INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 4 | Issue 4 | 2025 Art. 19

The Evolution of the Right to Be Forgotten as a Fundamental Aspect of Privacy and Data Protection

Juveria Fatima
LLM Researcher,
Centre of Post-Graduate Legal Studies,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar University, Lucknow

Sakshika Singhal
LLM Researcher,
Centre of Post-Graduate Legal Studies,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar University, Lucknow

Recommended Citation
Juveria Fatima and Sakshika Singhal, *The Evolution of the Right to Be Forgotten as a Fundamental Aspect of Privacy and Data Protection*, 4 IJHRLR 347-359 (2025).
Available at www.humanrightlawreview.in/archives/.

The Evolution of the Right to Be Forgotten as a Fundamental Aspect of Privacy and Data Protection

Juveria Fatima
LLM Researcher,
Centre of Post-Graduate Legal Studies,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar University, Lucknow

Sakshika Singhal
LLM Researcher,
Centre of Post-Graduate Legal Studies,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar University, Lucknow

Manuscript Received	Manuscript Accepted	Manuscript Published
13 July 2025	18 July 2025	26 July 2025

ABSTRACT

This study focuses on the Right to Be Forgotten (RTBF), a vital and evolving component of the broader right to privacy in the digital age. As personal data continues to be widely disseminated and stored online, individuals increasingly seek mechanisms to regain control over their digital identities. The research examines the legal recognition and scope of RTBF in India, especially in light of the Digital Personal Data Protection Act, 2023, and its interplay with constitutional rights such as freedom of expression and the public's right to know. Drawing parallels with the European Union's General Data Protection Regulation (GDPR), the study explores international-best practices and highlights the challenges in balancing RTBF with other competing interests. Through analysis of case law, statutory provisions, and regulatory frameworks, the study identifies gaps in implementation and enforcement mechanisms in the Indian context. It further proposes a structured and rights-based approach to operationalizing RTBF that ensures protection of individual privacy while preserving transparency and accountability. The study underscores the need for clear guidelines, robust grievance redressal mechanisms, and increased public awareness to effectively uphold the right in a digitally connected society.

KEYWORDS

GDPR, DPDP, Right to be forgotten, Right to privacy

EVOLUTION OF THE RIGHT TO PRIVACY

- ***Historical Background of Privacy***

Information has played a powerful role in every stage of human life. Throughout history information has been a powerful tool for humanity. Information serves primarily as a means of connection. The primary function of information is to connect individuals forming networks that shape societal structures. Be it old stories, religious texts or modern-day AI systems, all these help form networks by creating, disseminating and controlling information. Human society is deeply rooted in our unparallel ability to cooperate in large numbers. Thus, extensive cooperation is facilitated by shared narratives, stories, myths and ideologies that bind people together even in the absence of direct personal relationships. Though information can foster cooperation and understanding, it can also propagate falsehood and manipulation. Information does not always reflect reality and is not synonymous with truth. Information in the form of stories go beyond geographical boundaries. They are the social glue without which no human network can survive. As society started growing, oral conversation was not enough. It became necessary to record things in a systematic way, which led to the emergency of documentation. Verbal information is limited, but written information can be secured and organized. Documents become more important because they can be easily verified. Before, information was in the form of stories and documents, but today it has become digital or part of AI network.

The naive view is that "*information is an essentially good thing, and the more information we have of it, the better.*" Inventions that have revolutionized human culture, from the printing press to the telegraph to the internet, have not eradicated prejudice or violence .There are many cases where more information has improved the world, comparing child mortality rates from the 18th century to the modern day as a demonstration of a time when the naive view of information proved to be correct. While information is essential, it also has the potential to infringe on privacy. The concept of privacy is not new rather, it has evolved and adapted over time.

Because of technological advancement, privacy has become an important subject of discussion. However, privacy is not a new concept, it has existed throughout history. For example, ancient

legal codes from Greek, Roman and Anglo-saxm[1] civilizations addressed privacy. Aristotles's[2] distinction between the public and private spheres polis (public life) and oikes (private life) is often cited as an early reference to privacy. Modern day privacy as we understand it is approximately 150 years old. Ancient days privacy may be as follows:

- To ensure separate rooms.
- Praying and reading silently.
- People started using single bed.

Even though the ancient codes do not hold any binding authority, nevertheless, the principle enumerated in these codes can be related to the present privacy and data protection issues, particularly in the questions of ownership and responsibilities of data collectors. There are a series of dogmas in the ancient codes, for example, the code of Hammurabi[3], which included principles containing responsibilities for the data controller.

Likewise, the classic "*Hippocratic oath*"[4] contained the privacy statement about their patients. Alan Westin[5] remarked that the desire for privacy is not limited to humans only rather every creature essentially searches for privacy in a small-group intimacy. The ecological studies of Westin exhibited that the scarcity of intimate space may cause huge threats to survival. Adam D. Moore[6] finds that in the absence of intimate personal life, the beasts may destroy them or grossly involve in the suicidal decrease of their population. Westin[7] observes the development of privacy into four different periods-(1945-1960): This is the first phase of privacy. (1961-1979): early age of privacy understanding as the roots of informational privacy were ingrained in this high tech era. (1980-1989): No major changes were taken place about the perception of informational privacy. (1990-2002): Important phase as during the time, privacy has become one of the influential social and political issues in the US and beyond, especially after the incident of 9/11.

The term privacy may find no straightforward indication in either the Hindu literature or the Islamic literature. If we read the dharmshastras, acaras, vedas, smritis and puranas we would

[1] Islam MT and Karim ME, 'A Brief Historical Account of Global Data Privacy Regulations and the Lessons for Malaysia' (2019) 28(2) *Sejarah: Journal of the Department of History, University of Malaya* 169
[2] ibid
[3] ibid
[4] ibid
[5] Alan F Westin, *Privacy and Freedom* (Athenum 1967)
[6] See n 1.
[7] See n 5.

observe that man and women started to incorporate the notion of privacy once they realised what is sacred to them and what they would not like to share with anyone. A great example of their ideology is depicted in their division of separate bathing areas for men and women or imposing restrictions to enter one's property.

Even the bible recognizes this concept and preaches that embarrassment and anger are few of the symptoms of violation of privacy.

The privacy was almost nil from the ancient times to the 19th century, socializing gradually helped people to move out and urbanize in the cities for better mental and physical space and for their personal growth, the cities being crowded led to invasion of this privacy.

In 1890 an article "*The Right to Privacy*" written by Samuel D. Warren and Luis D. Brandeis[8] which gained great fame as it was first of any document to recognise the dangers to privacy due to technological and societal development and from this started of the awakening of the acknowledgment of how to reduce such threats for smooth advocacy of a private life. The period from 2003 to 2019 can also be referred to as a time of technological breakthrough, including social media, Google and wikileaks, and internet of things etc., when the use of personal data are witnessing an unbelievable extension having unprecedented privacy implications.

Privacy is a sweeping concept, encompassing freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. Privacy problems are often not well articulated, and as a result, we frequently lack a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve these problems. Thus the need to conceptualize privacy is significant.

- ***Contemporary Approaches To Privacy Protection***

Privacy is enshrined as a fundamental right in the constitutional law of many countries. Like in India, the right to privacy has been recognized in Justice KS Puttaswamy's case in 2017[9].

[8] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193

[9] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1

According to the Universal declaration of Human Rights of 1948,

"*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.*"[10]

The ECHR of 1950 provides that "Everyone has the right to respect for his private and family life, his home and his correspondence."[11]

Thus, there appears to be worldwide consensus about the importance of privacy and the need for its protection. All the technology available today contains individual data. What the majority of people do not know or try to ignore is the fact that every digital item they possess gathers huge amount of data. The GDPR[12] and DPDP[13] act 2023 were introduced to improve data protection and recognizes their personal data and the need to process such personal data for lawful purposes and for matters connected therewith. Data protection has become important because of the following reasons:

- Globalisation in communication.
- Growing attention on data processing by the government and non government actors.
- Deliberate data sharing on social media.
- Commercialization of data.
- Utilization of cloud computing.
- Privacy as one of the basic human rights

EVOLUTION OF THE RIGHT TO BE FORGOTTEN

"*Nothing fixes a thing so intensely in memory as the wish to forget it*".

\- Michel De Montaigne.

- ***Introduction***

Right to forget involves erasing information that has been publicly known for a certain time and preventing access to it for others. According to E.A, Voynikanis (2016)[14], the attention of the

[10] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) art 12
[11] European Convention on Human Rights (ECHR) art 8
[12] 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 (General Data Protection Regulation) https://gdpr-info.eu/ accessed 20 April 2025
[13] Digital Personal Data Protection Act 2023 (India)
[14] EA Voynikanis, 'The Right to Be Forgotten: Legal Regulation and Its

European community to the right to be forgotten takes place in connection with the existing belief that the Internet, as a technology that allows storing a potentially unlimited amount of information, is a threat to privacy. In the context of this problem, the right to be forgotten is perceived as a certain additional means of controlling the personal data subject over the processing of their personal information in an online environment.

It is safe to say that the analogue age has been mostly forgotten in today's highly digitalised society, when cutting-edge technology are effortlessly interwoven into our everyday lives. The vast majority of people who use the internet either are not aware of the fact that every digital tool or platform they use captures a significant quantity of personal information or choose to ignore it knowingly. To put it simply, our personal information has evolved into a type of currency that we unintentionally exchange for services that are sold to us as being "free." Due to the fact that technology has become so interwoven in our daily routines, we frequently fail to recognise the extent to which it influences us. A privacy campaigner from Austria named Max Schrems made a request to Facebook in 2011 to provide all of the information that the company had saved on him. By the year 2013, he had gotten 1,200 pages that detailed his likes, clicks, relationships, images, and even advertisements that he had already seen. Regardless of whether or not this information was put to use, it was present. Eric Schmidt[15], who was serving as chairman of Google at the time, freely declared, "We know where you are. We are aware of your whereabouts.

To a greater or lesser extent, we are aware of what you are contemplating." The inadequacy of the policies that are now in place to deal with contemporary online dangers is brought to light by such disclosures. As the digital world has progressed, there is an immediate and pressing requirement for law that is both up to date and robust. In the modern era of digital technology, where information can be easily saved, retrieved, and shared all over the world, the concept that "knowledge is power" has taken on a far more profound significance. The clandestine surveillance, the concealed sharing of personal data, and the commercialization of personal data, notably for marketing purposes, highlight the urgent need for better legislative protections. Individuals need to be given the ability to manage the amount of personal information they disclose as well as the sort of information they share in order to accommodate a world in which our identity is increasingly

Theoretical Understanding' (2016) 3 *Jurisprudence* 70

[15] Tereziia Popovych, Mariia Blikhar, Svitlana Hretsa, Vasyl Kopcha and Bohdana Shandra, 'The Right to Be Forgotten as a Special Digital Right' (2023) 15(2) *Law, State and Telecommunications Review* 42

defined by our data. From a normative point of view, privacy is understood to be the right of an individual to deliberately limit their exposure to society, exerting autonomy over their own information for the purpose of protecting their privacy.

- ***Enactment Of General Data Protection Rights***

The General Data Protection Regulation (GDPR) is an example of an effort to bring privacy laws up to date so that they are more comparable to the realities of the current world. In contrast to the previous Directive, it seeks to establish a data protection framework that is uniform throughout the European Union. In addition, it includes a variety of individual rights with the intention of regaining people's authority and control over their personal data. Furthermore, the GDPR presents contentious concerns, particularly in respect to the fundamental right to freedom of expression and information, which is outlined in Article 11 of the Charter of Fundamental Rights of the European Union. Despite the fact that the GDPR is founded on great objectives, it also raises these worries. Businesses will be subject to considerable requirements that could potentially be expensive as a result of the rule. Furthermore, in view of recent developments such as the invalidation of the Safe Harbour agreement[16], the exposures made by Snowden, and the crisis involving Cambridge Analytica, in which the data of more than 71 million Facebook users was hacked, the GDPR needs to be interpreted and enforced with a more global and comprehensive perspective.

The concept of data protection gained momentum after the European court of justice (CJEU) ruling in the case of *Google Spain SL and Goolge Inc. v. Agencia espanola de proteccion de datos (AEPD) and Mario Costeja Gonzalez (2014)*[17]. In this case it was held that individuals had the right to ask search engines like Google to remove links to certain personal information from search results essentially the right to be forgotten.

Later in 2017 European Union passed the General Data Protection Regulation to protect individuals and the data that describes them and to ensure the organisations that collect that data to do so in a responsible manner. Organisations must have a valid legal reason for processing personal data. They must make

[16] Commission Decision 2000/520/EC of 26 July 2000 on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7

[17] *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/12) EU:C:2014:317

it clear exactly how they are going to use their data.

- ***Commencement And Enactment Of The Digital Personal Data Protection Act***

Data protection as a right in India has evolved through time by various judicial decisions, legislative developments, and global influences. Some of the important judgments that helped to shape the data protections laws in India are *K.S. puttaswamy v. Union of India*[18] in this case Supreme court recognized the Right to privacy as a fundamental right under Article 21 of the constitution. This decision laid the foundation for stronger data protection laws in India.

In *Jorawar Singh Mundy v. Union of India*[19] the Delhi High court recognized the potential application of RTBF but did not grant an absolute right to removal.

Though not directly about Right to be forgotten, the Supreme court in *Google v. Sabu Mathew George*[20] directed google and other search engines to remove advertisements related to pre-natal sex determination, indicating that online content removal is possible under Indian law.

Justice Amit Mahajan in *ABC v. State and Others*[21]. states "*there is no reason why an individual who has been duly cleared of any guilt by laws should be allowed to be haunted by the remnants of such accusations easily accessible to the public*". The facts of the case were that a plea was filed in the Delhi High court seeking directions upon the court registry to mask his name from the orders and pleadings filed in a criminal case. The aforesaid proceedings against the man had been quashed and hence he presented himself before the Delhi high court. His counsel argued that irreparable damage would be caused to him and his social life or career prospects would be hampered. He argued that he was entitled to protection under right to privacy and right to forgotten which has been well defined is recognized as a fundamental right. The court directed the removal of the names of both the businessman and the complainant from case records and search results. The court allowed the businessman to approach portals and public search engines to mask the judgment by replacing names with anonymized identifiers. Justice Mahajan emphasized that social media platforms and search engines are expected to honor the principles of the Right to privacy and the

[18] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[19] *Jorawar Singh Mundy v Union of India* WP (C) 3918/2021 (Del HC, 2021)
[20] *Google v Sabu Mathew George* (2018) 3 SCC 229
[21] *ABC v State and Anr* CRL MC 495/2019 (Del HC, 6 November 2024)

right to be forgotten. The court also advised removing any additional material related to the criminal case to protect the privacy of the involved parties.

The above mentioned-cases have contributed to recognize right to be forgotten as a right. Although there are no specific legal provisions explicitly governing the right to be forgotten however, there are laws that indirectly address the right to be forgotten, including the following: The information technology (intermediary guidelines and digital media ethics code) rules 2021[22] provide a process for removing personal information from the internet if it was gathered without consent. The Digital personal data protection act, enacted in 2023[23], acknowledges the right to erasure but does not explicitly address the right to be forgotten**.** The act does not provide a standalone right to be forgotten as seen in the GDPR instead it focuses on data erasure as part of broader data protection rights.

The DPDPA includes provisions for the right to correction and erasure of personal data under section 12[24]. This allows individuals to request the removal of their personal data if the purpose for which it was collected has been fulfilled and it is not required for legal purposes. The act aims to balance individual rights with public interest.it ensures that data erasure requests are considered in light of other rights like freedom of speech and expression, and public interest.

DPDP Act, 2023 in India showcases a significant advancement in data protection efforts, yet it holds certain deficiencies regarding online privacy. One main concern centres on the susceptibility to exploitation or infringement of data privacy due to loopholes or ambiguities within the legislation. These gaps could lead to the unauthorized use of personal information, tracking of data, and the improper utilization of user data on online platforms, as a result endangering individuals' privacy.

The right to be forgotten in EU and the right to erasure in the India share similarities but also have distinct differences in their legal frameworks and applications. The right to be forgotten is not explicitly codified in Indian law but is recognised through judicial interpretations, particularly in the context of the right to privacy under Article 21 of the constitution. The digital protection act 2023 provides for data erasure but does not explicitly address the

[22] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 https://www.meity.gov.in accessed 9 March 2025
[23] Digital Personal Data Protection Act 2023 https://www.dpdpa.in/ accessed 9 March 2025.
[24] Ibid.

right to be forgotten. The right to erasure is explicitly codified in the GDPR providing a clear legal framework for individuals to request the removal of their personal data under specific conditions. The GDPR provides a comprehensive framework with specific conditions for erasure such as when data is no longer necessary for its original purpose or when consent is withdrawn. The enforcement is more uniform across EU member states, on the other hand in India the application of the right to be forgotten is more limited and subject to judicial discretion with varying interpretations across different High courts.

While the Indian courts have acknowledged the need to balance privacy with public interest and freedom of expression the lack of a specific statute means that these balances are often determined on a case by case basis. The GDPR also balances privacy with public interest and freedom of expression but provides clearer guidelines on when erasure requests may be denied such as for journalistic purposes or historical records.

While both India and the EU recognize the importance of allowing individuals to control their personal data the EU's GDPR provides a more comprehensive and explicit legal framework for the right to erasure compared to India's evolving judicial approach to the right to be forgotten.

The DPDPA requires explicit consent from individuals before their personal data can be processed, except in specific cases like state functions or legal obligations. The individuals have the right to access, correct, update, erase, and restrict the processing of their personal data. They can also nominate someone to exercise these rights on their behalf in case of death or incapacity. The Act applies to both online and offline data, including data that is digitized later. It extends to data processing outside India if it involves offering goods or services to Indian residents. Overall, the DPDPA 2023 enhances privacy rights by providing individuals with more control over their data and imposing stricter obligations on data fiduciaries. However, it also presents challenges in balancing privacy with state functions and ensuring compliance across different sectors

CONCLUSION

The evolution of data protection laws, particularly the EU General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 (DPDP Act), signifies a global shift towards recognizing individual autonomy over personal data. Both frameworks acknowledge privacy as a fundamental right and aim to empower individuals to exercise control over their digital identities, particularly through the Right to Be Forgotten (RTBF).

Under Article 17 of the GDPR, the RTBF enables data subjects to request the erasure of personal data when it is no longer necessary, when consent is withdrawn, or when the data has been unlawfully processed. This provision emerged prominently in the landmark *Google Spain* case, where the Court of Justice of the European Union affirmed individuals' rights to request delisting of search results that infringe their privacy, balancing it with the public's right to information. The GDPR's structured approach to RTBF integrates clear grounds for erasure, procedural obligations for controllers, and exceptions to protect freedom of expression, public interest, and legal compliance. Its practical application across EU jurisdictions has set a benchmark for how digital rights can coexist with other societal interests, including transparency and accountability.

The DPDP Act, while inspired by the GDPR, adopts a narrower formulation of RTBF under Section 12, allowing data principals to request the erasure of their personal data and de-listing from public access when the purpose of data processing is no longer served, consent is withdrawn, or the retention period has expired. However, the implementation of RTBF under the DPDP Act is contingent upon the adjudication by the Data Protection Board of India, adding a layer of regulatory oversight absent in the GDPR's model. This may address concerns around potential misuse of RTBF to suppress legitimate speech but may also slow down the exercise of the right by data principals in practice.

The challenges of enforcing RTBF are significant in both frameworks. On the one hand, it is a powerful tool to protect individuals from perpetual digital harm, reputational damage, and psychological distress caused by outdated or irrelevant data. On the other, it raises tensions with freedom of expression, the right to information, and the operational realities of the digital ecosystem where data replication and cross-border transfers are ubiquitous. The GDPR's nuanced exceptions and balancing tests can guide India in shaping its jurisprudence on RTBF under the DPDP Act, ensuring proportionality in requests for erasure while respecting journalistic freedom and public interest.

Further, RTBF under the DPDP Act requires robust procedural clarity, clear definitions of 'public interest', and effective mechanisms for stakeholders to challenge or defend erasure requests. As Indian courts, following *Justice KS Puttaswamy* and cases like *Jorawar Singh Mundy*, continue to interpret digital privacy rights, the DPDP Act's RTBF provisions will require harmonization with constitutional principles, evolving global practices, and India's socio-legal context.

However, the GDPR offers a matured framework for operationalizing RTBF, the DPDP Act provides a promising but cautious start in India's privacy regime. The effective realization of RTBF will require a fine balance between individual privacy, technological realities, and societal interests, ensuring that the digital landscape respects the dignity and autonomy of individuals without undermining the collective right to information.