THE RIGHT TO BE FORGOTTEN IN INDIA: CURRENT LEGAL STANCE, JUDICIAL TRENDS AND EMERGING CHALLENGES

Abhipsa Pati

The "Right to Be Forgotten" (RTBF) allows individuals to request the removal of personal information from online platforms and databases when that information is outdated, inaccurate, irrelevant, or no longer serves its original purpose. The doctrine is intended to balance an individual's interest in privacy with the public's interest in access to information, often requiring search engines and data controllers to delete or delist material under defined circumstances.

RTBF first received formal recognition in the European Union through the Court of Justice of the European Union's 2014 decision in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*[1]. The court interpreted the 1995 Data Protection Directive to permit individuals to request the removal of search results linking to personal data. This principle was later incorporated into the General Data Protection Regulation (GDPR), adopted in April 2016 and effective from May 2018. Article 17[2] of the GDPR codifies RTBF, authorizing erasure where data is no longer needed for its original purpose, where consent is withdrawn, or where the processing lacks a lawful basis.

Public concern over the handling of personal data has expanded sharply in recent years, leading to greater scrutiny of how digital platforms collect and use information. A 2023 Cisco survey[3] reported that 92 percent of global consumers favor stronger data protection laws, and 81 percent have taken steps such as modifying privacy settings or using VPNs. The rise of social media and search engine indexing has intensified the demand for legal mechanisms that allow individuals to control their online presence.

Google's Transparency Report illustrates the trend: as of July 2025, the company had received over 5.8 million URL delisting requests under RTBF since 2014, approving roughly 45 percent of them. This is a significant increase from the 2.4 million requests recorded in early 2018,

---

[1] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317 (May 13, 2014)

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) 1

[3] Cisco, Cisco 2023 Consumer Privacy Survey (2023), <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2023.pdf>

when approximately 43 percent were approved. The economic impact is also notable. The global data privacy software market, valued at $2.76 billion in 2023, is projected to reach between $25.85 and $48.28 billion over the next decade, with growth driven by regulatory requirements and rising cybersecurity risks. A 2024 Pew Research survey similarly found that 79 percent of adults expressed concern about corporate use of personal data, and 85 percent had taken steps to strengthen their own privacy.

The *Google Spain* case underscored the conflict between privacy and the free flow of information. In 1998, Spanish national Mario Costeja González placed a newspaper notice about a property sale linked to a period of financial difficulty. Years later, the digitized version of the notice continued to appear in search results, damaging his reputation despite the matter being resolved. In 2010, González lodged a complaint with Spain's AEPD, leading to a referral to the CJEU. On May 13, 2014, the court ruled in his favor, establishing that individuals may demand the delisting of personal data from search results even if it was lawfully published at the time, provided that the public interest does not outweigh the request. A 2019 CJEU decision in *Google LLC v. CNIL*[4] clarified that RTBF applies within EU jurisdictions but does not impose a global delisting obligation.

In India, the RTBF has emerged through case law rather than direct legislation. The Supreme Court's 2017 judgment in *K.S. Puttaswamy v. Union of India*[5] recognized privacy as a fundamental right under Article 21 of the Constitution, creating the foundation for RTBF as an extension of that right. The Digital Personal Data Protection Act (DPDP Act) 2023 now provides a statutory framework. Section 8(7) permits individuals to request deletion of personal data where it is unnecessary, processed without consent, or handled unlawfully. As of July 2025, the Act awaits full implementation pending the creation of the Data Protection Board and subsidiary rules.

Indian courts have approached RTBF cautiously, weighing privacy against public record obligations. In *Sri Vasunathan v. Registrar General* (2017)[6], the Karnataka High Court ordered the removal of a petitioner's name from online court records to protect his reputation. Conversely, the Gujarat High Court in *Dharamraj Bhanushankar Dave v. State of Gujarat* (2015)[7] refused to erase an acquittal judgment, holding that judicial records form part of the public domain. A 2023 Internet Freedom Foundation study documented over 50 RTBF-related

[4] Case C-507/17, Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL), ECLI:EU:C:2019:772 (Sept. 24, 2019)

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

[6] Sri Vasunathan v. Registrar Gen., 2017 SCC OnLine Kar 424 (India)

[7] Dharamraj Bhanushankar Dave v. State of Gujarat, 2015 SCC OnLine Guj 2019 (India)

petitions since 2017, with courts siding with privacy interests in approximately 60 percent of sensitive cases.

RTBF addresses the persistence of online records in an era where past information can shape present opportunities. Its relevance is clear in employment contexts: studies show that 70 percent of employers review candidates' online presence, and 57 percent acknowledge that older digital content influences hiring decisions.

This paper analyzes India's current legal stance on the Right to Be Forgotten, the fragmented judicial approaches shaping its contours, and the constitutional and administrative challenges that continue to hinder its consistent enforcement.

LITERATURE REVIEW

The Right to Be Forgotten (RTBF) is a legal mechanism that allows individuals to request the removal of personal data from digital archives when the information has become outdated, inaccurate, or harmful. It seeks to navigate the tension between privacy rights and access to information. RTBF became a defined legal right in the European Union through Article 17 of the General Data Protection Regulation (GDPR), adopted in 2016 and in force since 2018. Article 17 provides for erasure when data is no longer relevant, when consent has been withdrawn without other legal justification for retention, or when the processing itself is unlawful.

The idea behind RTBF is rooted in both dignity-based theories of privacy and pragmatic balancing tests. It reflects the view that control over one's personal information is tied to autonomy and self-determination, while also requiring that individual claims be weighed against the public value of retaining data. In Europe, this balance is overseen by both regulatory bodies and courts. France's Commission Nationale de l'Informatique et des Libertés (CNIL), empowered under the amended 1978 Data Protection Act, has taken an active role in ordering the removal of online material to prevent reputational harm. German law approaches the issue through the concept of informational self-determination, first articulated in the Federal Constitutional Court's 1983 Census Judgment, and applies proportionality analysis when weighing privacy under Article 8 of the European Convention on Human Rights against freedom of expression.

The CJEU's 2014 decision in *Google Spain SL v. AEPD* established the doctrinal framework for RTBF in the EU. The court adopted a "fair balance" test, requiring outdated or irrelevant search results to be removed while protecting journalistic activity. Five years later, *Google LLC v. CNIL* clarified the territorial scope, limiting delisting obligations to EU domains to avoid imposing global censorship. These rulings reflect the use of proportionality as the core

tool for reconciling privacy and speech within a digital environment. The debate has also been shaped by Helen Nissenbaum's[8] contextual integrity theory, which views privacy violations as the disruption of expected information flows, and by the European Court of Human Rights' doctrine of legitimate expectations in data processing, which recognizes that information should not remain perpetually accessible without limit.

The United States takes a markedly different view. First Amendment jurisprudence places a heavy thumb on the scale for speech, leaving little room for RTBF-type claims. The California Court of Appeal's decision in *Melvin v. Reid* (1931)[9] hinted at a privacy-based remedy for reputational harm, drawing on the Warren and Brandeis[10] conception of the "right to be let alone" from their 1890 Harvard Law Review article. Yet subsequent cases cut against such claims. In *Sidis v. F-R Publishing Corp.* (1940)[11], the Second Circuit held that the press could revisit the private life of a former public figure, and in *Garcia v. Google* (2015)[12], the Ninth Circuit rejected takedown demands, warning of the chilling effect on expression. American courts have thus generally prioritized the public value of historical records and open discourse over deletion requests.

Outside the Atlantic axis, other jurisdictions have developed their own approaches. In Latin America, habeas data provisions in constitutions such as Argentina's 1994 charter allow individuals to access and correct personal information, and courts have applied these provisions to search engines in cases like *Rodriguez v. Google* (2006)[13]. Japan's Act on the Protection of Personal Information, amended in 2017, incorporates RTBF elements while reflecting the United Nations'[14] Guiding Principles on Business and Human Rights, which frame corporate obligations in data governance. Recent UN reports have described RTBF as part of a broader "digital dignity" agenda, especially in contexts where information asymmetries make individuals vulnerable to exploitation.

In India, RTBF has taken shape primarily through judicial decisions. The Supreme Court's ruling in *K.S. Puttaswamy v. Union of India* (2017) recognized privacy as a fundamental right under Article 21 of the Constitution and laid the groundwork for RTBF as an extension of that

[8] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford Univ. Press 2010)
[9] Melvin v. Reid, 112 Cal. App. 285 (Ct. App. 1931)
[10] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).
[11] Sidis v. F-R Publ'g Corp., 113 F.2d 806 (2d Cir. 1940)
[12] Garcia v. Google, Inc., 786 F.3d 733 (9th Cir. 2015)
[13] Rodriguez v. Google, Inc., Corte Suprema de Justicia de la Nación [CSJN] [National Supreme Court of Justice], 28/10/2014, "Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios" (Arg.)
[14] U.N. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011)

right. The Digital Personal Data Protection Act (DPDP Act) 2023 now provides statutory authority. Section 12 of the Act allows erasure when data is unnecessary, when consent has been withdrawn, or when processing violates the law. The Act grants the Data Protection Board power to weigh privacy claims against the public interest in access to information, echoing proportionality analysis used in other jurisdictions.

Indian courts have issued divergent rulings. In *Sri Vasunathan v. Registrar General* (2017), the Karnataka High Court ordered a petitioner's name removed from online records to prevent reputational damage. In *Dharamraj Bhanushankar Dave v. State of Gujarat* (2015), the Gujarat High Court refused a similar request, holding that judicial decisions form part of the public record. A review by the Internet Freedom Foundation in 2023 identified more than fifty RTBF-related petitions since 2017, with courts granting relief in a majority of sensitive cases while emphasizing the need to balance privacy against open justice.

RTBF faces structural challenges that go beyond doctrine. The durability of online data makes complete erasure difficult. Google's index surpassed 130 trillion pages by 2024, and archival services like the Internet Archive's Wayback Machine had stored over 866 billion captures by 2025. Distributed storage systems, cloud backups, and blockchain's immutability compound the problem. In India, the question of how to address the lingering stigma of acquittals remains underexplored. Courts have not yet fully confronted the tension between RTBF claims and the press's role in documenting judicial proceedings, leaving a gap in both jurisprudence and scholarship.

RESEARCH METHODOLOGY

Methods of inductive reasoning, deductive reasoning, and comparative analysis were employed to address the research questions. The research began with an inductive approach by analyzing specific landmark judicial rulings related to the Right to Be Forgotten in India. The cases provided critical insights into how Indian courts have interpreted privacy rights and RTBF. From the cases, broader patterns of judicial reasoning were identified, particularly concerning privacy, dignity, and the balance between the right to be forgotten and the public's right to information. Inductive reasoning enabled the researcher to observe how the cases shaped the understanding of RTBF within the Indian context. After identifying trends and principles from individual cases, deductive reasoning was applied to test these conclusions against established legal principles, including those found in international frameworks such as the General Data

Protection Regulation (GDPR) of the European Union. These comparisons allowed an upstart research path to determine whether the reported reasoning of the Indian courts aligned with the international context as discussed in the GDPR. This facilitated the

validation of the conclusions drawn from Indian cases and positioned India's legal approach within a global context. A detailed comparative analysis was also conducted to assess how RTBF is handled in India compared to other jurisdictions, such as the European Union and the United States. legal framework for RTBF, highlighting areas where reforms are necessary.

DATA COLLECTION

The research was based on secondary data containing multiple judicial decisions, scholarly articles, and legislative documents. Key judicial decisions were sourced from reputable legal databases such as SCC Online, LexisNexis, and Manupatra, with search queries like "Right to Be Forgotten" and "privacy rights". The legal provisions were taken from Digital Personal Data Protection Bill,2023. Additionally various journals and articles were referred to get a thorough understanding of the topic.

SAMPLE AND SAMPLING METHOD

The sample for this research was purposive and based on specific criteria, focusing on judicial rulings that significantly impacted the development of RTBF in India. The following factors guided the selection of cases:

- Only cases that directly dealt with privacy rights, data protection, or the right to be forgotten were considered.
- Cases that set important precedents in the Indian legal system were included, ensuring the analysis was grounded in well-established rulings.
- The sample also covered various issues, such as sexual privacy, criminal records, and public records, to help establish how the RTBF is used across different situations and settings.

The final set of cases include:

- Kharak Singh vs State of Uttar Pradesh (1964)[15]
- R. Rajagopal vs State of Tamil Nadu (1994)[16]
- Mr X vs Hospital Z (1998)[17]

[15] Kharak Singh v. State of U.P., (1964) 1 SCR 332 (India)
[16] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (India).
[17] Mr. 'X' v. Hospital 'Z', (1998) 8 SCC 296 (India).

- State of Punjab vs Gurmit Singh (1996)[18]
- State of Karnataka vs Puttaraja (2004)[19]
- K.S. Puttaswamy vs Union of India (2017)
- Dharamraj Bhanushankar Dave vs State of Gujarat & Others (2015)
- Sri Vasunathan vs The Registrar General (2017)
- Customs vs Jorawar Singh Mundy (2021)
- Zulfiqar Ahman Khan vs M/S Quintillion Business Media Pvt. Ltd. (2019)[20]
- Subhranshu Rout vs State of Odisha (2020)

CASE ANALYSIS

Kharak Singh v. State of U.P.

Kharak Singh is one of the first cases in which the Supreme Court of India confronted the question of privacy after independence. It set an uneasy foundation for the connection between personal liberty and privacy, a link that would later shape the understanding of the Right to Be Forgotten (RTBF). Kharak Singh, a resident of Uttar Pradesh with past allegations of involvement in dacoity cases but no convictions, was placed under police surveillance under Regulation 236 of the Uttar Pradesh Police Regulations. The measures included "history-sheeting," night-time visits to his home, secret watch over his movements, and routine inquiries about his activities. Singh argued that these practices violated his fundamental rights under Articles 19(1)(d) and 21 of the Constitution. He maintained that constant monitoring without justification intruded on his private life and eroded his dignity and freedom.

In a split decision delivered in December 1963, the Court struck down the provision authorizing domiciliary visits at night. The majority held that entering a person's home in this manner violated Article 21 because it amounted to an unjustified intrusion into personal liberty. However, the bench stopped short of recognizing a wider right to privacy. The judges defined "personal liberty" narrowly, limiting it to freedom from physical restraint and rejecting the idea that the Constitution guaranteed protection for private life. They wrote that the "right of privacy is not a guaranteed right under our Constitution," signalling that

[18] State of Punjab v. Gurmit Singh, (1996) 2 SCC 384 (India).
[19] State of Karnataka v. Puttaraja, (2004) 1 SCC 475 (India).
[20] Zulfiqar Ahman Khan v. Quintillion Bus. Media Pvt. Ltd., 2019 SCC OnLine Del 8494 (India).

surveillance of movements alone did not violate a fundamental right.

Justice Subba Rao dissented, taking a broader view. He argued that personal liberty necessarily includes the right to be free from unwarranted interference in one's private life. In his words, "the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life." Drawing on the Universal Declaration of Human Rights, he emphasized that surveillance without cause undermines human dignity and autonomy. Although Rao's opinion did not command the majority, it became the foundation for later developments in privacy law. Its relevance to RTBF lies in its recognition that sustained surveillance and record-keeping can harm individuals long after any legitimate need has passed, a concern mirrored in today's debates over digital permanence. More than fifty years later, in K.S. Puttaswamy v. Union of India (2017), the Supreme Court explicitly adopted Rao's reasoning, declaring privacy to be a fundamental right under Article 21 and including informational privacy as part of that protection. This shift opened the door for RTBF claims where individuals seek removal of outdated or irrelevant personal data to safeguard dignity.

Kharak Singh is often seen as a missed opportunity: the Court's reluctance to recognize privacy delayed stronger constitutional protection. Yet the dissent ensured that the conversation continued, and its language now underpins modern decisions on data protection and the control of personal information. The case also reflects the post-colonial tension between state security concerns and individual rights, a balance that continues to shape RTBF debates where privacy claims are weighed against public interest in retaining information.

***R. Rajagopal v. State of Tamil Nadu* (1994)**

Commonly known as the Auto Shankar case, this decision marked a turning point in the recognition of privacy under the Indian Constitution and set boundaries that continue to shape the Right to Be Forgotten (RTBF). The dispute arose when Gopalkrishna Naidu, known as Auto Shankar, a convicted serial killer on death row, wrote an autobiography describing his crimes and alleging collusion by police and prison officials. Journalists R. Rajagopal and the magazine Nakkheeran planned to publish the manuscript. The Tamil Nadu government attempted to block publication, claiming it defamed officials and violated privacy. The petitioners challenged the restraint under Articles 19(1)(a) and 21, arguing that prior censorship was unconstitutional. In its judgment of October 7, 1994, the Supreme Court held that the right to privacy is inherent in Article 21's guarantee of life and personal liberty. Justice B.P. Jeevan Reddy, writing for the bench, described privacy as "a right to

be let alone" and extended it to cover personal matters such as family, marriage, and childbearing. At the same time, the Court drew a clear line: once information becomes part of the public record, privacy protection falls away, and the material becomes open to comment and publication. The Court reasoned that official and judicial records serve a public function and cannot be shielded from scrutiny on privacy grounds.

This distinction has lasting consequences for RTBF. It creates a presumption of openness for public records, making it difficult for individuals to seek deletion of court documents or official files even if they have lost relevance or continue to harm reputation. The Court balanced this position against free speech rights and emphasized that unauthorized publication of private facts can still be challenged unless justified by public interest. The judgment borrowed from comparative jurisprudence, including U.S. cases such as New York Times v. Sullivan, in outlining limits on prior restraint. The ruling illustrates a structural tension in RTBF claims: individuals may control purely private information, but information preserved as part of the public record is resistant to erasure. In the digital era, where online archives preserve material indefinitely, this line has become even more significant. Critics argue that the Court could not have anticipated the harm caused by the persistence of digital records, especially for acquitted individuals or those involved in resolved disputes. Nonetheless, the case provided the doctrinal base on which later privacy jurisprudence, including K.S. Puttaswamy v. Union of India (2017), was built. Rajagopal remains central to RTBF discussions because it frames the conflict between dignity and transparency and underscores the need to balance erasure with public interest.

***Mr. X v. Hospital Z* (1998)**

This case addressed the scope of medical confidentiality and privacy, and though decided before RTBF entered Indian law, it foreshadows how sensitive personal information might qualify for erasure once it loses relevance. The petitioner, referred to as Mr. X, learned he was HIV-positive during a routine blood donation at Hospital Z. Without his consent, hospital staff disclosed his status to his fiancée's family, which led to the cancellation of their marriage and widespread social stigma. Mr. X sued the hospital, claiming breach of confidentiality and violation of his right to privacy under Article 21. The hospital defended its actions as necessary to protect the fiancée's health. In its judgment of September 21, 1998, the Supreme Court accepted the disclosure as justified but affirmed that privacy is a protected interest under Article 21, albeit not absolute. The Court stated that individuals with HIV have a right to keep their status confidential but that this right can yield when disclosure is necessary to prevent harm to others. Relying on medical ethics and

comparative standards, the bench emphasized that any breach of confidentiality must be narrowly tailored and grounded in a compelling need.

Although the Court sided with the hospital, it acknowledged the profound personal consequences of exposing intimate medical information. It observed that disclosure of true private facts can destabilize a person's life and cause deep psychological harm. This recognition ties closely to RTBF debates: once the immediate public health concern has passed, the continued availability of such sensitive information can become disproportionate and justify erasure to restore dignity.

The case builds on the principles set out in Rajagopal (1994), reinforcing privacy as part of Article 21, and anticipates the informational privacy framework that the Court later formalized in Puttaswamy (2017). In the context of digital archives, Mr. X v. Hospital Z highlights the argument for time-bound limits on sensitive data and reflects the balance RTBF tries to achieve between individual autonomy and legitimate public interest.

***State of Punjab v. Gurmit Singh* (1996)**

This case remains one of the most important Supreme Court rulings on the protection of rape victims' identities and the treatment of sensitive information in criminal proceedings. It also laid a foundation for later arguments linking privacy to the Right to Be Forgotten (RTBF). The matter arose from the 1990 abduction and rape of a minor in Punjab. The trial court convicted the accused, but in 1994 the Punjab and Haryana High Court acquitted them, citing inconsistencies in the testimony and casting doubt on the survivor's character. The State appealed, arguing that the high court's reasoning had effectively subjected the victim to a second round of public humiliation.

On January 16, 1996, a two-judge bench of the Supreme Court, comprising Justices S. Saghir Ahmad and Kuldip Singh, reversed the acquittal and restored the convictions under Sections 363, 366, 368, and 376 of the Indian Penal Code. Beyond the verdict itself, the Court issued strong directions on the handling of sexual offence cases. It ordered in-camera proceedings under Section 327 of the Criminal Procedure Code and stressed that the identity of victims must not be disclosed, invoking Section 228A of the IPC. The Court noted that disclosing a victim's name or details serves no public interest and only compounds the harm. It observed that many survivors describe testifying as a "second assault" when they are exposed to public scrutiny and harsh questioning in court. The judgment also addressed evidentiary standards, holding that the testimony of a rape victim requires no corroboration unless compelling reasons exist to doubt it. The bench emphasized that cross-examination should avoid unnecessary

intrusion into the survivor's private life, and that dignity must remain at the center of the trial process. It stated that courts have a duty to ensure victims are not subjected to embarrassment or humiliation in proceedings, recognizing that the justice system itself can cause lasting damage if handled insensitively.

Although the case predates the language of the RTBF, its reasoning aligns with its core principles. The insistence on anonymity and the recognition of lasting stigma from public exposure mirror arguments for erasing or anonymizing case details once proceedings conclude, particularly in the context of digital records. In later years, Gurmit Singh has been cited in petitions seeking removal of names and identifying details from online judgments to prevent continued harm long after cases are resolved. The ruling also reflects a broader shift in Indian jurisprudence towards protecting dignity as part of personal liberty. It built on early privacy discussions and anticipated the emphasis on autonomy and informational control that the Supreme Court would later endorse in K.S. Puttaswamy v. Union of India (2017). While initially framed in the context of sexual offence trials, the Court's insistence on limiting the circulation of sensitive personal information has informed debates about data permanence and the RTBF in the digital age.

State of Karnataka vs Puttaraja (2004)

This Supreme Court decision arose from the sentencing of a man convicted of raping a minor in Karnataka and reinforced the protection of victim identity in sexual offence cases. Although focused on punishment, the case contributed to the privacy framework that later supported the Right to Be Forgotten (RTBF). Puttaraja was convicted by the trial court and sentenced to ten years' imprisonment. In 2001, the Karnataka High Court reduced the sentence to five years, citing mitigating factors such as his personal circumstances. The State appealed, arguing that the reduction failed to reflect the seriousness of the crime. On January 9, 2004, a two-judge bench of Justices Doraiswamy Raju and Arijit Pasayat reinstated the ten-year sentence. The Court described rape as "not only a crime against the person of a woman, it is a crime against the entire society," noting its profound and lasting impact on survivors. It cautioned against leniency, observing that undue sympathy leading to inadequate punishment undermines public confidence in the justice system.

The judgment placed particular emphasis on protecting the dignity of victims. Citing Section 228A of the Indian Penal Code, the Court directed that the identity of sexual assault survivors must not be disclosed, even in judicial opinions. It stressed that maintaining

anonymity is essential to safeguard the victim's honour and prevent further harm beyond the trial itself.

Although the case did not address digital records, its reasoning parallels RTBF principles. It recognised that exposing identifying details serves no public interest and prolongs the harm experienced by victims, particularly once proceedings have concluded. In the context of online archives, this aligns with the argument for redacting or anonymizing judgments to prevent indefinite circulation of sensitive information. The Court also discussed factors relevant to sentencing, including the victim's age, and made clear that punishment should not depend on the social status of either the survivor or the accused, but on the gravity of the offence and the harm inflicted. This victim-centred approach builds on the principles set in State of Punjab v. Gurmit Singh (1996) and underscores the importance of dignity and privacy as part of fair justice.

***K.S. Puttaswamy v. Union of India* (2017)**

Widely known as the Privacy Judgment, this case marked a turning point in Indian constitutional law. The Supreme Court unanimously recognised privacy as a fundamental right, creating the constitutional foundation for the Right to Be Forgotten (RTBF) by explicitly protecting informational privacy in the digital era. The case arose from challenges to the Aadhaar scheme, the government's biometric identification program designed for distributing welfare benefits and services. In 2012, retired Karnataka High Court judge K.S. Puttaswamy filed a petition arguing that mandatory collection of biometric data without sufficient safeguards violated the right to privacy and opened the door to surveillance and misuse of personal information. The matter was referred to a nine-judge bench to resolve whether privacy was protected under the Constitution.

On 24 August 2017, the Supreme Court delivered a unanimous judgment overruling earlier decisions such as M.P. Sharma (1954) and Kharak Singh (1963), which had denied privacy the status of a fundamental right. The bench held that privacy is inherent in Article 21's protection of life and personal liberty and also forms part of the broader guarantees under Part III of the Constitution. Justice D.Y. Chandrachud, writing the lead opinion, described privacy as "the constitutional core of human dignity" and emphasised informational privacy as the individual's ability to control personal data and its dissemination. The judgment defined privacy broadly, covering decisional autonomy, bodily integrity, and control over personal information, and adopted a proportionality test to assess state actions that interfere with it. Justice S.K. Kaul's concurring opinion explicitly referred to the challenges of the digital age, noting that

information placed online can become permanent and that individuals should have the ability to exercise control over it, including "the right to forget." This acknowledgment linked the judgment directly to RTBF principles, recognising that outdated or irrelevant personal data can undermine dignity and autonomy. The decision laid the groundwork for courts to order erasure when information ceases to serve a legitimate public interest. It also influenced the framing of the Digital Personal Data Protection Act of 2023, which provided statutory support for RTBF claims. While the judgment left the precise contours of implementation to future legislation, it shifted privacy from a limited judicial inference to a constitutional guarantee and firmly placed informational privacy at its centre.

Puttaswamy remains one of the most significant cases in India's constitutional history. Its emphasis on dignity, autonomy, and control over personal data provides the legal basis for balancing individual rights with state and societal interests in an age defined by mass data collection and digital permanence.

***Dharamraj Bhanushankar Dave v. State of Gujarat* (2015)**

This Gujarat High Court case exposed the tension between an individual's privacy interests and the permanence of judicial records in the digital age. It highlighted the difficulty of applying the Right to Be Forgotten (RTBF) when acquitted individuals continue to face reputational harm because judgments remain accessible online. Dharamraj Bhanushankar Dave was acquitted in 2007 of charges under Sections 302, 364, 120B, 201, 404, and 34 of the Indian Penal Code. After the judgment was uploaded to online platforms, including Indian Kanoon and indexed by search engines, Dave argued that the continued availability of the record damaged his personal and professional reputation despite his exoneration. He filed a petition seeking removal of the judgment from public access, invoking Article 21 and framing the issue as one of dignity and privacy in the face of digital permanence.

On 19 January 2017, Justice R.M. Chhaya dismissed the petition. The Court held that judgments of the High Court are public records by nature and cannot be removed simply because they cause discomfort or reputational harm. It emphasised that the High Court, as a court of record, has a duty to preserve judgments for public access and accountability. The Court also clarified that marking a judgment as "non-reportable" relates to publication in law reports and does not prevent online availability. The ruling underscored the lack of statutory basis for RTBF at the time and highlighted the judiciary's prioritisation of transparency over erasure. The Court noted that without legislative backing or proof of error or malice, Article

21 could not be used to remove accurate judicial records. The case became a reference point in later debates on RTBF, illustrating the unresolved conflict between archival permanency and individual rehabilitation. Critics argue that while the decision protected openness, it undervalued the long-term dignity interests of acquitted persons in the digital environment.

***Sri Vasunathan v. Registrar General* (2017)**

In this Karnataka High Court decision, the judiciary expressly acknowledged the Right to Be Forgotten in India for the first time. The case involved a petition by Sri Vasunathan on behalf of his daughter, whose name appeared in digitised judgments from a resolved marital annulment case and related criminal proceedings against her former husband. Although the matter had been settled, the continued online presence of the records was said to be harming her reputation and affecting her new marriage. On 23 January 2017, Justice Anand Byrareddy granted relief and directed the removal of her name from public search results and cause titles. The order instructed the court registry to ensure that internet searches did not display the petitioner's daughter's name in connection with the case, while allowing her name to remain in certified copies and internal court records. The Court explicitly referenced the emerging "right to be forgotten" in other jurisdictions and applied the principle to protect dignity in a sensitive personal matter.

The judgment placed emphasis on proportionality, noting that the continued public availability of the information served no ongoing public interest but caused demonstrable harm. It marked the first judicial step in India toward recognising RTBF, particularly in cases involving intimate personal details. Although the order focused on a woman's privacy and reputation, it set a broader precedent for anonymisation of digital records when perpetual access imposes lasting harm without benefit to public accountability. The case has since influenced other RTBF petitions and underscored the need for a structured legal framework balancing openness with individual dignity.

***Jorawar Singh Mundy v. Union of India* (2021)**

This Delhi High Court decision marked an important step in the development of the Right to Be Forgotten (RTBF) in India by recognising the reputational harm faced by acquitted individuals when judgments remain permanently available online. Jorawar Singh Mundy, a U.S. citizen, had been acquitted under the Narcotic Drugs and Psychotropic Substances Act in 2013. Despite his exoneration, the judgment from *Customs v. Jorawar Singh Mundy* (Crl.A. 14/2013) remained accessible on platforms such as Indian Kanoon and appeared prominently

in search engine results. Mundy argued that the continued online presence of the judgment was damaging his career prospects in the United States, particularly during background checks for employment. He filed a petition under Article 226 seeking to delist or restrict access to the decision. On 12 April 2021, Justice Prathiba M. Singh granted interim relief. The Court directed Indian Kanoon to block access to the judgment from search engines pending further orders and acknowledged the risk of "irreparable prejudice" to the petitioner's reputation and professional life. Citing *K.S. Puttaswamy v. Union of India* (2017), the Court observed that the right to privacy included protecting individuals from lasting harm caused by the indefinite availability of sensitive personal information once its public relevance had diminished. While the order was limited to interim relief and did not decide the larger question of RTBF for public judicial records, it reflected a shift towards balancing transparency with post-acquittal dignity. The case underscored the judiciary's growing willingness to engage with RTBF principles where digital permanence threatens rehabilitation and social reintegration, especially in an era where online records shape personal and professional opportunities.

Zulfiqar Ahman Khan vs M/S Quintillion Business Media Pvt. Ltd. (2019)

Similarly, the case of Zulfiqar Ahman Khan vs M/S Quintillion Business Media Pvt. Ltd. (2019) addresses RTBF in protecting privacy and reputation. Zulfiqar Ahman Khan, a media professional, filed a petition to remove defamatory articles from the news website The Quint that had been published against him, arguing that these articles damaged his reputation and caused significant harm to his personal and professional life. Khan sought the application of the RTBF, asking that these articles be removed from online platforms to protect his privacy and reputation. The Delhi High Court, while recognizing the RTBF, granted interim relief by directing the removal of the articles in question from The Quint's website, acknowledging that they had the potential to cause irreparable harm to Khan's dignity. This case is a landmark in the development of the RTBF in India, as it underscored the growing judicial recognition of individuals' rights to control harmful or outdated information about them that continues to exist in the public domain, even when it no longer serves any public interest. The Court's order was grounded in the fundamental Right to privacy. The Zulfiqar Khan case highlights the tension between the RTBF and freedom of speech, as it involved the removal of published content, raising concerns about censorship and the suppression of journalistic expression. However, the Court found that the balance tilted in favour of protecting individual privacy and reputation, particularly given the

defamatory nature of the content.

Subhranshu Rout vs State of Odisha (2020)

The case of Subhranshu Rout vs State of Odisha (2020) extends the discussion of the RTBF, particularly regarding the misuse of personal information on social media platforms. The petitioner, Subhranshu Rout, was accused of committing sexual assault and subsequently uploading intimate photographs of the victim on a fake Facebook account to blackmail and intimidate her. The Court recognised the severity of the crime. It highlighted the challenges victims face in such cases, particularly the difficulty in permanently removing objectionable content from social media platforms once uploaded. In its analysis, the Orissa High Court emphasised that while the Indian legal system provides solid penal actions against offenders for such crimes, a lack of statutory mechanisms allows victims to enforce the deletion of objectionable content from digital platforms. The Court noted the absence of a comprehensive legal framework in India for implementing the RTBF, particularly in cases where sensitive personal data continues to exist in the public domain despite the victim's desire to have it erased. This case highlighted the practical difficulties in enforcing the RTBF in India, mainly when dealing with tech companies like Facebook, which control the servers where such content is stored. The Court referred to the General Data Protection Regulation (GDPR) in the European Union, which grants individuals the Right to request the removal of personal data under specific circumstances. The Court highlighted the urgent need for India to adopt similar legislative measures to protect victims' privacy, especially in cases involving sensitive content like sexual assault.

INTERPRETATION AND FINDINGS

The findings regarding the Right to Be Forgotten (RTBF) in India reveal several critical gaps in its application, especially in cases relating to sexual privacy and criminal records. Despite recognizing privacy as a fundamental right, the RTBF still needs to be developed regarding legal implementation and societal understanding.

When it comes to cases involving victims of sexual offences, such as State of Punjab vs Gurmit Singh and Sri Vasunathan vs Registrar General, the Indian judiciary has shown its readiness to protect the identity of the victims under the RTBF. Such cases are aware of the nature of sexual crimes and the stigma that takes ages to wash off when personal information remains available online. However, no standardised legal protection is available to victims since there is no nationwide statutory code exclusively addressing sexual privacy concerns. This creates a convoluted situation where some victims are granted protection. In

contrast, others continue to face public ridicule and stigmatisation due to inconsistent case law and the lack of clear and coherent legislative guidelines. For individuals with criminal records, the RTBF seeks to allow them to reform by erasing their past misdeeds. Judicial decisions such as Dharamraj Bhanushankar Dave vs State of Gujarat and Jorawar Singh Mundy vs Union of India highlight people's difficulties in escaping their digital footprint. Despite being cleared or having charges long behind them, they continue to suffer, as these records negatively impact their job prospects and social reputation. There is still much uncertainty regarding the applicability of the RTBF—while Jorawar Singh Mundy received temporary relief, the case demonstrates that courts have not been consistent in their decisions. This comparison raises the question of a conflict between public interest, the right to information, and personal privacy. To address the issue of outdated criminal records being publicly accessible, individuals can pursue two primary legal avenues. First, they may request a court injunction directing the delisting of these records from search engine results, thereby limiting public visibility. Alternatively, they can petition to have the records sealed in government databases, such as those maintained by the National Crime Records Bureau (NCRB) and judicial databases. These steps allow individuals, particularly those who have been acquitted or completed their sentences, to protect their reputation and privacy while balancing the public interest in criminal transparency. The continuous legal battle in cases like X vs UOI and Laksh Vir Singh Yadav vs UOI also proves that India still needs to embark on the right path of implementing RTBF in its legal system. Among these are the issues of consent, data sharing, data portability, automated decisions, and representative actions, which the proposed Digital Personal Data Protection Bill attempts to address. However, the provisions are insufficient to guarantee efficient and consistent nationwide implementation. Most notably, the Bill shifts more of the burden to the Data Protection Authority to decide on RTBF claims while leaving the definition of ‘public interest’ somewhat ambiguous. There has also been conflict in applying RTBF in India when dealing with privacy versus the Right to Freedom of Speech and Expression (Article 19) and the Right to Information (RTI).

PERSONAL OPINION

The existing RTBF framework currently being implemented in India does not provide adequate provisions to address the dynamics of the modern world. This creates confusion for the courts, as there is no authoritative law governing privacy, putting those who wish to exercise their right to privacy in a very volatile situation. Furthermore, the lack of clear

standards concerning protecting public interest against personal privacy further leads to the continued use of victims' data and people's criminal history. India's future privacy laws must address these deficits while ensuring that the RTBF is acknowledged as a right and comprehensively practiced to protect against the ongoing digital stripping of individuals' identities. The RTBF in India must be strengthened significantly, particularly for survivors of sexual privacy violations and people with criminal records. Indeed, the most critical and pressing area for development is the need to provide a clear legal basis for the RTBF. Currently, no specific rules and regulations under the law define how one can demand that platforms erase their harmful or unnecessary data. By amending existing laws, such as the Information Technology Act 2000, or incorporating RTBF provisions into the upcoming Digital Personal Data Protection Bill, India can provide clear, actionable pathways for individuals, particularly victims of sexual violence, to reclaim control over their personal information. These amendments should also include rapid content removal mechanisms to ensure that intimate content shared without consent is taken down quickly and efficiently, protecting victims from further harm. These amendments should also include simple procedures for removing vulnerable content, particularly intimate material shared without the victim's consent, to avoid inflicting additional pain. The RTBF can also significantly assist people with criminal records, especially those who have been acquitted or served their sentences. However, the current legal framework does not sufficiently account for the consequences that digital permanence poses for these individuals in the long term. To strengthen privacy measures, the RTBF should provide for the erasure of criminal records that are no longer in the public interest. At the same time, legal reforms must consider the public's need for access to serious offenders' records or recidivists when necessary. Beyond legal changes, technological measures are crucial for making RTBF more efficient. Online firms, such as search engines and social media platforms, should be required to set up programmatic systems to monitor and delete data when an individual exercises their RTBF. These platforms must also ensure that deleted information does not re-emerge.

Additionally, consent-based data processing and sharing frameworks should be implemented, allowing individuals to withdraw consent to retain their data. This should trigger self-erase requests across all databases where the data is stored. Other legal reforms should address the conflict between RTBF and the public's right to know. Judicial systems should be able to redact personal identifiers in certain circumstances, such as when

disclosing a person's identity may cause reputational damage or violate their privacy. This approach, discussed in some legal cases, should be elaborated on with modifications to the Indian Evidence Act and the development of proper procedures for handling court records.

Additionally, awareness campaigns should inform vulnerable groups, such as survivors of sexual violence and those with criminal records, about their privacy rights and the protection available to them. Finally, a robust Data Protection Authority (DPA) must be developed to support the scope of RTBF. The DPA should ensure that requests are processed according to RTBF, and it should also have the power to investigate compliance by online platforms, acting as a mediator between the data subject and the data controller in case of disputes.

Furthermore, the DPA should oversee an open appeal procedure, allowing individuals to contest the non-acceptance of RTBF requests. Performing routine checks on platform compliance with RTBF requests will be necessary to ensure accountability and balance between privacy and the public interest.

LIMITATIONS AND DISCRETION FOR FUTURE RESEARCH

The first and most significant source of bias in this project is that it seeks to analyze secondary data. The research is based on legal precedents, scholarly articles, and legal regulations, which, although they provide valuable insights, do not encompass the entire picture regarding the RTBF in India. The absence of primary data collection, such as interviews with legal scholars, practitioners, or individuals who have experienced privacy violations or have criminal records, limits the depth of understanding from an individual and pragmatic perspective. Without interviews or surveys that offer firsthand experiences on how the RTBF is being applied or viewed by those directly affected, the research provides only a more generalized view of the law's impact. The study's focus on case-based analysis makes it difficult to generalize the outcomes. Implementing RTBF in India has been somewhat inconsistent, as court interpretations vary significantly depending on the case circumstances, the judge's discretion, and public interest considerations. Therefore, the findings may not be easily generalized to every privacy violation case, criminal history, or background check. The study focuses on a few landmark cases, meaning the application of RTBF may differ in other legal contexts or jurisdictions within India. This limitation calls for more research that can integrate quantitative data involving people's opinions and perceptions of the RTBF, which would provide a broader picture of the situation in India.

Moreover, the study relies heavily on high-profile cases, which might obscure how RTBF operates in less publicized instances. Individuals from less privileged backgrounds or those whose cases do not attract media attention may face different experiences, making it challenging to assess the coherence and accessibility of RTBF protections for everyone,

particularly vulnerable groups. This makes it cumbersome to appraise the availability and efficacy of RTBF protections, especially for those in vulnerable categories. Several directions for future research could provide a better understanding of the implementation and effectiveness of RTBF in India. One notable gap is the lack of quantitative research that captures the experiences of individuals whose privacy has been violated or examines the overall impact of the RTBF. Interviewing victims of sexual privacy violations, those with criminal records, and legal professionals could offer firsthand insights into the strengths and weaknesses of the current legal framework. Such empirical studies could also explore how individuals manage RTBF requests and the difficulties they face in attempting to remove their information from the internet. Another significant direction for future research involves developing technological infrastructures that appropriately implement RTBF. As the volume of online content grows exponentially, manual enforcement of RTBF may become impractical. Future research could focus on creating software systems designed to monitor, identify, and eliminate individuals' data across the internet. These systems should be equipped with robust protocols to protect privacy rights while safeguarding freedom of information, ensuring that data erasure is done correctly without unduly limiting public access to information.

Furthermore, additional research should explore the relationship between RTBF, media ethics, and press freedom. The tension between privacy rights and freedom of speech remains a crucial challenge. Research into how media companies handle RTBF requests and the potential impact on journalism could help establish best practices, allowing the press to exercise its freedom responsibly while respecting individuals' privacy.

CONCLUSION

The Indian jurisprudence on the Right to Be Forgotten reflects a constitutional dialogue between privacy, dignity, and the imperatives of transparency in a digital society. Emerging from the foundational recognition of privacy as a fundamental right in *K.S. Puttaswamy v. Union of India*, RTBF has developed incrementally through case law rather than comprehensive statutory articulation. Decisions such as *State of Punjab v. Gurmit Singh*, *Sri Vasunathan v. Registrar General*, and *Jorawar Singh Mundy v. Union of India* demonstrate the judiciary's willingness to shield sensitive personal information where continued public access serves no legitimate societal interest and imposes disproportionate harm. Conversely, rulings such as *Dharamraj Bhanushankar Dave v. State of Gujarat* underscore

the judiciary's enduring commitment to the public character of judicial records, revealing the doctrinal tension between rehabilitation and archival permanence.

The Digital Personal Data Protection Act of 2023 introduces a nascent statutory framework, yet its reliance on undefined "public interest" standards and discretionary adjudication risks perpetuating the inconsistency already evident in judicial approaches. Without a principled and uniform proportionality framework, RTBF remains a contingent remedy rather than a robust right. The persistence of digital archives, combined with the asymmetries of access to legal recourse, threatens to render RTBF protection uneven, particularly for those most vulnerable to reputational harm.

For RTBF to mature into a meaningful constitutional entitlement, India must move beyond case-specific relief and establish clear procedural and substantive standards grounded in proportionality, necessity, and temporal limitation. Such a framework must reconcile the individual's claim to autonomy and dignity with the democratic value of an open judicial record. If effectively implemented, RTBF has the potential to become one of the most significant doctrinal evolutions in Indian privacy law since *Puttaswamy*, providing a measured mechanism to balance the competing demands of memory and erasure in an era defined by the permanence of digital information.