The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

ERASING THE DIGITAL SHADOW: THE RIGHT TO BE FORGOTTEN IN INDIA

~ Arun Kumar S

ABSTRACT:

"WHEN THE INTERNET NEVER FORGETS"

The rapid growth of digital technology has fundamentally altered the manner in which personal information is stored, shared, and accessed. In the modern digital era, individuals leave behind permanent online traces through social media platforms, search engines, online databases, and digital communication networks. Unlike traditional forms of information that gradually disappear with time, digital data often remains accessible indefinitely, thereby affecting an individual's dignity, reputation, employment opportunities, and psychological well-being. This permanence of online information has intensified concerns regarding privacy and informational autonomy, leading to the emergence of the Right to Be Forgotten (RTBF).

The Right to Be Forgotten refers to the right of individuals to request the removal, deletion, or de-indexing of personal information from digital platforms when such information becomes outdated, irrelevant, excessive, or harmful. The concept gained international recognition after the landmark judgment in Google Spain SL v. Agencia Española de Protección de Datos (AEPD), where the Court of Justice of the European Union acknowledged the right of individuals to seek removal of certain online search results. In India, although RTBF has not been expressly codified, the Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India recognized privacy as a fundamental right under Article 21 and laid the constitutional foundation for informational privacy.

This paper critically examines the constitutional dimensions, judicial developments, and legal challenges associated with RTBF in India. It further analyzes the tension between privacy and

competing principles such as freedom of speech, judicial transparency, and public interest, while emphasizing the need for a balanced and comprehensive legal framework.

Keywords: Right to Be Forgotten, Digital Privacy, Article 21, Informational Privacy, GDPR, Online Reputation, Data Protection, Freedom of Speech.

INTRODUCTION:

The digital revolution has transformed the modern world into an interconnected information society where data is continuously created, stored, and circulated across online platforms. Every social media post, online transaction, photograph, search history, and digital interaction contributes to an individual's permanent digital footprint. Unlike traditional forms of communication that gradually fade from public memory, information available on the internet often remains permanently accessible and searchable. This permanence has created significant concerns relating to privacy, dignity, reputation, and informational autonomy in the digital age.

The rapid expansion of social media platforms and search engines has intensified the problem of digital permanence. Information uploaded years earlier may continue to affect individuals long after its relevance has disappeared. In many cases, personal photographs, criminal accusations, acquittal records, matrimonial disputes, or embarrassing online content remain publicly available indefinitely, thereby affecting employment opportunities, social relationships, and psychological well-being. The internet's inability to forget has therefore generated an urgent need for legal mechanisms capable of protecting individuals from perpetual digital exposure.

In response to these concerns, the concept of the Right to Be Forgotten (RTBF) emerged as an important privacy-based principle. RTBF broadly refers to the right of individuals to request the removal, deletion, or de-indexing of personal information from digital platforms when such information becomes outdated, excessive, misleading, or no longer relevant.[1] The concept gained international prominence after the landmark decision of the Court of Justice of the European Union in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, where the Court recognized the right of individuals to seek removal of certain online search results containing personal information.[2]

In India, the Right to Be Forgotten has evolved primarily through constitutional interpretation and judicial recognition. Although the Constitution of India does not expressly recognize RTBF, the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy v. Union of India* fundamentally altered Indian privacy jurisprudence by recognizing privacy as a fundamental right under Article 21 of the Constitution. [3.] The Court observed that informational privacy forms an essential component of individual dignity and personal liberty. This recognition created a constitutional foundation for the gradual development of RTBF in India.Subsequently, several Indian High Courts acknowledged RTBF in cases involving acquittal records, sensitive personal disputes, and protection of identity. In *X v. Registrar General, High Court of Karnataka*, the Karnataka High Court emphasized the importance of protecting individuals from unnecessary disclosure of personal information available through online judgments. [4.] Similarly, the Delhi High Court in *Jorawar Singh Mundy v. Union of India* recognized that continued online publication of acquittal records could seriously prejudice an individual's reputation and future prospects. [5.] Despite these developments, India still lacks a comprehensive statutory framework specifically governing RTBF. While the Digital Personal Data Protection Act, 2023 provides certain protections concerning personal data processing and erasure, the scope and enforcement of RTBF remain uncertain. [6.]Moreover, RTBF raises complex constitutional questions involving freedom of speech, public interest, judicial transparency, and press freedom. Excessive recognition of RTBF may potentially lead to suppression of legitimate public information and historical records. This paper critically examines the emergence and development of the Right to Be Forgotten in India within the broader framework of constitutional privacy and digital governance. It analyzes the constitutional basis of RTBF, evaluates important judicial precedents, studies comparative international approaches, and explores the challenges associated with balancing informational privacy against competing democratic interests. The paper further argues that India requires a balanced and clearly defined legal framework capable of protecting digital dignity while preserving transparency and freedom of expression in a democratic society.

LITERATURE REVIEW:

Evolution of Privacy and the Emergence of RTBF

The concept of privacy has evolved significantly with technological advancement and digital communication. Initially, Indian constitutional jurisprudence did not expressly recognize privacy as a fundamental right. In *M.P. Sharma v. Satish Chandra*, the Supreme Court observed

that the Constitution did not specifically guarantee a right to privacy. [7.] Similarly, in *Kharak Singh v. State of Uttar Pradesh*, the majority refused to recognize privacy as an independent right, although Justice Subba Rao's dissent emphasized the importance of personal liberty and dignity.[8.] Over time, judicial interpretation expanded the scope of Article 21. In *Gobind v. State of Madhya Pradesh*, the Supreme Court acknowledged that privacy could be inferred from fundamental rights under Part III of the Constitution.[9.] This development culminated in *Justice K.S. Puttaswamy v. Union of India*, where privacy was unanimously recognized as a fundamental right. [10.] The Right to Be Forgotten (RTBF) emerged as a response to the permanent nature of digital memory. The concept enables individuals to seek removal or de-indexing of personal information that has become outdated, irrelevant, or harmful. RTBF gained international recognition after the decision in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, where the Court of Justice of the European Union held that individuals may request removal of certain online search results. [11.]

3.2 Global and Indian Academic Perspectives

Scholars have increasingly associated RTBF with informational privacy and human dignity. The European Union strengthened the principle through Article 17 of the General Data Protection Regulation (GDPR), which formally recognizes the "right to erasure."[12] However, legal scholars continue to debate the tension between privacy and freedom of expression. While some argue that RTBF protects individuals from perpetual social stigma, others contend that excessive recognition may undermine transparency and public access to information.[13.] In India, academic discussions largely focus on balancing RTBF with constitutional principles such as freedom of speech, judicial transparency, and public interest. Existing literature suggests that although Indian courts have gradually recognized informational privacy, India still lacks a comprehensive statutory framework governing RTBF. [14.]

UNDERSTANDING THE RIGHT TO BE FORGOTTEN

Meaning and Nature of the Right to Be Forgotten

The Right to Be Forgotten (RTBF) refers to the right of an individual to seek deletion, removal, or de-indexing of personal information from digital platforms when such information becomes outdated, irrelevant, misleading, or harmful. In the digital era, personal data shared online often remains permanently accessible through search engines, social media platforms, and online

archives. RTBF therefore seeks to restore individual control over personal information and protect informational privacy in cyberspace.

Unlike traditional privacy rights that focus on preventing unauthorized intrusion into personal life, RTBF specifically addresses the long-term consequences of digital permanence. The right recognizes that individuals should not be indefinitely judged for past actions, mistakes, or personal disputes that no longer possess public relevance. It is closely connected with the concepts of human dignity, reputation, autonomy, and the ability to reintegrate into society without continuous digital stigma.

The modern understanding of RTBF gained international recognition through the landmark decision in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, where the Court of Justice of the European Union held that individuals may request search engines to remove links containing personal information under certain circumstances. [15.] The judgment emphasized that privacy rights may outweigh public interest when the information becomes excessive or irrelevant over time.

RTBF and Informational Privacy in India

In India, RTBF has evolved primarily through constitutional interpretation and judicial recognition. The Supreme Court's judgment in *Justice K.S. Puttaswamy v. Union of India* recognized privacy as a fundamental right under Article 21 and highlighted the importance of informational self-determination. [16.]The Court observed that individuals must possess control over dissemination of personal information in the digital domain.

Indian courts have gradually applied RTBF principles in cases involving acquittal records, matrimonial disputes, and protection of identity. The Karnataka High Court in *X v. Registrar General, High Court of Karnataka* recognized the need to protect individuals from unnecessary disclosure of sensitive personal information available through online records. [17.]

However, RTBF is not an absolute right. Its implementation requires balancing privacy with competing constitutional values such as freedom of speech, judicial transparency, press freedom, and public interest. Consequently, courts often adopt a case-by-case approach while determining whether online information should remain publicly accessible.

THE DIGITAL FOOTPRINT CRISIS

Digital Permanence and Online Reputation

The growth of the internet and social media has created an environment where personal information remains permanently accessible. Photographs, videos, social media posts, online comments, news reports, and judicial records can be stored and reproduced indefinitely through digital platforms. Unlike traditional communication, digital content rarely disappears completely, thereby creating a permanent "digital footprint" capable of influencing an individual's identity and reputation for years. Search engines further intensify this problem by making personal information easily searchable and globally accessible. Even outdated or inaccurate information may continue to appear in search results long after its social relevance has ended. Consequently, individuals who were acquitted in criminal cases, involved in personal disputes, or victims of cyber harassment often continue to face reputational harm due to the continued availability of online records. [18.] The permanence of online information has also increased instances of cyberbullying, revenge pornography, identity misuse, and social stigma. In many situations, individuals lose control over their personal data once it enters digital space.

Social and Psychological Impact of Digital Memory

The continuous accessibility of harmful or embarrassing online content may seriously affect employment opportunities, educational prospects, and interpersonal relationships. Employers and educational institutions frequently rely upon online searches while evaluating candidates, making digital reputation an important aspect of modern social identity. The psychological consequences of digital permanence are equally significant. Constant exposure to past mistakes or traumatic experiences may lead to anxiety, emotional distress, and social isolation. Individuals are often denied the opportunity for rehabilitation because the internet preserves information without considering passage of time or changing circumstances. In this context, the Right to Be Forgotten has emerged as an important mechanism for protecting informational privacy and human dignity. By allowing individuals to seek removal or de-indexing of harmful and irrelevant information, RTBF attempts to balance technological advancement with the fundamental values of privacy. [19.] [1]

15. Jeffrey Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88 (2012).
16. Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ECLI:EU:C:2014:317 (2014).

THE DIGITAL FOOTPRINT CRISIS:

Digital Permanence and Online Reputation

The growth of the internet and social media has created an environment where personal information remains permanently accessible. Photographs, videos, social media posts, online comments, news reports, and judicial records can be stored and reproduced indefinitely through digital platforms. Unlike traditional communication, digital content rarely disappears completely, thereby creating a permanent "digital footprint" capable of influencing an individual's identity and reputation for years. Search engines further intensify this problem by making personal information easily searchable and globally accessible. Even outdated or inaccurate information may continue to appear in search results long after its social relevance has ended. Consequently, individuals who were acquitted in criminal cases, involved in personal disputes, or victims of cyber harassment often continue to face reputational harm due to the continued availability of online records. [20.]

Social and Psychological Impact of Digital Memory

The continuous accessibility of harmful or embarrassing online content may seriously affect employment opportunities, educational prospects, and interpersonal relationships. Employers and educational institutions frequently rely upon online searches while evaluating candidates, making digital reputation an important aspect of modern social identity. The psychological consequences of digital permanence are equally significant. Constant exposure to past mistakes or traumatic experiences may lead to anxiety, emotional distress, and social isolation. Individuals are often denied the opportunity for rehabilitation because the internet preserves information without considering passage of time or changing circumstances. In this context, the Right to Be Forgotten has emerged as an important mechanism for protecting informational privacy and human dignity. By allowing individuals to seek removal or de-indexing of harmful and irrelevant information, RTBF attempts to balance technological advancement with the fundamental values of privacy, autonomy, and social reintegration. [21.]

17. Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88 (2012).
18. *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI:EU:C:2014:317 (2014).

CONSTITUTIONAL AND LEGAL FRAMEWORK OF RTBF IN INDIA

Article 21 and the Evolution of Privacy Jurisprudence

The Constitution of India does not expressly recognize the Right to Be Forgotten (RTBF) as a fundamental right. Nevertheless, the constitutional basis for RTBF has gradually developed through judicial interpretation of Article 21, which guarantees the right to life and personal liberty. Over the years, the Supreme Court has interpreted Article 21 expansively to include various rights necessary for ensuring dignity, autonomy, and meaningful existence. Privacy emerged as one such essential component of personal liberty.

Initially, Indian constitutional jurisprudence adopted a restrictive approach toward privacy rights. In *M.P. Sharma v. Satish Chandra*, an eight-judge bench of the Supreme Court held that the Constitution did not specifically guarantee a right to privacy. [22.] The Court observed that unlike the American Constitution, the Indian Constitution lacked an explicit privacy provision. Similarly, in *Kharak Singh v. State of Uttar Pradesh*, the majority refused to recognize privacy as an independent constitutional right while examining police surveillance regulations. [23.] However, Justice Subba Rao's dissent became highly influential because it emphasized that unauthorized intrusion into an individual's private life violates personal liberty and human dignity.

Subsequent judicial decisions gradually expanded the scope of privacy protection under Article 21. In *Gobind v. State of Madhya Pradesh*, the Supreme Court acknowledged that privacy could be inferred from the freedoms guaranteed under Part III of the Constitution. [24.] The Court recognized that privacy encompasses personal autonomy and the ability of individuals to control aspects of their private lives. Although the Court stated that privacy is not absolute, the judgment marked an important transition in Indian constitutional jurisprudence.

Further expansion occurred in cases such as *R. Rajagopal v. State of Tamil Nadu*, where the Supreme Court recognized an individual's right to safeguard the privacy of personal matters against unauthorized publication. [25.] Similarly, in *People's Union for Civil Liberties v. Union of India*, the Court held that telephone tapping violates the right to privacy unless conducted according to established legal procedure. [26.] The constitutional recognition of privacy reached its most significant milestone in *Justice K.S. Puttaswamy v. Union of India*. [27.] In this landmark judgment, a nine-judge bench unanimously declared privacy to be a fundamental right protected under Article 21 and other freedoms guaranteed by Part III of the Constitution. The

Court observed that privacy is intrinsic to dignity, liberty, and autonomy. Importantly, the judgment recognized informational privacy as an essential aspect of constitutional protection in the digital age.Justice Chandrachud, speaking for the majority, emphasized that individuals possess the right to control dissemination of personal information. The Court acknowledged that technological developments and digital data collection create serious threats to informational autonomy. Consequently, the *Puttaswamy* judgment laid the constitutional foundation for recognizing RTBF in India.

Informational Privacy and Human Dignity

Informational privacy refers to the ability of individuals to exercise control over the collection, storage, and dissemination of personal data. In the digital era, personal information can easily be collected and circulated without consent through social media platforms, search engines, data brokers, and online archives. The permanent accessibility of such information often affects reputation, employment opportunities, social relationships, and mental well-being. The recognition of informational privacy is closely linked to the constitutional value of human dignity. Article 21 protects not merely physical existence but also the right to live with dignity and self-respect. Continuous online exposure of outdated or harmful information may deprive individuals of the opportunity to rebuild their lives and reintegrate into society. RTBF therefore seeks to protect dignity by allowing individuals to request removal or de-indexing of irrelevant personal information.

The Supreme Court in *Puttaswamy* acknowledged that informational privacy is necessary in modern constitutional democracies because digital technologies possess the ability to create extensive profiles of individuals. [28.] The judgment emphasized that individuals should maintain control over their personal data and online identity. This principle directly supports the philosophical foundation of RTBF.At the same time, informational privacy cannot operate in isolation from other constitutional values. Courts must balance privacy against freedom of speech, public interest, and transparency. Consequently, the constitutional framework governing RTBF involves competing rights rather than absolute entitlements.

Judicial Recognition of RTBF in India

Following the *Puttaswamy* judgment, Indian courts gradually began recognizing RTBF in specific factual situations. One of the earliest judicial recognitions emerged in *X v. Registrar*

General, High Court of Karnataka. [29.] In this case, the petitioner sought removal of her name from an online judgment involving sensitive personal matters. The Karnataka High Court allowed the request and observed that RTBF is consistent with the evolving trend of protecting privacy in modern societies.

The Delhi High Court further expanded recognition of RTBF in *Jorawar Singh Mundy v. Union of India*. [30.] The petitioner had been acquitted in a criminal case but continued to face reputational harm because the judgment remained accessible through online search results. The Court acknowledged that unrestricted availability of acquittal records could prejudice employment opportunities and social reputation. Consequently, it directed removal of certain online records from search engine results.

However, courts continue to adopt a case-by-case approach because India lacks comprehensive legislation specifically governing RTBF. The absence of uniform standards creates uncertainty regarding scope, procedure, and enforcement.

RTBF and Freedom of Speech

One of the most complex constitutional issues surrounding RTBF is its relationship with freedom of speech and expression guaranteed under Article 19(1)(a). While RTBF seeks to protect privacy and dignity, unrestricted recognition of the right may suppress legitimate public information and undermine democratic transparency. Freedom of speech includes the right of journalists, researchers, and citizens to access and disseminate information relating to matters of public importance. Court judgments, criminal proceedings, and news reports often serve important public functions. Consequently, courts must carefully balance privacy against public interest while deciding RTBF claims. The principle of proportionality has emerged as the primary constitutional balancing mechanism in such cases. Restrictions on access to information must satisfy tests of legality, necessity, and proportionality. [31.] Therefore, information relating to public officials, serious crimes, or matters affecting society may continue to remain publicly accessible despite privacy claims.

Thus, RTBF in India is not an absolute right but a carefully balanced constitutional principle operating within the framework of democratic accountability and free expression.

6.5 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 represents India's most significant legislative effort toward regulating personal data protection. [32.] The Act grants individuals certain rights concerning correction and erasure of personal data processed by data fiduciaries. It also imposes obligations regarding lawful processing, consent, and protection of personal information. Consequently, while the constitutional and statutory framework for informational privacy in India has evolved considerably, a comprehensive and clearly enforceable RTBF regime remains absent. Future reforms must therefore balance privacy, dignity, transparency, and democratic accountability in the digital age.

CHALLENGES AND THE FUTURE OF RTBF IN INDIA

Conflict Between Privacy and Freedom of Speech

One of the major challenges associated with the Right to Be Forgotten (RTBF) is balancing privacy with freedom of speech and expression under Article 19(1)(a) of the Constitution. While RTBF aims to protect individuals from perpetual digital stigma, unrestricted recognition of the right may suppress information that is relevant to society. Journalists and media organizations often argue that excessive deletion of online content may undermine transparency, accountability, and press freedom.[33]

The issue becomes particularly significant in cases involving public officials, criminal proceedings, and matters of public importance. Information that may appear outdated for one individual could still possess historical or social relevance for the public. Therefore, courts are required to balance privacy rights against public interest on a case-by-case basis.

Judicial Transparency and Public Records

Another important concern relates to judicial transparency. Court judgments are public documents intended to ensure openness and accountability in the administration of justice. However, digital publication of judgments has increased the accessibility of personal information, especially in sensitive cases involving matrimonial disputes, acquittals, or sexual offences.

The continued availability of such records online may negatively affect an individual's reputation and future opportunities. At the same time, complete removal of judicial records

may weaken public confidence in the legal system and affect legal research. Consequently, courts often prefer limited measures such as anonymization or de-indexing instead of complete deletion. [34.]

Technological and Enforcement Challenges

Implementation of RTBF also faces practical and technological difficulties. Digital information spreads rapidly across multiple platforms, servers, and jurisdictions, making complete erasure almost impossible. Even if information is removed from one website, copies may continue to exist elsewhere through screenshots, archives, or reposts.

Search engines and social media companies further complicate enforcement because they operate across different countries with varying privacy laws. This creates jurisdictional challenges for Indian courts while enforcing RTBF orders against global digital intermediaries. [35.]

The Future of RTBF in India

Despite these challenges, RTBF is likely to become increasingly significant in India due to growing internet usage and concerns regarding digital privacy. Judicial recognition of informational privacy after *Justice K.S. Puttaswamy v. Union of India* has already created a constitutional foundation for future development. [36.]

However, India still lacks a comprehensive legal framework specifically governing RTBF. Future reforms must therefore establish clear standards regarding removal of online information while balancing privacy, free speech, transparency, and public interest. A balanced approach will be essential to ensure protection of dignity without undermining democratic values.

SUGGESTIONS AND REFORMS

Need for a Comprehensive RTBF Framework

India currently lacks a specific statutory framework exclusively governing the Right to Be Forgotten (RTBF). Although courts have recognized informational privacy through judicial interpretation, the absence of clear legislation creates uncertainty regarding enforcement, scope, and procedural safeguards. Therefore, Parliament should enact a comprehensive legal

framework clearly defining the circumstances under which individuals may seek removal or de-indexing of personal information. [37.]

Such legislation should specify factors including public interest, nature of information, passage of time, and potential harm to reputation while evaluating RTBF claims. A codified framework would also ensure consistency in judicial decisions and reduce ambiguity in privacy disputes.

Establishment of Uniform Judicial Guidelines

Indian courts currently decide RTBF cases on a case-by-case basis, resulting in inconsistent standards. Uniform judicial guidelines are therefore necessary to balance privacy with freedom of speech and transparency. Courts should distinguish between private individuals and public figures while evaluating requests for removal of online content. [38.]

Information relating to public officials, serious criminal offences, or matters affecting public welfare should generally remain accessible, whereas sensitive personal information lacking public relevance may deserve greater protection.

Strengthening the Role of Data Protection Authorities

The effective implementation of RTBF also requires strong institutional mechanisms. A specialized Data Protection Authority should be empowered to address complaints relating to unlawful retention or dissemination of personal information. Such an authority could provide faster remedies and reduce excessive dependence on lengthy judicial proceedings. [39.]

Additionally, search engines and social media platforms should be required to establish transparent grievance redressal mechanisms enabling individuals to request removal of harmful or outdated information.

Promoting Digital Awareness and Responsible Data Governance

Public awareness regarding digital privacy remains limited in India. Many individuals unknowingly share sensitive personal information online without understanding its long-term consequences. Therefore, digital literacy and awareness programs should be promoted to educate citizens about privacy rights, cyber safety, and responsible online behavior. [40.]

Technology companies must also adopt ethical data governance practices by ensuring responsible collection, storage, and dissemination of personal data. Stronger intermediary accountability can significantly reduce misuse of personal information in the digital ecosystem.

Overall, India requires a balanced RTBF framework capable of protecting individual dignity and informational autonomy while simultaneously preserving transparency, accountability, and freedom of expression in a democratic society.

CONCLUSION

The emergence of the Right to Be Forgotten (RTBF) reflects the growing need to protect individual dignity and informational privacy in the digital age. The internet's ability to permanently preserve and circulate personal information has fundamentally altered the relationship between privacy, reputation, and technology. In many instances, individuals continue to suffer social, professional, and psychological consequences because outdated or irrelevant information remains indefinitely accessible online. RTBF therefore seeks to provide individuals with greater control over their digital identity and personal data.

In India, the constitutional foundation for RTBF has evolved through judicial interpretation of Article 21 and the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India*.Subsequent High Court decisions further acknowledged the importance of protecting individuals from unnecessary digital exposure. However, despite these developments, India still lacks a comprehensive statutory framework specifically governing RTBF.

At the same time, RTBF cannot function as an absolute right. Excessive recognition of digital erasure may adversely affect freedom of speech, judicial transparency, press freedom, and public access to information. Therefore, a careful balance must be maintained between privacy rights and democratic accountability. Courts and lawmakers must ensure that RTBF protects genuine privacy interests without enabling censorship or suppression of historically relevant information.

The Digital Personal Data Protection Act, 2023 represents an important step toward strengthening informational privacy in India, yet further reforms remain necessary. India

requires a balanced and clearly enforceable RTBF framework supported by uniform judicial standards, effective institutional mechanisms, and responsible data governance practices.

Ultimately, in a society increasingly shaped by digital memory, the right to move beyond one's past and reclaim personal dignity has become essential to meaningful liberty in the twenty-first century.

REFERENCES

Books

1. Orla Lynskey, The Foundations of EU Data Protection Law (Oxford University Press 2015).
2. Tal Z. Zarsky, Privacy and Data Collection in a Digital Era (Cambridge University Press 2014).

Journal Articles

3. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, *4* Harv. L. Rev. 193 (1890).
4. Jeffrey Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88 (2012).
5. Ambika Kumar, Right to Be Forgotten: An Analysis of the Conflict Between Privacy and Freedom of Expression, 12 Indian J.L. & Tech. 45 (2020).
6. Apar Gupta & Raghav Sharma, Privacy and Data Protection in India: A Critical Analysis, 9 Indian J.L. & Tech. 112 (2018).

Case Laws

7. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
8. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
9. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
10. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
11. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
12. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
13. Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ECLI:EU:C:2014:317 (2014).

14. X v. Registrar General, High Court of Karnataka, W.P. No. 62038 of 2016 (Karnataka High Court, Jan. 23, 2017).
15. Jorawar Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306.
16. S. Karuppannan v. The Commissioner of Police, 2021 SCC OnLine Mad 8096.
17. Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.

Statutes and Regulations

18. The Constitution of India, 1950.
19. The Digital Personal Data Protection Act, No. 22 of 2023 (India).
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

Reports and Online Sources

25. Justice B.N. Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).
26. Law Commission of India, Report No. 276: Legal Framework for Data Protection in India (2018).
27. United Nations Human Rights Council, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/39/29 (2018).