

AN EXPLORATORY STUDY OF RECONCILING THE RIGHT TO BE FORGOTTEN AND THE RIGHT TO KNOW IN INDIA THROUGH PRIVACY, TRANSPARENCY AND PUBLIC INTEREST

Jyoti

Ph.D. Research Scholar
Faculty of Law, University of Lucknow, Lucknow

Dr. Ashok Kumar Sonkar

Professor
Faculty of Law, University of Lucknow, Lucknow

ABSTRACT

Recent advances in technology have revolutionized how information is created, collected and shared. This newfound interconnectedness has led to tension between people's right to privacy and societal interests including transparency and access to information. This essay looks at how Indian constitutional and legal doctrine can balance two conflicting concerns, the Right to Know and the Right to Be Forgotten. The Right to Information Act of 2005, the Information Technology Act of 2000, the Digital Personal Data Protection Act of 2023, and the legal developments surrounding the Right to be Forgotten thru significant rulings like Justice K. S. 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 are all examined. We also compare the approaches of EU, UK, US and India towards these two rights. Our review of developments in this field leads us to conclude that privacy and access to information are not absolutes. We present a Privacy–Transparency–Public Interest Framework rooted in principles of proportionality, necessity, public interest, accuracy/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.

Keywords: Right to Be Forgotten, Right to Know, Privacy, Transparency, Public Interest, Informational Privacy, Proportionality, Freedom of Expression, Digital Personal Data Protection, Right to Information, India.

1. INTRODUCTION

1.1 Background of the Study

The unprecedented growth of digital technologies have changed the way in which personal information is generated, stored and shared, making it available online. What may have been accessible for a short time only, could now become permanently searchable through internet searches and online archives. Such developments give rise to an ongoing conflict between the reasonable expectation of privacy, dignity and informational self-determination of an individual vs the public's right to access information. The Right to Be Forgotten caters to this privacy-based need by limiting the perpetual availability of certain information about an individual. On the other hand there is also a Right to Know which allows citizens to have access to information that supports democratic processes. Both rights need to be balanced against each other in India by examining constitutional rights, public interest & proportionality.

1.2 Emergence of the Right to Be Forgotten in the Digital Era

The Right to Be Forgotten came into existence because of how information is stored and accessed in the digital world. In online spaces, personal data and past information published on websites through media coverage or any other means can stay accessible indefinitely. This accessibility can lead to ongoing reputational, social, and privacy harms. In some circumstances, persons can request that this information about them be erased from search results by exercising their right to be forgotten. However, this right needs to be weighed against other crucial rights including the right to free speech, information access, the public interest, and historically significant data.

1.3 Concept and Significance of the Right to Know

A person's or society's right to obtain knowledge is referred to as the "right to know." This right is closely related to the concepts of accountability, transparency, freedom of speech and expression, and access to information held by public bodies in India. The Right to Information Act enables citizens to hold their government responsible for its policies and actions. When information impacts public safety, is of broad public interest, or relates to the actions of public authorities, institutions, and officials, the right to know becomes crucial. Nonetheless, there are situations in which an individual's right to privacy may clash with their right to know. Because of this, issues about privacy, dignity, secrecy, and the public interest should all be taken into account whenever the Right to Know is exercised.

1.4 Privacy, Transparency and Public Interest as Competing Values

Three values that occasionally conflict with one another are privacy, transparency, and public interest. A person's right to their own information and control over it is referred to as privacy. Open communication and the capacity to challenge information are made possible by transparency. The broader criterion that might be used to determine whether something should be kept confidential or made public is the public interest. Under the Right to be Forgotten, information that is private and unimportant to the general public may be kept secret. Information might be considered of public interest if it has significant historical value, pertains to national and public security, or refers to the accountability of institutions, authorities, and the government. Therefore, we need to consider when transparency is preferred and when the public's right to privacy supersedes the public interest.

1.5 Statement of the Research Problem

The need for this study stems from the fact that there is no clear framework or consistent parameters defined for balancing the Right to Be Forgotten and Right to Know in India. Allowing unrestricted deletion or delisting could jeopardize freedom of speech, openness, historical records, and the public interest, even tho it is crucial to shield people from ongoing harassment by persistent information. It becomes considerably more difficult to strike a balance between privacy and the public interest when material pertains to criminal history, public authorities, legal proceedings, journalistic publications, or is of public significance. Both information and privacy interests are addressed by laws and constitutional guaranties. Understanding how these interests might be balanced in relation to elements like proportionality, necessity, time, context, and public interest is necessary.

1.6 Rationale and Significance of the Study

India faces this issue because technology allows once-private information to become permanent, searchable and available at a global scale. Past information about a person may continue to affect their dignity and reputation long after the information itself has become irrelevant. However, allowing free-flow of information all the time can also impact freedom of speech, press, public records and

democracy. There is a need to balance privacy concerns with public interest in democratic societies. This study helps to understand how Indian lawmakers, courts and society can strike this balance. The significance of this study is that it will analyse constitutional values, statutes, case laws and factors involving public interest to identify potential standards that can be applied to strike an equitable balance. The framework established through this study may help policymakers, courts, executives and general public to deal with conflicts between these rights.

1.7 Scope and Delimitations

The study will look into Right to Be Forgotten and Right to Know as legal concepts and frame of analysis. It will focus on how these rights relate to each other in the Indian context through the lens of privacy rights, transparency and public interest. This includes looking into constitutional provisions such as Article 19 and Article 21, legislations such as RTI Act 2005, Information Technology Act 2000 and Digital Personal Data Protection Act 2023 and major judicial interpretations. The author will also look into global frameworks such as those of the European Union, United Kingdom, United States and Canada for a comparative analysis. The study will be delimited by its focus on legal concepts and not measuring opinions through surveys or interviews. This study will focus specifically on digital age challenges such as online information, delisting of links and deletion of personal data.

1.8 Research Questions

1. The reconciliation of Right to Be Forgotten and Right to Know under Indian Constitution and statutes.
2. Role of privacy, transparency, proportionality and public interest while balancing Right to Be Forgotten and Right to Know.
3. What would be the perfect Judicial and Statutory framework balancing privacy of individuals and democratic accountability/access to information in the age of internet.

1.9 Research Objectives

1. Explore conceptual, constitutional and legal basis of the Right to be Forgotten and the Right to Know in India.
2. Study the privacy-transparency-public interest conundrum involved in the decision to erase, delist or retain personal information.
3. Suggest a balancing framework guided by proportionality and sensitive to factors such as public interest, status of the individual, relevance, time and possible harm.

1.10 Research Methodology

It examines the relationship between the Right to Know and the Right to Be Forgotten in the Indian legal setting using an exploratory and doctrinal approach to legal research. Statutes, case law, constitutional clauses, and pertinent legal precepts concerning privacy, openness, freedom of speech, and the public interest are examined. The Indian Constitution, the RTI Act of 2005, the Information Technology Act of 2000, and the Digital Personal Data Protection Act of 2023 are examples of primary legal sources. In addition to regulatory and statutory changes from other jurisdictions such as the European Union (EU), United Kingdom (UK), United States (US), and Canada, significant rulings concerning the rights to privacy, information, and freedom of speech and expression have also been examined. To identify differences, comprehend balancing standards, and propose a flexible framework appropriate for the situation, qualitative and analytical methods are employed.

2. CONCEPTUAL AND THEORETICAL FRAMEWORK

The idea and advancements surrounding the Right to Be Forgotten are covered in this study's theoretical and conceptual foundation. This includes going over the distinction between the right to be delisted from search engines and the right to be erased. The Right to Know will also be defined and explained in this research, along with how it is essential to maintaining the principles of democratic governance. Aspects of the Right to Information (RTI) as a democratic empowerment instrument have been examined. In addition to freedom of speech and expression, concepts of informational privacy have also been researched. Discussions about the public interest and the value of democratic transparency fall under this category. Finally, proportionality as a balancing doctrine and the theoretical tension between the right to privacy and the right to information has been examined.

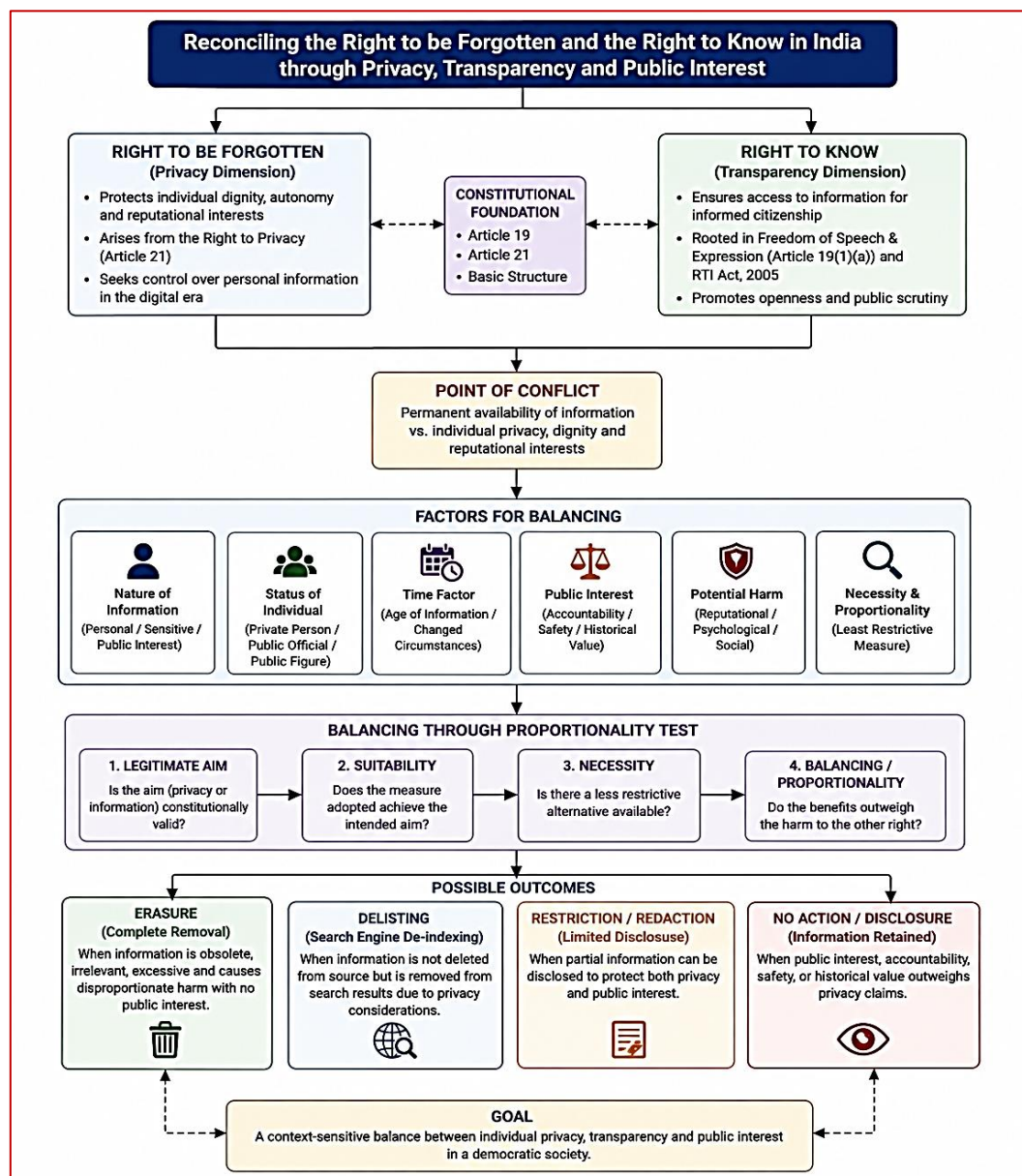


Figure 2.1: Conceptual Flowchart for Reconciling the Right to Be Forgotten and the Right to Know

3. CONSTITUTIONAL FRAMEWORK IN INDIA

3.1 Article 19 and Freedom of Speech and Expression

Article 19(1)(a) enshrines the freedom of speech and expression for all citizens. It is the constitutional bedrock for free communication and the Right to access information. This right implicitly guarantees that all citizens can receive and impart information. Article 19(2) allows the State to impose reasonable restrictions on the exercise of this right on grounds specified therein, which include sovereignty, integrity, security, public order, decency or morality and defamation among others. Therefore, RTK as well as privacy interests have to be balanced within this framework.

3.2 Article 21 and the Right to Privacy

Article 21 of the Constitution guarantees the protection of life and personal liberty. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court recognised privacy as a fundamental right guaranteed under the Constitution. Privacy includes within its ambit concepts of dignity, autonomy and personal liberty. This right is not absolute, and therefore interference by the State would have to meet certain requirements to be constitutionally valid. Establishing that privacy is protected as a fundamental right lays down an important premise for privacy based arguments such as the Right to Be Forgotten claim.

3.3 Informational Autonomy and Personal Data

Informational autonomy can be defined as the capacity of an individual to exert substantial control over their personal information. Constitutional recognition of the right to privacy further fortifies the arguments against unwarranted collection, usage or disclosure of personal data. The right to privacy has been extensively connected with autonomy, dignity and personal liberty by the Supreme Court in *Puttaswamy*. Informational autonomy is crucial in the context of digital technologies because once personal data is converted into digital form, it can be readily stored, processed, reproduced and accessed numerous times.

3.4 Right to Know under Constitutional Jurisprudence

The Right to Know has primarily evolved through judicial interpretation of Article 19(1)(a). Information is vital for citizens to effectively take part in democratic governance and hold public authorities accountable. The RTI Act 2005 went on to create a statutory mechanism through which citizens can access information under the control of public authorities. Section 3 of the RTI Act further explicitly states that all citizens have the right to information that is required by them subject to only such exceptions as are provided under the Act. Therefore, the constitutional right to freedom of speech and expression and a statutory right to transparency coexist.

3.5 Relationship between Articles 19 and 21

Articles 19 and 21 overlap in many ways to protect liberty, freedom of expression and human dignity. Privacy could allow withholding personal data from disclosure. Freedom of speech and expression could allow publication of information and seeking information from others. However, the jurisprudence on privacy developed by the Supreme Court acknowledges that any infringement upon privacy would have to be compatible with the restrictions allowed on the pertinent fundamental right. For example, if a certain restriction affects Article 21 then it would have to pass the proportionality test as laid down under Article 21 jurisprudence. Therefore, any conflicts between privacy and free speech would have to be balanced against each other.

3.6 Constitutional Limitations on Privacy

The Right to Privacy is not an absolute right. The Supreme Court in Puttaswamy acknowledged that legitimate State interests and public interests could still ground restrictions if constitutional requirements are met. Subsequent Supreme Court decisions have clarified that requirements of legality, legitimate State aim, necessity and proportionality must be met for privacy intrusions to be justified. Restrictions on privacy must therefore have some legal basis and cannot be arbitrary, excessive or disproportionate to meet a legitimate aim.

3.7 Public Interest as a Constitutional Consideration

Instances when privacy impacts issues of transparency and disclosure often turn on questions of public interest. Information relating to public safety concerns, governmental accountability, crime prevention or public officials’ conduct have significant public-interest considerations. Notably, the RTI Act also accepts that there could be circumstances where the larger public interest would justify disclosure despite these protected interests. In this way public interest can play a major role in determining whether privacy interests or the need for continued information access should take precedence.

3.8 Balancing Fundamental Rights

Privacy and freedom of information are fundamental rights that must be balanced against each other in cases where they conflict. Balancing does not mean that one right is inherently superior to another. Instead, courts must consider the constitutional interests at stake in each case. Factors relevant for purposes of this balancing include the nature of the information at issue, the sensitivity of the information, the status of the affected individual, the passage of time, the public-interest value of the information, the likelihood of harm supported by the specific facts, the historical significance of the information and the necessity and efficacy of less restrictive measures. Proportionality can be used as an effective tool to determine whether privacy or free flow of information produces the result that is more justified under the Constitution.

4. LEGAL AND REGULATORY FRAMEWORK

India’s privacy and access to information-related legal framework includes the RTI Act 2005, Information Technology Act 2000, IT Rules 2021, and Digital Personal Data Protection Act 2023. Under RTI, the general rule is to promote transparency and disclosure with protections around the release of personal information which would constitute an unwarranted invasion of privacy. Disclosure could still be considered if public interest justifies the release of such information. The IT Act governs electronic records and online activity and the IT Rules provide for due-diligence and grievance-redressal responsibilities of internet intermediaries. The DPDP Act governs rights around digital personal data and establishes the rights of individuals around their data including rights to correction and erasure. It also defines roles and responsibilities for processing personal data of “Data Principal” by a “Data Fiduciary”. The DPDP Act is scheduled to be implemented in phases as per government notifications. Rules.gov.in notified the DPDP Rules, 2025 in November 2025.

Table 4.1: Legal and Regulatory Framework for Reconciling the Right to Be Forgotten and the Right to Know

Legal/Regulatory Instrument	Relevant Provision/Principle	Relevance to the Study
RTI Act, 2005	Right of citizens to access information held by public authorities	Promotes transparency, accountability and democratic participation
Privacy Exemptions under	Section 8(1)(j) protects specified personal	Creates a direct privacy–transparency

RTI	information from disclosure, subject to larger public interest	balancing mechanism
Information Technology Act, 2000	Provides the foundational statutory framework for electronic records and digital transactions	Regulates the broader digital environment in which personal information is processed
IT Rules, 2021	Intermediary due diligence, grievance redressal and content-related obligations	Relevant to removal, restriction and handling of online information
DPDP Act, 2023	Controls how digital personal data is processed	Provides a modern data-protection framework for informational privacy
Right to Erasure	Section 12 recognises correction, updating and erasure subject to legal requirements	Directly relevant to the Right to Be Forgotten
Data Principal	Individual to whom personal data relates	Places the individual at the centre of data-protection rights
Data Fiduciary	Entity determining the purpose and means of processing personal data	Bears statutory responsibilities for lawful and secure processing
Data Protection–RTI Relationship	Privacy protection must be considered alongside legitimate access to public information	Represents the central legal tension examined in the study
Emerging Regulatory Challenges	Digital permanence, algorithmic visibility, archives, AI and cross-border processing	Require context-sensitive balancing of privacy, transparency and public interest

Source: Synthesized from legislation cited in the study and present-day legal documents. The study uploaded here clearly mentions RTI Act, IT Act, IT Rules, DPDP Act, right to be forgotten guidelines, Data Fiduciaries/Data Principals and Data protection vs RTI as constituents of the legal framework.

Clearly defines personal information and lays down a public-interest override provision in Section 8(1)(j); Section 8(2) also acknowledges instances where the larger public interest in disclosure is served.

5. JUDICIAL EVOLUTION OF THE RIGHT TO BE FORGOTTEN IN INDIA

5.1 Early Judicial Recognition

While India did not see an explicit development of a Right to Be Forgotten before that terminology gained currency, certain principles fundamental to it such as privacy, dignity, reputation and right to be left alone have been developed by courts in India. Recognising privacy as a fundamental right emanating from Article 21, the Supreme Court in *R. Rajagopal v. State of Tamil Nadu* (1994) put curbs on the unauthorised publication of personal matters but held that information already in public records enjoyed higher protection from disclosure. This case laid the groundwork for subsequent jurisprudence on RTBF.

5.2 Privacy Jurisprudence after *Justice K.S. Puttaswamy v. Union of India*

The nine judge Bench of the Supreme Court unanimously held privacy as a fundamental right in *Justice K. S. Puttaswamy v. Union of India* (2017), especially as related to dignity, liberty and autonomy under Article 21 of the Constitution. The judgment offered constitutional basis for informational privacy and ensuing RTBF claims. The judgment stopped short of fashioning a freestanding statutory RTBF that could be directly enforced in courts; lower courts have since fleshed out the principle on a piecemeal basis, case-by-case.

5.3 *Rajagopal v. State of Tamil Nadu*

In *R. Rajagopal v. State of Tamil Nadu* (1994), popularly known as the Auto Shankar case, the Supreme Court upheld that Right to Privacy conflicts with the freedom of press. According to the

Court, privacy applies to personal affairs, which they termed as "right to be let alone." Matters of public records like court records, however, were open for publication. The case, therefore, set up an early limit between privacy and free speech.

5.4 Dharamraj Bhanushankar Dave v. State of Gujarat

Dharamraj Bhanushankar Dave v. State of Gujarat involved a petitioner requesting redress related to criminal proceedings information remaining available online about which he was later acquitted. The Gujarat High Court took a narrow view and declined to grant sweeping RTBF relief. The ruling gained attention due to courts being hesitant to view online removal of judicial information as a presumed privacy right.

5.5 Subhranshu Rout v. State of Odisha

RTBF was considered by the Orissa High Court in *Subhranshu Rout v. State of Odisha* (20CRIM202/20). In the case related to objectionable photographs and videos of intimate nature which were allegedly shared without consent of the involved party, the Court noted that there was no law explicitly providing for the right to be forgotten in India at that point of time but linked RTBF to the right to privacy under Article 21. While doing so, it stated that this right cannot trump freedom of speech and expression and other activities like legal reliance, public interest, historical research or any other legitimate interest when there is a need for that information to be available.

5.6 Jorawar Singh Mundy v. Union of India

Jorawar Singh Mundy v. Union of India involved a petition before the Delhi High Court challenging accessibility online of a criminal judgment after acquittal. The petitioner sought relief claiming that continued searchability was adversely affecting his employment opportunities. The Delhi HC issued interim relief granting protection from interim steps relating to removal/ de-indexing on April 20, 21 essentially bringing the privacy–public- access conflict full circle before the Court. The petition got clubbed with larger proceedings relating to RTBF.

5.7 Other Relevant High Court Decisions

Some High Courts have also issued judgments on RTBF issues. The Karnataka High Court in the case of *Sri Vasunathan v. Registrar General* noted privacy based protection in intimate issues. The Karnataka High Court also allowed a woman to get her daughter's name removed from an online judgment in a separate case. The Delhi High Court in *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.* acknowledged RTBF and right to be left alone as facets of the right to privacy.

5.8 Emerging Judicial Standards

Indian courts are beginning to show signs of adopting a contextual approach rather than absolutizing RTBF claims. Considerations highlighted include the type of information, sensitivity, passage of time, stature of the person involved, accuracy, potential harm and damage, public-interest element, historical value and freedom of speech considerations. Courts may even differentiate between content deletion vs delisting from search engines. Proportionality and necessity are emerging principles as considerations for determining whether privacy concerns trump public access.

5.9 Gaps in Judicial Consensus

India lacks judicial clarity on several aspects of the exact contours, enforceability and limitations of RTBF. Courts have varied in their decisions especially with regards to online court records, public documents and the interplay between privacy and public interest in information. Lack of statutory

clarity has led to adjudication on a case-by-case basis. Ongoing cases in Delhi High Court further illustrate the conflicts between requests for erasure and open courts, transparency, accurate press reporting and access to judicial information.

6. RIGHT TO KNOW AND THE IMPERATIVE OF TRANSPARENCY

RTK) movement has gained increasing importance as a citizen's right to participate in a democratic society and have transparency and accountability from their government in India. Constitutionally, RTK movement is intimately linked to Article 19(1)(a). Statutorily speaking, citizens have the right to access information under the RTI Act, 2005 that is held by or under the control of public authorities. Individuals may inspect and take copies of documents or "information in electronic form" under the RTI Act. However, there are exemptions to this right under section 8 which allows withholding of information in the interests of national sovereignty and integrity, defence, foreign relation and information including commercial confidence or trade secrets in possession of the state. The Right to Privacy also has to be balanced against the Right to Know especially where larger public interest is involved. Information pertaining to public records, investigative journalism and information on public officials can greatly aid in keeping elected officials and those in power accountable. Over blocking of information can harm democratic oversight of the government, ruin our historical record and hinder freedom of speech. It is for this reason that a healthy balance has to be struck between transparency and the right to privacy. Balancing privacy with RTK forms the main focus of this paper.

7. RECONCILING PRIVACY WITH THE RIGHT TO KNOW

Finding the middle ground between Privacy and RTK forms the main focus of analysis of this paper. Privacy and RTK often come into conflict because the former seeks to protect personal liberties like dignity and autonomy as well as personal information. On the other hand, RTK aids in transparency and accountability. This becomes especially confusing when we deal with public personalities/public figures, public officials, criminal records, judgements/orders, etc. and archives maintained by news/media organisations. This paper differentiates between delisting from search engines and erasure because delisting from search engines doesn't truly erase anything. Taking factors like proportionality, necessity, public interest involved, status of the individual concerned, harm that may be caused to the individual, importance in terms of history and the amount of time that's passed into consideration, we can definitely find a middle ground as to when Privacy should take precedence over making information continue to remain accessible to the public.

8. PUBLIC INTEREST AS THE CENTRAL BALANCING PRINCIPLE

Public interest can provide fairness across the balancing test of Right to Be Forgotten and Right to Know. Specifically in cases where disclosure would contribute to public safety, crime prevention, official accountability, journalism or historical memory. However, there is an important distinction between true public interest and public curiosity, with the latter not justifying an invasion of privacy. Information about public officials, institutional wrongdoing and public safety may carry more weight for continued access. Likewise those who are vulnerable may deserve additional protection. News publication can contribute towards democratic accountability if the material relates to matters of public interest. Historical and archival data may also preserve public value despite being older. Public interest considerations should be weighed against the nature, sensitivity, accuracy, relevance, age of information, potential harm, historical significance, status of individual and proportionality of continued publication or disclosure.

9. COMPARATIVE LEGAL PERSPECTIVE

9.1 European Union

One of the most advanced legislative frameworks in the world to strike a balance between privacy rights and information access is found in EU law. Article 11 of the EU Charter of Fundamental Rights safeguards freedom of expression and information, whereas Articles 7 and 8 protect private life and personal data. In *Google Spain SL v. AEPD and Mario Costeja González* (C-131/12, 2014), the Court of Justice of the European Union significantly established privacy rights against Google search engine results. According to the Court's ruling, search engines may be forced to remove information about an individual if it is excessive, irrelevant, or insufficient when weighed against other public interests. Delisting regarding individuals became a crucial European privacy remedy as a result of this significant ruling.

9.2 Google Spain v. AEPD and Mario Costeja González

The Court of Justice of the European Union's landmark ruling, C-131/12 (2014), is *Google Spain*. Mario Costeja González's efforts to have his name removed from Google search results that linked him to previous newspaper ads on property sale notices were at issue in this case. Google was found to be a data controller with regard to search engine processing by the CJEU. It outlined the few situations in which Google could have to remove information from its list at a person's request. The Court weighed the public's right to access that information against each person's right to data privacy. Articles 7 and 8 of the EU Charter and the then-current Directive 95/46/EC served as the foundation for the decision. The most significant European court case pertaining to the modern Right to Be Forgotten was *Google Spain*.

9.3 General Data Protection Regulation and the Right to Erasure

The Right to Erasure is guarantyd by Article 17 of the General Data Protection Regulation. The Right to Be Forgotten is a typical term for it. In situations such when the information is no longer required, consent is revoked, data is processed illegally, or the data subject objects, GDPR allows the erasure of personal data. However, recital 53 has many flaws. The right to freedom of expression and information is exempt under Article 17(3). For example, where processing is necessary to fulfill a legal requirement, there is a public interest in doing so, public health issues, archiving, scientific-historical research, or establishing legal rights. Therefore, erasing is not seen as an absolute right in European law. The GDPR clause strikes a crucial balance between genuine public access interests and privacy.

9.4 United Kingdom

The United Kingdom and the European Union (UK) are essentially still operating under the UK GDPR and Data Protection Act 2018 regime, which permits a right to erasure with some restrictions. Right to Erasure: Under Article 17 of the UK GDPR, people have the right to have their personal data deleted under specific conditions. However, the right to erasure is not unqualified because there are exceptions to the right, such as when keeping the material related to exercising the right to freedom of expression and information, legal obligations, public-interest tasks, or legal claims. Additionally, the Data Protection Act of 2018 provides exceptions to the UK GDPR for literary, artistic, scholarly, and journalistic reasons. In essence, the British approach seeks to strike a balance between the need for the public interest, freedom of expression, and individual privacy rights.

9.5 United States

The United States takes a significantly different stance since the country's legal system weighs privacy considerations pertaining to information dissemination against a strong First Amendment tradition. A general right to be forgotten thru statutory procedures comparable to GDPR Article 17 is not provided by the U.S. Constitution. Instead, in *Packingham v. North Carolina* (2017), the Supreme Court overturned a sweeping clause that made it illegal for registered sex offenders to access social media sites while upholding the importance of the internet and social media for the Constitutionally protected right to free speech. As a result, the American judiciary places more stress on information access and freedom of speech. This creates resistance to any widespread mandatory delisting or deletion policy.

9.6 Canada

When weighing privacy rights against freedom of expression and court-ordered removal of internet content, Canada takes a more contextual approach. In *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34, Canadian courts ordered Google to de-index specific websites worldwide because they engaged in illegal business activities. Because it was necessary to stop ongoing injury, the Supreme Court of Canada ruled that such a global injunction was legitimate. This demonstrates that Canadian courts are prepared to provide wide orders of delisting when it is required to prevent harm, even tho it was not precisely a personal-data RTBF case. However, this ruling has sparked a number of questions regarding jurisdiction, worldwide ramifications of court rulings based online, and freedom of expression.

9.7 Comparative Approaches to Privacy and Public Access

In comparison, the European model offers a somewhat more robust acknowledgment of data privacy regulations and search engine delisting. However, there are some exceptions that weigh the rights against the public interest, freedom of speech, and information. The UK's GDPR and Data Protection Act of 2018 take a similar stance when it comes to striking a balance between rights.

The United States lacks a general RTBF framework and places more emphasis on First Amendment rights, giving freedom of expression more weight. In Canada, there is more judicial recognition of the need to issue delist orders in order to protect against ongoing injury. Therefore, compared to the United States, the European Union, the United Kingdom, and Canada provide their citizens superior data protection regulations (shown by Packingham).

However, these distinctions show that judicial interpretations, statutory recognition, and constitutional framework are crucial in striking a balance between privacy and public access.

9.8 Lessons for the Indian Legal Framework

India may benefit from a couple of the conclusions. First of all, the right to be forgotten should not be unqualified or function as a direct right to erasure. By keeping the concepts of erasure and delisting outside from search engines, the European framework adds value to this strategy. Additionally, as demonstrated by GDPR Article 17, there ought to be clear exceptions for the public interest. Second, the United States of America has demonstrated how important it is to safeguard information access and freedom of speech and expression. Thirdly, certain exclusions for scholarly and journalistic objectives are valuable in the UK. Canada demonstrates how courts can issue customized de-indexing orders. Therefore, the framework for India should include proportionality analysis based on elements including information sensitivity, accuracy, age, public interest, individual status, historic relevance, and least restrictive ways.

Comparative Legal Position at a Glance

Jurisdiction	Principal Legal Basis	Leading Case/Provision	Dominant Approach
European Union	EU Charter; GDPR	<i>Google Spain</i> ; GDPR Article 17	Strong privacy and delisting protection, subject to exceptions
United Kingdom	UK GDPR; Data Protection Act 2018	Article 17; journalism exemptions	Privacy balanced with expression and public interest
United States	First Amendment	<i>Packingham v. North Carolina</i>	Strong protection for freedom of expression
Canada	Privacy/common law and judicial remedies	<i>Google v. Equustek</i>	Contextual and remedy-oriented de-indexing
India	Articles 19 & 21; RTI Act 2005; DPDP Act 2023	<i>Puttaswamy, Jorawar Singh Mundy</i> and other High Court decisions	Emerging, case-by-case proportionality approach

10. EMERGING CHALLENGES IN THE DIGITAL ENVIRONMENT

Nature of technology can undermine RTBF requests. Digital information can be ubiquitous, persistent, searchable and easily replicated. Search engines and algorithms control what information surfaces and can easily amplify old or sensitive information. Social-media platforms enable exponential unregulated sharing. Artificial intelligence enables machine profiling and algorithmic discrimination and poses new threats to informational self-determination; According to UNESCO ".

AI-powered systems increasingly impact how our information is processed, moderated, and used to make decisions that affect privacy." Deepfake technology harms digital identities and reputations. Data brokers enable mass commercial surveillance and processing. Re-publication and digital archives pose obstacles to deletion for historical preservation. International data-transfer poses additional complexities.

DPDP Act, 2023 provides a Right to correction and erasure under Section 12 subject to conditions. According to UNESCO "Incidents of misuse of AI-generated deepfake content increased 26-fold from 2012 into last year." Ubiquity of technology can make RTBF remedies ineffective.

11. EXPLORATORY ANALYSIS

The Exploratory Analysis puts together the legal conclusions drawn from the precedents and the concepts presented within the framework by mapping out the conflicts between the Right to Privacy and Right to Know which have been highlighted during the study. Right to privacy majorly conflicts with dignity, freedom of speech and expression, transparency and public access. Private information which is highly sensitive, intimate and vulnerable person data should be given more protection under the privacy laws whereas data which can affect public safety, state accountability, expose crime and relate to public interest should lean towards the right to know and transparency. Information which receives consent from the data principal for processing would have a strong ground to be kept private but that will not absolutely hold up against legit public interest and lawful conditions. Considering factors such as lapse of time, context, veracity of information, status of the individual and potential harm can help resolve these conflicts. Harm to an individual can be physical, financial, psychological or emotional. Past information which has historical significance or value should be considered for public interest. Constitution of India recognizes privacy as a fundamental right from *Puttaswamy* and DPDP Act, 2023 recognizes right to correction and erasure..

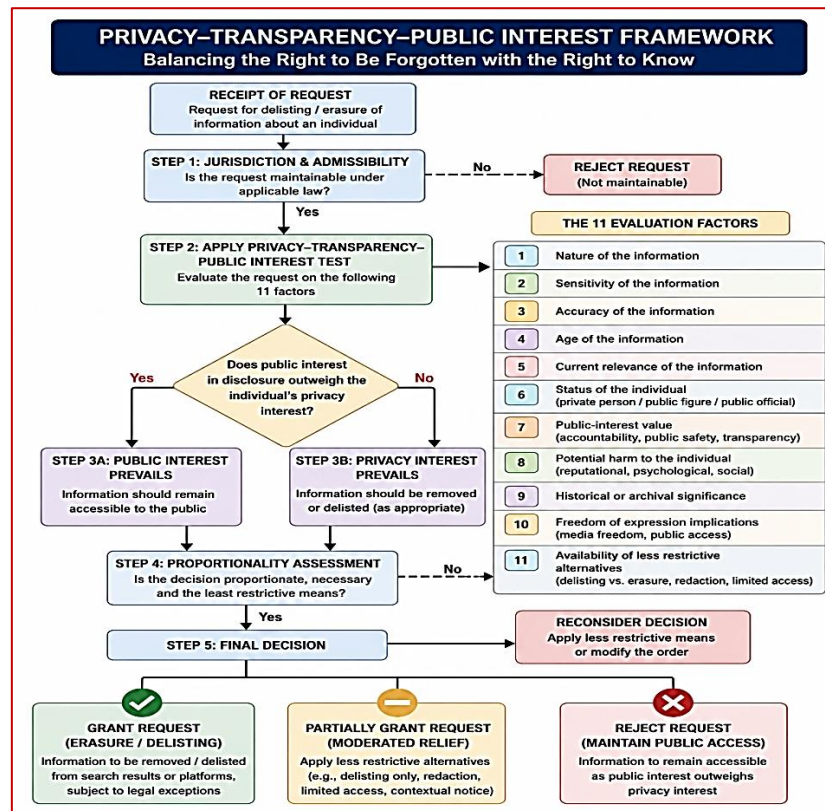
Factor	Supports Right to be Forgotten	Supports Right to Know
Nature of information	Highly personal	Public-interest information
Passage of time	Long passage	Recent/relevant information
Individual status	Private individual	Public official/public figure
Potential harm	Significant reputational/privacy harm	Limited individual harm
Public interest	Low	High
Historical value	Low	High
Criminal/public accountability	Limited	Strong
Consent	Withdrawn/absent	Information already lawfully public

12. FINDINGS AND DISCUSSION

The study comes to the conclusion that courts can harmonize the Right to Know and the Right to Be Forgotten by using a context-dependent balancing approach. The right to freedom of speech and expression under Article 19(1)(a) and the right to privacy, dignity, and personal liberty under Article 21 are in contradiction with one another. There are unclear gaps in Indian jurisprudence, with courts taking different stances on information erasure, delisting, and ongoing accessible. The Digital Personal Data Protection Act, 2023 does not provide complete erasure, even tho it strengthens an individual's right to data protection. In order to balance these rights, statutes must establish clear guidelines based on the concepts of necessity, proportionality, and constraint, in addition to the general public's interest, the accuracy of the material, its relevance to public knowledge, potential harm, the individual's stature, the type of historical information, and its historical value. Courts can use this balancing test when hearing cases, authorities can be tasked with developing standard operating procedures, online platforms can be programd to protect valid privacy concerns, and citizens can be informed about their rights to information and privacy.

13. PROPOSED FRAMEWORK FOR BALANCING THE TWO RIGHTS

Four-step tests are recommended as a systematic method to manage requests for delisting or erasure in Guidance paper No. 15 on the proposed "Privacy–Transparency–Public Interest Framework." First, assess the type and severity of the sought information, as well as its timeliness, correctness, current relevance, and the person's stature. Second, examine its significance as historical or archive information, its impact on freedom of expression issues, and its public-interest value in relation to any possible harm to an individual. Third, think about whether there are less restrictive options that could sufficiently address privacy issues without unreasonably constraining the information, such as delisting or limiting access to the link. Last but not least, decision-makers should use a proportionality test, weighing other constitutional and public interests against the necessity of erasing or continuing to publish the link.



14. RECOMMENDATIONS

It implies that by using a context-based approach, judicial guidelines with particular norms might be developed for the uniform implementation of RTBF. Public interest exclusions should be clearly acknowledged when interpreting valid grounds. Expression via academic, research, and journalistic endeavors must be sufficiently protected. Celebrities and public officials can be distinguished based on how the material relates to their accountability. History and archival materials should not be delisted. Delisting requests should be accessible, transparent, and supported by independent oversight. The connection between RTI and data-protection regulations should also be clarified. Citizens should participate in data protection awareness campaigns that address digital privacy, data rights, information rights, and remedies.

CONCLUSION

Based on privacy concerns, the RTBF is an emerging right. It seeks to safeguard people's autonomy, dignity, and privacy. Conversely, the Right to Know encourages responsibility, openness, and informed citizens. Neither of these rights is absolute; they must be balanced. When determining whether it is appropriate to withhold or remove information, proportionality, necessity, and the public interest should be taken into consideration. Finding a middle ground should take into consideration a number of factors, including the nature of the information, its sensitivity, accuracy, age, and relevance, the person's standing, the possible harm that may be inflicted, and the importance of history. India must create a sophisticated and moral framework that safeguards privacy without compromising the right to free speech and information access. The evolution of this jurisprudence by courts, the function of digital platforms, regulatory frameworks, and global models could all be the subject of more investigation.

REFERENCES

Books

1. Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.
2. Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
3. Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.
4. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
5. Richards, N. M. (2015). *Intellectual privacy: Rethinking civil liberties in the digital age*. Oxford University Press.
6. Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Journal Articles

1. Ambrose, M. L. (2013). It's about time: Privacy, information lifecycles, and the right to be forgotten. *Stanford Technology Law Review*, 16, 369–422.
2. Ambrose, M. L., & Ausloos, J. (2013). The right to be forgotten across the pond. *Journal of Information Policy*, 3, 1–23.
3. Cohen, J. E. (1999). Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, 52(5), 1373–1438.
4. Fabbrini, F., & Celeste, E. (2020). The right to be forgotten in the digital age: The challenges of data protection beyond borders. *German Law Journal*, 21, 55–65.
5. Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal*, 89(3), 421–471.
6. Koops, B.-J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the “right to be forgotten” in big data practice. *SCRIPTed*, 8(3), 229–256.
7. Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–158.
8. Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online*, 64, 88–92.
9. Youm, K. H., & Park, A. (2016). The “right to be forgotten” in European Union law: Data protection balanced with free speech? *Journalism & Mass Communication Quarterly*, 93(2), 373–390.

Cases

10. Dharamraj Bhanushankar Dave v. State of Gujarat, 2015 SCC OnLine Guj 2019 (Gujarat High Court).
11. Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), Case C-507/17 (Court of Justice of the European Union, 2019).
12. Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, Case C-131/12 (Court of Justice of the European Union, 2014).
13. Google Inc. v. Equustek Solutions Inc., 2017 SCC 34 (Supreme Court of Canada).
14. Jorawar Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306 (Delhi High Court).
15. Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).
16. Packingham v. North Carolina, 582 U.S. 98 (2017) (Supreme Court of the United States).
17. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (Supreme Court of India).
18. Subhanshu Rout v. State of Odisha, 2020 SCC OnLine Ori 878 (Orissa High Court).

Reports and Policy Documents

19. Article 29 Data Protection Working Party. (2014). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217). European Commission.

-
20. Article 29 Data Protection Working Party. (2019). Guidelines 5/2019 on the criteria of the right to be forgotten in the search engines cases under the GDPR (Part 1). European Data Protection Board.
 21. European Commission. (2012). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM/2012/011 final).
 22. Google Advisory Council. (2015). Report of the advisory council to Google on the right to be forgotten. Google.
 23. Ministry of Electronics and Information Technology. (2018). A free and fair digital economy: Protecting privacy, empowering Indians (Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna). Government of India.
 24. United Nations Human Rights Council. (2013). The right to privacy in the digital age (A/HRC/27/37). United Nations.