurate reporting on matters of continuing public concern, particularly reporting concerning public officials, corporate malfeasance, or matters under active judicial or regulatory scrutiny. Consistent with the Puttaswamy proportionality standard and with the approach taken in *Google LLC v. CNIL*, this paper further suggests that any erasure or de-referencing order issued by an Indian court or the Data Protection Board should, at least for the present, operate territorially within India, given the practical and diplomatic difficulties inherent in enforcing extraterritorial deletion against foreign-domiciled intermediaries.

10.0 Legislative and Policy Framework

The principal statutory framework presently governing data erasure in India is the Digital Personal Data Protection Act, 2023 India's first comprehensive data protection legislation.¹⁰ The Act confers upon a "Data Principal" the right to seek correction, completion, updating and erasure of personal data that has been processed on the basis of consent, under Section 12; establishes a mechanism of grievance redressal against a "Data Fiduciary" under Section 13; and constitutes the Data Protection Board of India, under Sections 18 and 19, as the principal

adjudicatory and enforcement authority. Section 17 simultaneously carves out broad exemptions from these obligations, including for the processing of personal data in the interests of the sovereignty and integrity of India, security of the State, and public order, as well as for research, archiving and statistical purposes subject to prescribed safeguards.

The Act's limitations, however, are substantial when assessed against the specific demands of a Right to Be Forgotten framework. First, its erasure right applies only to consent-based processing of digital personal data, and does not squarely address the position of data such as judicial orders or news reporting that was never "processed" pursuant to the Data Principal's consent in the first place. Second, the Data Protection Board, whose members are appointed and whose terms of service are prescribed by the Central Government, lacks the structural independence that characterises supervisory authorities under the GDPR. Third, the Act contains no express, codified balancing test analogous to Article 17(3) of the GDPR, leaving courts and the Board to continue developing standards on an ad hoc, case-by-case basis. Fourth, the Act is silent on the practicalities of cross-border enforcement against data fiduciaries and intermediaries domiciled outside India. For these reasons, while the DPDP Act constitutes an important legislative first step, it remains, in its present form, considerably short of a comprehensive Right to Be Forgotten regime.⁷

10.1 Critical Analysis of the DPDP Act, 2023

A closer examination of Section 12 reveals several specific structural deficiencies that bear directly upon its capacity to accommodate RTBF claims of the kind considered by Indian High Courts.

First, the Act nowhere uses the phrase "Right to Be Forgotten"; it speaks only of a narrower right to "correction and erasure," framed principally as a data-accuracy and consent-withdrawal mechanism rather than as a dignitary or rehabilitative right. This drafting choice risks obscuring the constitutional lineage traced in Puttaswamy and in the subsequent High Court decisions discussed above.

Second, Section 12 does not clarify how the erasure right interacts with judicially published records, government gazettes, or news archives precisely the categories of data that have generated the overwhelming majority of RTBF litigation in India to date. The absence of any

¹⁰The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), received the assent of the President on 11 August 2023.

¹¹Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 17(3).

express carve-out or, conversely, any express inclusion of such records leaves the position doctrinally uncertain.

Third, the exemptions available to government instrumentalities under Section 17 are drafted in broad, open-textured terms "sovereignty and integrity of India," "security of the State," "public order" without the accompanying procedural safeguards, such as periodic review or judicial oversight, that would guard against their disproportionate invocation.

Fourth, as noted above, the Data Protection Board's want of structural independence raises legitimate concern as to its capacity to adjudicate impartially in disputes to which the government itself, or a politically influential data fiduciary, is a party a concern that finds no parallel in the institutionally insulated data protection authorities of EU Member States.

Fifth, the Act contains no equivalent of the specific, codified exceptions to erasure found in Article 17(3) of the GDPR namely, exercise of the right of freedom of expression and information, compliance with a legal obligation, and archiving in the public interest, for scientific or historical research, or for statistical purposes.¹¹ The absence of such a list means that Indian courts and the Board must continue to improvise a balancing standard through case-by-case adjudication, replicating rather than resolving the very uncertainty that has characterised the pre-2023 jurisprudence.

Sixth, the Act offers no mechanism for enforcing erasure or de-referencing orders against data fiduciaries whose servers and principal place of business lie outside India's territorial jurisdiction a gap of considerable practical consequence given that the dominant search engines and hosting platforms implicated in Indian RTBF litigation are foreign-domiciled entities. Taken cumulatively, these deficiencies suggest that Section 12, while representing a necessary legislative acknowledgment of the erasure principle, requires substantial elaboration whether through delegated rules, judicial interpretation, or future amendment before it can function as an effective Right to Be Forgotten framework comparable to its European counterpart.

11.0 Balancing Privacy and Information Rights

11.1 The Proportionality Test and Judicial Balancing

Since Puttaswamy, Indian courts have consistently deployed the four-fold proportionality standard legality, legitimate aim, necessity and proportionality *stricto sensu*, and procedural safeguards as the analytical lens through which competing privacy and transparency claims are adjudicated.

Applied to the RTBF context, the exercise typically requires a court to weigh, on one side, the individual's interest in dignity, rehabilitation and freedom from continuing stigma, and, on the

other, the public's interest in the transparency of judicial and governmental records. The pattern discernible across the decisions discussed in Part 8 is that erasure or masking has generally satisfied this balancing exercise where the underlying matter was resolved through compromise, acquittal, or involved matters of intimate or sexual nature with no continuing accountability function; conversely, relief has been denied where the underlying matter involved corruption, serious or violent offences, or persons holding public office, on the reasoning that the State and citizenry retain a continuing and legitimate interest in the availability of such information.

11.2 Public Interest versus Individual Dignity

At the core of this jurisprudence lies an irreducible tension between individual dignity and society's interest in the availability of information. An individual whose name continues to appear in connection with a decades-old, since-resolved dispute may legitimately contend that continued visibility offends both dignity and the capacity for social and economic reintegration. The countervailing position holds that the public retains a general interest in the availability of judicial and governmental records as an instrument of institutional accountability, historical record-keeping, and the deterrence of future wrongdoing. No court has yet articulated a bright-line rule capable of resolving this tension in the abstract; the prevailing judicial consensus, consistent with the approach adopted in *GC and Others v. CNIL*, is that where data possesses continuing public value as in matters of corruption, serious crime, or the conduct of public office it ought ordinarily to be retained, whereas data that causes stigma without any corresponding public value such as old matrimonial disputes or minor offences long since concluded in acquittal is a more appropriate candidate for erasure or masking.

12.0 Socio-Legal Implications

12.1 Impact on Journalism and Free Speech

An unqualified right to erasure poses a distinct risk to investigative journalism and, by extension, to democratic accountability. Historical reporting on corruption, regulatory violations, and the conduct of public officials constitutes an indispensable resource for both contemporaneous and retrospective public scrutiny. Were such reporting to be readily susceptible to removal upon a bare assertion of privacy, powerful individuals could effectively rewrite the historical record and insulate themselves from accountability for past conduct. It is for this reason that a codified journalism and public-interest exception, comparable to that found in the GDPR, is a structural necessity rather than a mere drafting refinement.

12.2 Criminal Justice and Rehabilitation

The Right to Be Forgotten carries particular significance for the criminal justice system's rehabilitative objectives. Individuals who have been acquitted, or who have completed a sentence for a comparatively minor offence, frequently continue to experience the practical consequences of their earlier prosecution difficulty securing employment, impediments to marriage prospects, and enduring social stigma long after the State's own interest in the matter has been exhausted. At the same time, the public retention of criminal records serves an independent and legitimate function: it operates as a check upon the possibility of wrongful conviction, assists in the prevention of recidivism, and protects collective security, particularly in matters involving offences against the person or the State. A workable balance, consistent with the approach already visible in the Karnataka and Delhi High Court decisions, would retain public visibility for serious offences with continuing public interest, while permitting erasure or masking for minor offences, and for acquittals, after the elapse of a reasonable period during which no fresh public interest has emerged.

12.3 Employment and Digital Reputation

The growing prevalence of employers conducting online background checks only underscores the far-reaching implications of the Right to Be Forgotten. Even relatively trivial and resolved issues an anodyne lawsuit, a past report of an eviction, or an out-of-date, but nonetheless false, report of a bankruptcy may have an outsized effect on a person's ability to find a job in the face of active and unequivocal deleting rights. But at the same time, there are certain kinds of jobs notably ones in the financial, educational and childcare fields where a certain kind of meaningful and ongoing employer interest in verifiable background information arguably exists that should not be defeated by an overbroad erasure right. A proper balancing, again, can be informed by the proportionality standard: ongoing relevance and public-interest value must be measured against the individual's countervailing interest in a truthful digital reputation.

13.0 Challenges in Implementation

13.1 Technical Challenges

The practical realisation of any Right to Be Forgotten confronts significant technical obstacles. De-indexing a webpage from a search engine does not equate to its deletion; the underlying content typically persists on the host server, in web-archiving services such as the Wayback Machine, and across a proliferating universe of content-aggregator and mirror websites that routinely scrape and republish judicial databases. The growing use of personal data in the

training of artificial intelligence systems introduces a further, as yet largely unaddressed, complication: data that has been erased from its original source may nonetheless persist, in some derivative form, within a trained model. Neither the DPDP Act nor the accompanying Rules presently offer a comprehensive answer to these emergent technical realities.

13.2 Jurisdictional Challenges

A substantial proportion of the intermediaries implicated in Indian RTBF litigation principally the major search engines are incorporated and headquartered outside India. As the Court of Justice of the European Union recognised in *Google LLC v. CNIL*, a domestic erasure order faces inherent practical limits when sought to be enforced against a foreign-domiciled entity beyond the territorial reach of the ordering jurisdiction. In the absence of bilateral or multilateral cooperation agreements addressing cross-border data-erasure enforcement, Indian courts and the Data Protection Board will likely continue to depend upon the voluntary compliance of dominant technology platforms, a state of affairs that is structurally precarious and difficult to reconcile with the constitutional character of the underlying right.

13.3 Risk of Misuse

Finally, any Right to Be Forgotten regime carries an inherent risk of misuse. Well-resourced litigants including public officials and corporate entities may invoke privacy claims strategically to suppress accurate and legitimately newsworthy reporting concerning corruption, financial impropriety, or regulatory non-compliance. Smaller media organisations and independent journalists, lacking the resources to sustain protracted litigation, may find it commercially expedient to comply with even questionable erasure demands, producing a chilling effect on investigative reporting disproportionate to any corresponding privacy gain. Robust, codified public-interest exceptions, coupled with appropriate costs or penalty consequences for manifestly frivolous or vexatious erasure claims, are accordingly necessary safeguards against this risk.

14.0 Future Directions and Reforms

Building upon the preceding analysis, this paper recommends the following reforms. First, the Rules framed under the DPDP Act should explicitly recognise a Right to Be Forgotten as a distinct facet of the Section 12 erasure right, rather than leaving its constitutional lineage to inference. Second, a codified list of public-interest exceptions covering journalism, ongoing legal proceedings, open justice, historical archiving, and research should be incorporated,

whether by rule or by future amendment, along lines comparable to Article 17(3) of the GDPR. Third, a defined response timeline, such as the thirty-day period contemplated under the GDPR, should be prescribed for data fiduciaries responding to erasure requests, with a corresponding appellate mechanism before the Data Protection Board and, ultimately, the High Courts. Fourth, the composition and appointment procedure for the Data Protection Board should be reformed to secure genuine institutional independence, including fixed tenure, security of remuneration, and a broad-based, non-executive-dominated appointment process. Fifth, in the absence of workable mechanisms for extraterritorial enforcement, erasure and de-referencing orders should, for the present, be confined in their territorial operation to India, consistent with the approach adopted in *Google LLC v. CNIL*, while India continues to pursue international cooperation frameworks for cross-border data governance.

15.0 Harmonizing Privacy with Transparency

The goal is not to choose between privacy and transparency. It is to design a system where both can coexist — where individuals can escape the permanent shadow of outdated personal information without undermining the public's access to knowledge about matters of genuine concern.

Harmonisation requires a tiered approach:

- Tier 1 Automatic anonymisation. Court records of acquittals, juveniles, and sexual offences can be considered for automatic anonymisation, removing the need to petition for anonymisation. The e-Committee rules should be made mandatory and broadened to apply to all High Courts and district courts.
- Tier 2 delisting ‘upon request’. Individuals must be able to request delisting of information from a search engine where the information is aged, inaccurate, or excessively damaging. Such a request would be determined by a Data Protection Authority employing a proportionality test, with a presumption in favour of delisting where the information relates to a private individual and offers no public value.
- Tier 3 Retention with qualification. In the case where the matter is considered to benefit the public interest using or relying upon as a source public interest journalism about public figures, legal proceedings involving those with public office, reporting of governance matters the IT matter should be retained; it might, however, be

accompanied by contextual notices (such as a banner stating the case was acquitted) or have a temporary-down ranking on search results.

- Tier 4 Open access The information will be required for future legal proceedings, regulation and compliance or historical analysis and thus needs to be freely available.

This layered approach maintains the spectrum between the degree of privacy and the transparency necessary to achieve the right level of facilitation. It enables the law to act selectively, as opposed to either choosing the extremes of both ends of the spectrum anonymization where appropriate, delisting when proportionate, keeping when essential.

16.0 Conclusion

In an era in which data persists indefinitely while human circumstances continue to evolve, the Right to Be Forgotten has moved from a theoretical proposition to a practical necessity within India's constitutional and digital governance framework. The continued availability of resolved personal disputes, judicial records, and archived news reporting exerts a disproportionate and often unwarranted toll upon individual dignity, employment prospects, and social reintegration, long after the underlying matter has ceased to serve any legitimate public function.

The Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India furnished the essential constitutional foundation for this right by recognising privacy as an intrinsic element of Article 21, while simultaneously insisting — through its four-fold proportionality standard — that the right cannot be asserted absolutely against the equally weighty guarantees of free expression and information under Article 19(1)(a). Indian High Courts, proceeding without direct legislative guidance, have responded with a measure of judicial statesmanship, granting relief in matters of intimate or resolved personal disputes, as in Sri Vasunathan and Jorawer Singh Mundy, while withholding it where the public retains a continuing and legitimate interest in the information's availability, as reflected in the more cautious approach of the Kerala High Court and in decisions concerning serious or ongoing matters of public concern.

The Digital Personal Data Protection Act, 2023, despite its clear importance as India's first omnibus data protection legislation, presently provides merely a skeletal and underelaborated right to erasure under section 12, without any codified exception for the public interest, without any prescribed compliance window, and without an institutionally autonomous adjudicatory

authority. If these gaps are left unfilled, the Right to Be Forgotten risks relegating itself to the occasional order of a High Court rather than a consistent, predictable statutory entitlement. As this paper has argued, the way forward cannot be based on the American free-speech model, or on the European template, but an Indian compromise one that draws upon the proportionality concepts articulated in Puttaswamy, takes the GDPR's procedural edifice, and remains mindful of the vital importance of an independent press, in the way of American jurisprudence. A framework of this sort guarantees that transparency and privacy remain not counterpoised, but coagonist: one an individual safeguard, the other a bulwark of accountable democratic institutions.

