
RECOGNISED BUT NOT REALISED: THE RIGHT TO BE FORGOTTEN IN INDIA'S EVOLVING LEGAL FRAMEWORK

Sai Prarthana M, School of Excellence in Law, Tamil Nadu Dr. Ambedkar Law University, Chennai.

ABSTRACT:

This research paper analysis the historical evolution, international perspective and the contemporary modern realities of the right to be forgotten, now at its very nascent stage of recognition under the Digital Personal Data Protection Act, 2023, read with its Rules of 2025. It traces the historical evolution from the recognition of the right to privacy as a fundamental right under Article 21 of the Constitution of India, 1950 to its newest specie with respect to informational autonomy and privacy, the right to be forgotten, by analysing the legislative jurisprudence formulated over the years, since its inception in the cases of MP Sharma and Kharak Singh. The paper also studies the international undertones of the right of erasure, recognised under the General Data Protection Regulation, 2016 of the European Union, which serves as the foundation for the legal framework established by the United Kingdom. It also analysis the lack of a coherent federal framework on the right to be forgotten in the United States akin to that of India, EU or the UK, although certain inchoate state legislations exist. The paper then analyses the case laws which are currently in vogue pertaining to the right, although they are few in number owing to its incipient stage. In conclusion, the study concludes with the question of the right's enforcement in light of the tremendous growth of Artificial Intelligence, specifically Generative Artificial Intelligence, which questions the enforceability and effectiveness of the right in its entirety, thus requiring a tighter framework to ensure proper recognition and protection.

Keywords: Right to be Forgotten – Right of Erasure – Right to Privacy – Data Protection – Artificial Intelligence.

A. INTRODUCTION:

The Right To Be Forgotten or the Right of Erasure is an extension of the Right to Privacy recognised under Article 21 of the Constitution of India, 1950¹ vide the landmark judgement of '*Justice K.S. Puttaswamy (Retired) vs. Union of India*.'² Simply put, it is the right granted to individuals to erase their personal data from the public domain if the same becomes irrelevant, outdated, inadequate, no longer serves a legitimate public interest or could inflict undue harm upon their reputation, dignity or well-being.³

B. EVOLUTION THROUGH JUDICIAL INTERPRETATION:

The dialectic on RTBF begins with its genus - the right to privacy. Initially narrow in scope, Article 21 has grown to become a holistic legal umbrella which encompasses any and all aspects pertaining to the fundamental concept of being human, along with the protection and preservation of fellow living creatures and environment. Pertaining to the right to privacy guaranteed under Article 21, preliminary cases in this arena of law include *M.P. Sharma vs. Satish Chandra*⁴ and *Kharak Singh vs. State of Uttar Pradesh*,⁵ which primarily dealt with the issues of search, seizure and surveillance by the police. The former held that such actions did not amount to a violation of privacy as the Constitution of India did not explicitly guarantee such a right. This stance was then changed to a premature idea of the right to privacy that is currently in vogue in the dissenting opinion in the case of *Kharak Singh*, on an implicit right to be left alone. Justice Subba Rao and others observed that mere physical freedom was inadequate. This called for larger protection against constant surveillance or intrusion on a whole. The cases of *Govind vs. State of Madhya Pradesh*⁶ and *R. Rajagopal vs. State of Tamil Nadu*⁷ ideated the concepts of privacy beyond mere protection from physical searches.⁸

Finally, in the year 2017, the Puttaswamy judgement recognised the right to privacy as a fundamental right under Part III of the Constitution, which implicitly includes the Right to be

¹ INDIA CONST. art. 21.

² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

³ The Right to Forgotten in India: Right to Privacy v. Right to Information, LAWS.IN (Mar. 2025), <https://www.law8.in/2025/03/the-right-to-forgotten-in-india-right.html>.

⁴ M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

⁵ Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

⁶ Govind v. State of Madhya Pradesh, AIR 1975 SC 1378.

⁷ R. Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264.

⁸ Aishwarya Agrawal, Right to Privacy in India, LAW BHOOMI (Apr. 7, 2025), <https://lawbhoomi.com/right-to-privacy/>.

Forgotten. The judgement further outlined certain situations where this right might not apply in cases involving public interest, public health, archival purposes, research and legal claims. It was held that the right to privacy covers bodily integrity, one's control over personal information and freedom to make autonomous personal choices. Justice Kaul emphasised that every individual is entitled to exercise control over their own life and image portrayed in the public domain and to control the commercial use of their identity.⁹

C. THE LEGAL FRAMEWORK IN INDIA:

The Right to be Forgotten was unspecified and ungoverned in the Indian legal framework, until the enactment of the Digital Personal Data Protection Act, 2023. In order to understand the harbinger of the right to be forgotten, emphasis needs to be given to the legislation which is fundamental and serves as the cornerstone for e-commerce transactions and electronic communication in India – the Information Technology Act, 2000.

1. The Information Technology ('IT') Act, 2000 read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The Information Technology ('IT') Act, 2000, based on the United Nations Commission on International Trade Law's (UNCITRAL) Model Law on Electronic Commerce, 1997, provides for the legal recognition of electronic transactions, electronic data interchange and electronic commerce holistically, along with facilitating the electronic filing of documents with government agencies. Although the IT Act, 2000 does not explicitly guarantee the right to be forgotten to users of e-commerce, Section 43A penalises businesses if their negligence in handling and securing the sensitive personal data or information (SPDI) of its users causes unauthorised gain or unauthorised loss to the affected persons, and mandates compensation for the same.

The imperative feature of the SPDI Rules, 2011 is its definition of 'sensitive personal data' under Rule 3.¹⁰ It states that term includes passwords, financial information, health conditions,

⁹ The Right to Be Forgotten: Reclaiming Dignity in Digital Age, DISPUTE RESOLUTION BLOG (Sept. 2025), <https://disputeresolution.cyrilamarchandblogs.com/2025/09/the-right-to-be-forgotten-reclaiming-dignity-in-digital-age/>.

¹⁰ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 3 (India).

sexual orientation, medical records or medical history, biometric information or any other detail relating to the above provided to a body corporate to avail their services. It excludes information which is available in the public domain or can be obtained under the Right to Information Act, 2005. Furthermore, it provides for collection of data for its utilisation in lawful purposes, mandates publication of their privacy policy on the websites of body corporates, transfer of information, reasonable security practices and redressal of grievances.

With the enactment of the Digital Personal Data Protection Rules, 2025, the relevance of this section and the adjoining rules on this area of law, the Sensitive Personal Data or Information (SPDI) Rules, 2011 has diminished since the enactment of Digital Personal Data Protection Act, 2023 which provides a comprehensive framework on personal data protection in India.

2. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Complimenting the IT Act, 2000 and the SPDI Rules, 2011, in this arena is the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the key features of which have been elaborated as follows:

1. Rule 3 – This Rule provides for due diligence to be carried out by intermediaries. Rule 3(1)(d) states that intermediaries must remove or disable unlawful information within 36 hours of a court order or government notice. Rule 3(2)(a)(i) states that Grievance Officers must acknowledge complaints within 24 hours and resolve them within a span of 15 days. It further states that removal requests pertaining to privacy violations must be resolved within a span of 72 hours. Rule 3(2)(b) states that if content exposes private areas, depicts nudity or sexual conduct or impersonation, intermediaries must remove such content within 24 hours of the lodging of the complaint. According to Rule 3(2)(c), intermediaries must devise a mechanism for individuals to submit details for removal requests.¹¹
2. Rule 3A – This Rule provides for a Grievance Appellate Committee if the requests for erasures are not resolved by the aforementioned Grievance Officer. Such appeals must

¹¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3 (India).

be decided within 30 days.¹²

3. Rule 4 – Rule 4(1)(d) provides for additional due diligence by means of monthly compliance reports which must include details of complaints received and the removed or disabled content. Rule 4(4) states that platforms must proactively devise and deploy technology to identify and block content which was already removed. Rule 4(8) states that if the platforms remove content on their own, they must notify the user, provides reasons which warranted the removal of such content and provide an opportunity to the said user to put forth their claims and the dispute the removal.¹³
4. Rule 12 – Self-regulatory bodies can direct publishers to delete or modify content if the same violates the Code of Ethics or could potentially incite the commission of offences.¹⁴
5. Rule 14¹⁵ – The Inter-Departmental Committee has been empowered under this Rule to recommend deletion or modification of content to prevent incitement of offences or for reasons stipulated under Section 69A of the IT Act, 2000.¹⁶
6. Rule 15 – The Ministry of Information and Broadcasting has been empowered with powers of oversight whereby it can direct the publishers or intermediaries to delete, modify or block content for public access within a specified time.¹⁷

3. Digital Personal Data Protection Act ('DPDP') Act, 2023

The Digital Personal Data Protection Act ('DPDP') Act, 2023 was enacted to provide for the processing of digital personal data (defined under Section 2(n))¹⁸ in a manner which recognises and balances both the right of individuals to protect their personal data and the necessity to process such data for lawful purposes and related matters. The following are the key provisions in the Act which deal with the right of erasure:

¹² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3A (India).

¹³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4 (India).

¹⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 12 (India).

¹⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 14 (India).

¹⁶ Information Technology Act, 2000, § 69A, No. 21, Acts of Parliament, 2000 (India).

¹⁷ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 15 (India).

¹⁸ Digital Personal Data Protection Act, 2023, § 2(n), No. 22, Acts of Parliament, 2023 (India).

1. Section 2(x) – This sub-section defines the term ‘processing’ with reference to personal data to mean a wholly or partly automated operation or set of operations performed on the digital personal data which includes collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction. By including erasure as one of the operations of processing digital personal data, the Act acknowledges the deletion or erasure of data as a recognised form of processing. This sub-section read with the object of the Act lays down the foundation for harmoniously balancing the rights of individuals to protect their personal data whilst ensuring legal compliance and associated matters.
2. Section 8 – This section outlines the general obligations of Data Fiduciaries. Their obligations include ensuring accuracy, security safeguards, notification to the Data Protection Board of India¹⁹ (established under Section 18) and the affected Data Principals in case of breach, grievance redressal and publication of the business contact information of Data Protection Officers, *inter alia*.²⁰ Sub-section (7) explicitly addresses the right of erasure, wherein it states that a Data Fiduciary shall erase personal data of the Data Principal upon the withdrawal of their consent or as soon as it is reasonable to assume that the purpose for which the personal data was collected is no longer being served, whichever is earlier and cause its Data Processor (defined under Section 2(k) to refer to a person who processes the personal data on behalf of the former)²¹ to erase any personal data that was made available by the former to the latter, unless the retention of the same is necessary for legal compliance with any law in vogue.
3. Section 12 – This section is the another key provision as it deals with the right to erasure of personal data *inter alia*, wherein a data principal (defined under Section 2(j) to refer to the individual to whom the digital personal data relates to),²² has been guaranteed the right to correction, completion, updating and erasure of their personal data after the purpose for which it was collected and consented to has been fulfilled. The Data Fiduciary (the entity processing the digital personal data) must comply with the same by correcting the inaccurate or misleading data, complete the incomplete data and

¹⁹ Digital Personal Data Protection Act, 2023, § 18, No. 22, Acts of Parliament, 2023 (India).

²⁰ Digital Personal Data Protection Act, 2023, § 8, No. 22, Acts of Parliament, 2023 (India).

²¹ Digital Personal Data Protection Act, 2023, § 2(k), No. 22, Acts of Parliament, 2023 (India).

²² Digital Personal Data Protection Act, 2023, § 2(j), No. 22, Acts of Parliament, 2023 (India).

update the personal data. The Data Fiduciary shall comply with the Data Principal's request of erasure, unless the same must be retained for the specified purpose or for legal compliance.²³

4. Sections 11, 13, 14 and 15 – These sections, under Chapter III of the Act of which Section 12 is a part, guarantee certain rights to and stipulate duties of Data Principals. Firstly, Section 11 grants Data Principals with the right to access information about their personal data from the Data Fiduciary.²⁴ Secondly, Section 13 guarantees the Data Principal's right of grievance redressal provided by either the Data Fiduciary or the Consent Manager in respect of their act or omission in fulfilling their obligations or the exercise of the Data Principal's rights under the provisions of this Act.²⁵ Thirdly, Section 14 provides the Data Principal with the right to nominate another to act of their behalf in situations of death or incapacity.²⁶ Finally, Section 15 stipulates the duties of Data Principals, wherein they are mandated to comply with the provisions of all applicable laws in force while exercising the provisions of this Act, ensuring against impersonation while providing personal data for a specified purpose and ensuring against suppression of materials information while providing her personal data, *inter alia*.²⁷
5. Section 40 – Under Section 40(2)(n), the Central Government by notification and subject to the condition of previous publications, may make rules on the manner in which a Data Principal shall make a request for erasure under Section 12(3) to the Data Fiduciary.²⁸

4. Digital Personal Data Protection ('DPDP') Rules, 2025

The Government of India notified the DPDP Rules, 2025 on 14th November 2025. Together, the Act and the Rules form a citizen-centric framework on the right to privacy and the right to be forgotten.²⁹ Rule 8 states that personal data which was processed for specific purposes must

²³ Digital Personal Data Protection Act, 2023, § 12, No. 22, Acts of Parliament, 2023 (India).

²⁴ Digital Personal Data Protection Act, 2023, § 11, No. 22, Acts of Parliament, 2023 (India).

²⁵ Digital Personal Data Protection Act, 2023, § 13, No. 22, Acts of Parliament, 2023 (India).

²⁶ Digital Personal Data Protection Act, 2023, § 14, No. 22, Acts of Parliament, 2023 (India).

²⁷ Digital Personal Data Protection Act, 2023, § 15, No. 22, Acts of Parliament, 2023 (India).

²⁸ Digital Personal Data Protection Act, 2023, § 40(2)(n), No. 22, Acts of Parliament, 2023 (India).

²⁹ Press Information Bureau, Government of India, DPDP Rules, 2025 Notified, PIB (Nov. 17, 2025), <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf>.

be deleted once the purpose is no longer served, unless the retention is required by law. It further states that if a data principal does not contact the data fiduciary or exercises rights within the prescribed period, the purpose is deemed complete and triggers the erasure of data. The fiduciaries must notify the principals at least 48 hours in prior before deletion and inform that their personal data shall be erased, unless they re-engage into their user account or initiates contact with their fiduciary or exercises rights in relation to the processing of their personal data.³⁰

Rule 14 provides for the rights of data principals, which states that data fiduciaries must provide mechanisms via websites, applications or contact points for principals to exercise their rights under the DPDP Act, 2023, including erasure requests. Any complaints and grievances received must be resolved within the prescribed timeframe, thereby ensuring effective enforcement of the right of erasure.³¹

D. PERSPECTIVES FROM THE INTERNATIONAL FRAMEWORK:

1. European Union

European Union's General Data Protection Regulation (GDPR) replaced its predecessor, the EU Data Protection Directive 95/46/EC, which governed the protection of personal data since 1995.³² The GDPR (Regulation (EU) 2016/679), enacted in 2016 and effective since 25th May 2018, governs the collection, processing and erasure of personal data. The landmark case which recognised the right of erasure is *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*³³ established the right to erasure, wherein the European Court of Justice (ECJ) held that individuals have a right to ask search engines (here, Google) to remove links to websites that contain their personal information if it satisfies one of the following criteria:

1. It is inadequate, or
2. It is irrelevant, or

³⁰ Digital Personal Data Protection Rules, 2025, r. 8 (India).

³¹ Digital Personal Data Protection Rules, 2025, r. 14 (India).

³² EU Privacy Directive: From Directive 95/46/EC to GDPR, GDPR LOCAL (Sept. 2025), <https://gdprlocal.com/european-unioni-privacy-directive/>.

³³ *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, EU:C:2014:317, 2014 E.C.R. I-317.

3. It is no longer relevant.

After its recognition in the aforementioned case, the right of erasure gained legal backing with its inclusion in the GDPR as Article 17, specifically under recitals 65 and 66. Article 17 of the GDPR guarantees data subjects the right to erase their personal data vested with the hands of organisations.³⁴ The right is not absolute in nature; it is discretionary.

Therein, the data subjects have the right to obtain from the controller the erasure of personal data concerning themselves without undue delay (here, considered to be about a month) and the controller shall have the obligation to erase the same, after due verification that the person requesting erasure is the bona fide data subject, if one of the following conditions apply.³⁵

1. The personal data is no longer necessary in relation to the purposes for which they were collected or processed.
2. The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) or point (a) of Article 9(2) and where there is no legal ground for the processing.
3. The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing or the data subject objects to the processing pursuant to Article 21(2).
4. The personal data has been processed for direct marketing purposes and the data subject objects to such processing.
5. The personal data has been processed unlawfully.
6. The personal data have to be erased for compliance with a legal obligation in a Union or Member State law to which the controller is subject to.
7. The personal data of a child has been processed to offer their information society

³⁴ Everything You Need to Know About the “Right to Be Forgotten,” GDPR.EU, <https://gdpr.eu/right-to-be-forgotten/> (last visited June 9, 2026).

³⁵ Art. 17 GDPR – Right to Erasure (“Right to Be Forgotten”), GDPR.EU, <https://gdpr.eu/article-17-right-to-be-forgotten/> (last visited June 9, 2026).

services referred to Article 8(1).

In the case of *GC and Others (De-referencing of sensitive data)*,³⁶ private individuals brought proceedings in the French *Conseil d'État* against the French Supervisory Authority, the National Commission on Data Processing and Civil Liberties (CNIL) for its refusal to order Google to de-reference links containing sensitive personal data on politics, religion and criminal offences. The Court of Justice of the European Union (CJEU) affirmed the aforementioned judgement and emphasised Article 17(3)(a), requiring a balance between the right of privacy under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union) and the freedom of information under Article 11. It held that search engines must assess on a case-by-case basis whether the inclusion of such links is strictly necessary for public access and that operators must ensure that search results relating to outdated criminal proceedings reflect the current legal situation to avoid misleading information.

Although not relating to the implementation of GDPR, a case on the right to be forgotten by the European Court of Human Rights (ECtHR) is that of *Mediengruppe Österreich GmbH vs. Austria*,³⁷ wherein the Court upheld Austria's restriction of publishing a photograph of a man labelled 'convicted neo-Nazi,' as his conviction was long past and erased from records. Although the Court did not blanketly restrict reporting on past crimes, it held that linking outdated convictions to current images without further context unfairly harmed a person's reputation and did not find a violation of Article 10 of the European Convention on Human Rights (ECHR). Another case is of *Węgrzynowski and Smolczewski v. Poland*, where two lawyers sought the removal of defamatory online articles. Previously, the domestic courts had ruled that the articles did breach their rights, but they still denied granting deletion of the same. The ECtHR upheld the same stance, by stating that since internet's permanence differs from print, it requires specific and tailored rules rather than applying the laws which governs traditional print media communication. Yet, since the applicants had claimed for total removal rather, it held that the prior refusal by domestic courts was valid as it was proportionate.³⁸

2. United States of America

The United States lacks a federal equivalent as that of India or the European Union. Balancing

³⁶ *GC and Others (De-referencing of Sensitive Data)*, Case C-136/17, EU:C:2019:773.

³⁷ *Mediengruppe Österreich GmbH v. Austria*, No. 37713/18 (Eur. Ct. H.R. Apr. 26, 2022).

³⁸ *Węgrzynowski and Smolczewski v. Poland*, No. 33846/07 (Eur. Ct. H.R. July 16, 2013).

the First Amendment's³⁹ strong protection of free speech and press with the right of erasure strives to be constitutionally problematic.⁴⁰ A few specific federal laws include the Children's Online Privacy Protection Act, 1998, parents can request the deletion of data collected from children below the age of 13 years. The Fair Credit Reporting Act (FCRA) regulates credit reporting agencies and provides individuals the right to remove outdated negative information pertaining to bankruptcies and delayed payments from their credit reports after a certain time period. The Video Privacy Protection Act, 1998 prevents the wrongful disclosure of video rental records.⁴¹

State-level privacy laws include California Consumer Privacy Act, 2018 (CCPA) and the California Privacy Rights Act, 2020 (CPRA) which grants the residents a 'right to delete' personal data collected by businesses, subject to certain exceptions, such as when the data is required to complete a transaction, for security purposes and exercising free speech. Other laws such as the Virginia Consumer Data Protection Act, 2021 (VCDA) and Colorado's Privacy Act, 2021 (CPA) and states like Utah and Connecticut have implemented the right on similar lines as that of California's.⁴²

3. United Kingdom

Article 17 of the UK GDPR provides individuals with the right to be forgotten. This right applies to the data held at the time the request is received and it does not apply to data that may be created in the future. Like EU's GDPR, the right is not absolute in nature and applies only in certain circumstances. This right is guaranteed to individuals if it fulfils certain criteria, which is similar to that of the EU. The Information Commissioner's Office (ICO) confirms that the right to erasure under the UK GDPR is not absolute. A few exemptions to the right are freedom of expression, legal obligation, public interest, scientific research and archiving.⁴³

In *NT1 & NT2 v Google LLC*,⁴⁴ two businessmen sought delisting of search results linking to

³⁹ The First Amendment: Your Ultimate Guide to Freedom of Speech, Press, and Religion, US LAW EXPLAINED, https://uslawexplained.com/first_amendment (last visited June 9, 2026).

⁴⁰ The Right to Be Forgotten: Explained, US LAW EXPLAINED, https://uslawexplained.com/right_to_be_forgotten (last visited June 9, 2026).

⁴¹ *Ibid.*

⁴² *Ibid.*

⁴³ Right to Erasure (Right to Be Forgotten), INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/> (last visited June 9, 2026).

⁴⁴ *NT1 & NT2 v. Google LLC*, [2018] EWHC 799 (QB).

reports of their past convictions. The High Court of England and Wales (Queen's Bench Division) balanced the right to privacy with the freedom of information, by applying the principles from the Google Spain case. While NT1's claim failed as his conviction for business fraud remain relevant; he did not show remorse and public interest outweighed his right of privacy, NT2's claim succeeded as his conviction was minor in character, he admitted guilt and expressed remorse and posed no risk of reoffending and the Court ordered to delist NT2's link alone.

E. DISTINCTION BETWEEN THE RIGHT OF ERASURE AND THE RIGHT TO BE FORGOTTEN

While the EU and UK provide for the right to be forgotten, India provides for the right of erasure, there is a subtle but important distinction. India's right finds legal backing under Section 18 of the DPDP Act, 2023 which grants individuals the right to request the deletion of their personal from data fiduciaries when it's no longer necessary, withdrawal of consent or unlawful processing. Therefore, India's right focusses on removal of personal of data from the fiduciary's system, data minimisation and individual control over personal data.

In the EU and UK, the focus is on the right to be forgotten, which is broader in scope than the right of erasure as it not just includes deletion, but allows individuals to exercise their rights to de-list and de-refer their personal data and information from the public domain. Therefore, it balances the freedom of speech and expression with public interest.

F. THE RIGHT TO BE FORGOTTEN IN INDIA'S JUDICIAL DECISIONS⁴⁵

The growing public discourse and jurisprudential dialectic by Indian courts on this right have expanded it to de-listing and de-indexing as well, as evinced by the following judgements.

In the case of *Karthick Theodore vs. Registrar General, Madras High Court*, Karthick Theodore, an Indian national, was acquitted of rape and cheating charges. He sought removal of his name from court records and online platforms and additionally sought directions to Ikanoon Software Development Private Limited to implement the redactions. But the Single Bench dismissed the petition. Theodore then filed a writ appeal seeking to set aside the dismissal and secure redaction of his identity. Thereafter, the Division Bench of the Hon'ble

⁴⁵ The Right to Be Forgotten: Reclaiming Dignity in Digital Age, DISPUTE RESOLUTION BLOG, supra note 9.

Court allowed limited anonymisation. In the aftermath of the Division Bench's decision,⁴⁶ Ikanoon Software Development Private Limited filed a Special Leave Petition⁴⁷ before the Hon'ble Supreme Court. Vide an order dated 24th July 2024, the Hon'ble Court stayed the decision of the Division Bench and tagged this matter with that of *Alka Malhotra vs. Union of India & Ors*⁴⁸ which raised similar questions on the right to be forgotten and the continued availability of court decisions. This case is sub-judice, and the Hon'ble Apex Court must now decide the extent and enforceability of the right.⁴⁹

The case of *Jorawar Singh Mundy vs. Union of India & Others*⁵⁰ deal with a petition filed by an Indian-American citizen, acquitted in a criminal case, against the continued availability of the judgement passed by an Indian court as it impaired his career prospects in the US. The Hon'ble Delhi Court recognised the right to be forgotten and directed search engines to de-index the said judgement. A similar stance was held in *Vysakh K.G. v. Union of India*⁵¹ where the Hon'ble Kerala High Court recognised the right to be forgotten to past cases and not ongoing ones, when continued publication of cases online causes social or professional harm. The same was held in the case of *Mr. SJ v. Union of India*.⁵²

G. THE RIGHT TO BE FORGOTTEN IN AN EVOLVING LANDSCAPE

With the permeability of AI in all aspects of daily life inevitable, the challenges that AI poses to the effective implementation of AI must be studied in depth. The tussle between the right and AI is while AI is designed to remember, the right grants individuals the ability to forget. AI models are trained on massive datasets and data becomes embedded in model weights and not just on stored records. Therefore, deleting original data does not amount to fully terminating its influence.⁵³ Generative AI systems can reproduce personal data and infer identities indirectly as training datasets often include publicly scraped data.⁵⁴ Any form of removal of data may require retraining the entire model as location and erasure of specific data is difficult

⁴⁶ Karthick Theodore v. Registrar General, 2024 SCC OnLine Mad 6529.

⁴⁷ Ikanoon Software Development Pvt. Ltd. v. Karthick Theodore, SLP (C) No. 15311 of 2024.

⁴⁸ Alka Malhotra v. Union of India, W.P. (C) No. 19 of 2024.

⁴⁹ The Right to Be Forgotten: Reclaiming Dignity in Digital Age, DISPUTE RESOLUTION BLOG, supra note 9.

⁵⁰ Jorawar Singh Mundy v. Union of India, W.P. (C) No. 3918 of 2021.

⁵¹ Vysakh K.G. v. Union of India, 2022 SCC OnLine Ker 7337.

⁵² Mr. SJ v. Union of India, W.P. (C) No. 5608 of 2023.

⁵³ Right to Be Forgotten in AI Systems: Technical and Legal Challenges, Advocate Ritik Khurana (Jan. 2026), <https://rkhurana.lmadvocates.com/articles/forgotten-ai.html>.

⁵⁴ The Right to Be Forgotten vs. AI's Infinite Memory: A Regulatory Dilemma, DPO INDIA BLOG (2026), <https://www.dpo-india.com/Blogs/right-to-forgot/>.

in AI systems.⁵⁵ Another crucial aspect which needs immediate attention is to extend the right to the entire data lifecycle which includes stages of collection, storage, training and output and not restrict to deletion.⁵⁶ These challenges risk the perpetuation of permanent digital stigmatisation of the concerned individuals. On the other hand, this right may hinder the right to information, historical truth, impede journalism and obstruct public interest.⁵⁷

H. CONCLUSION

India is at a nascent stage in protecting the personal data of its citizens, with the enactment of the DPDP Act and Rules as recent as 2023 and 2025 respectively. As a nation, we still have a long way to go and judicial battles to win to protect the right of erasure, and its extension, the right to be forgotten.

⁵⁵ Right to Be Forgotten in AI Systems: Technical and Legal Challenges, Advocate Ritik Khurana, *supra* note 53.

⁵⁶ The Right to Be Forgotten vs. AI's Infinite Memory: A Regulatory Dilemma, DPO INDIA BLOG, *supra* note 54.

⁵⁷ Right to Be Forgotten in India: Key Ingredients, SUPREME TODAY AI (2025), <https://supremetoday.ai/issue/right-to-be-forgotten-india-key-ingredients>.

REFERENCES:

A. Legislations:

1. Constitution of India, 1950.
2. Information Technology Act, 2000, No. 21 of 2000 (India).
3. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
5. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
6. Digital Personal Data Protection Rules, 2025 (India).

B. Bibliography:

1. European Court of Justice Issues Judgment on Right to Erasure Under EU Data Protection Rules, Lexology (2025), <https://www.lexology.com/library/detail.aspx?g=03f869f6-ba4b-4bf2-9a8f-6ca02b805903>.
2. The Right To be Forgotten: A Comprehensive Case Study Analysis, IJLR, <https://ijlr.iledu.in/wp-content/uploads/2024/10/V4I333.pdf>.
3. Plea in Delhi High Court: What Is the 'Right to Be Forgotten'?, Indian Express (2023), <https://indianexpress.com/article/explained/explained-law/right-to-be-forgotten-8466283/>.
4. The Right to Be Forgotten: Reclaiming Dignity in Digital Age, Dispute Resolution Blog (Sept. 2025), <https://disputeresolution.cyrilamarchandblogs.com/2025/09/the-right-to-be-forgotten-reclaiming-dignity-in-digital-age/>.
5. Drishti IAS Blog, Right to Be Forgotten in India (2025), <https://www.drishtias.com>.
6. The Right to Be Forgotten in India: Right to Privacy as a Fundamental Right, Law8.in (Mar. 2025), <https://www.law8.in/2025/03/the-right-to-forgotten-in-india-right.html>.
7. Right To Be Forgotten: A Step Forward In The Implementation Of Privacy Laws In India, ISSN 2456-9704, Supremo Amicus, <https://articles.manupatra.com/pdf/c54483d8-7f72-4d2a-9143-41f9611fc9e5.pdf>.

8. Right to Be Forgotten, GDPR.eu (Apr. 2026), <https://ks.echr.coe.int/documents/d/echr-ks/right-to-be-forgotten>.
9. Erasing Ourselves: The Case for a U.S. Right to Be Forgotten, 11 Wash. J.L. Tech. & Arts 75 (2015), <https://wjlt.com/2025/05/06/erasing-ourselves-the-case-for-a-u-s-right-to-be-forgotten/>.
10. A Right to Be Forgotten: The European Union vs. the United States, Juris Magazine (2020), <https://sites.law.duq.edu/juris/2025/12/03/a-right-to-be-forgotten-the-european-union-vs-the-united-states/>.
11. Right to Be Forgotten vs. Public Record: Supreme Court Stays Madras High Court Order, Desi Kaanoon (2025), <https://desikaanoon.in/right-to-be-forgotten-vs-public-record-supreme-court-stays-madras-high-court-order/>.
12. The Right to Be Forgotten and AI Legal Obligations, Technical Limits, and Innovation, Lund University (2025) <https://lup.lub.lu.se/luur/download?func=downloadFile&recordId=9189308&fileId=9197890>.
13. AI, Data Privacy, and the Right to Be Forgotten: Navigating Human Rights in the Age of Generative Technology, TechPolicy.Press (2025), <https://ijirl.com/wp-content/uploads/2025/04/AI-DATA-PRIVACY-AND-THE-RIGHT-TO-BE-FORGOTTEN-NAVIGATING-HUMAN-RIGHTS-IN-THE-AGE-OF-GENERATIVE-TECHNOLOGY.pdf>.
14. Rethinking the Right to Be Forgotten in India's AI Governance, Supreme Today AI (2025), <https://www.orfonline.org/expert-speak/rethinking-the-right-to-be-forgotten-in-india-s-ai-governance>.
15. The Right to Be Forgotten Is Dead: Data Lives Forever in AI, TechPolicy.Press (2025), <https://www.techpolicy.press/the-right-to-be-forgotten-is-dead-data-lives-forever-in-ai/>.
16. Your Right to Be Forgotten in the Age of AI, CSIRO (2025), <https://www.csiro.au/en/news/All/Articles/2023/September/your-right-to-be-forgotten-AI>.