DATA PRIVACY AND THE RIGHT TO BE FORGOTTEN IN INDIAN JURISPRUDENCE

Arundhati Chatterjee, Presidency University, Bangalore

ABSTRACT

This article delves into the intricate dynamics of the Right to be Forgotten within the framework of Indian jurisprudence, exploring its intersection with data privacy, freedom of expression, and the emerging digital landscape. It critically examines the Right to be Forgotten's evolution following the landmark judgment in K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors, which recognised the right to privacy as a fundamental right under Article 21 of the Indian Constitution. The article also provides a comparative analysis of international frameworks, especially the European Union's General Data Protection Regulation (GDPR), and evaluates India's approach through the proposed Digital Personal Data Protection Act, 2023 (DPDP Act). It further discusses the challenges in implementing the Right to be Forgotten, such as potential conflicts with freedom of speech under Article 19(1)(a) of the Constitution of India, 1950, and the practical complexities of data erasure. The article concludes by emphasising the need for a balanced, context-driven approach that ensures privacy protection without undermining democratic values like freedom of expression and public interest.

Keywords: Data Privacy, Digital Personal Data Protection Act, 2023, Freedom of Expression, Indian Jurisprudence, K.S. Puttaswamy Case, The Right to be Forgotten

I. INTRODUCTION

In today's digital age, the concepts of data privacy and the "*Right to be Forgotten*" have gained unprecedented significance, shaping the discourse on individual autonomy and informational self-determination. Data privacy pertains to the protection of personal information collected, stored, and processed by various entities, ensuring that such data is not misused or accessed without consent. In contrast, the right to be forgotten grants individuals the ability to request the removal of their personal data from online platforms, search engines, and databases, allowing them to control the dissemination of their personal history.[1]

The importance of these concepts is especially pronounced in India, where the exponential growth of digital platforms and the pervasive use of technology have led to increasing concerns about the misuse and unauthorised sharing of personal data. The landmark judgment of Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.[2], wherein the Supreme Court recognized the right to privacy as a fundamental right under Article 21[3] of the Indian Constitution, set the foundation for data protection and raised pertinent questions regarding the extent to which the right to be forgotten should be incorporated into Indian jurisprudence.[4]

Given this backdrop, the objective is to critically analyse the status of data privacy and the right to be forgotten within the Indian legal framework, examining the existing laws, landmark judgments, and ongoing debates. It will delve into how the right to be forgotten aligns or conflicts with fundamental rights such as freedom of speech and the right to information, and whether Indian law is equipped to balance these competing interests. Additionally, the article will explore how international frameworks, such as the European Union's General Data Protection Regulation (GDPR), can provide insights for evolving Indian jurisprudence. This exploration seeks to offer recommendations for a balanced legal framework that upholds individual privacy without compromising societal interests.

II. UNDERSTANDING DATA PRIVACY AND THE RIGHT TO BE FORGOTTEN

Data Privacy refers to the protection of personal information that individuals share with various entities, such as government bodies, private companies, and online platforms. It involves

[1] A.H. Robertson, "Privacy and Human Rights", Manchester University Press, 1972.
[2] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors*., [2019] (1) SCC 1.
[3] The Constitution of India, Article 21.
[4] Arthur R. Miller, "The Assault on Privacy" (The University as Michigan Press, 1971).

ensuring that such data is collected, processed, and stored with consent and in a manner that prevents unauthorised access, misuse, or breaches. In India, the significance of data privacy has gained momentum following the landmark judgment in Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.[5], where the Supreme Court unequivocally recognised the right to privacy as a fundamental right under Article 21 of the Indian Constitution. This ruling laid down the foundation for a broader conversation around safeguarding personal data in a digital era increasingly marked by data mining, profiling, and surveillance.[6]

The concept of the Right to be Forgotten is a relatively recent but vital extension of data privacy. The right to be forgotten allows individuals to request the removal or de-indexing of personal information from online platforms, search engines,[7] or databases, especially when such information is outdated, irrelevant, or potentially damaging. The essence of this right lies in granting individuals control over their digital footprint, enabling them to prevent the permanent availability of certain aspects of their personal history. In X v. Union of India (2017), the Karnataka High Court recognised the right to be forgotten for the first time, ordering the removal of a woman's name from a judgment to protect her identity and reputation. This case demonstrates India's nascent but evolving acknowledgement of the right to be forgotten.[8]

Global Context: The most comprehensive and explicit acknowledgement of the right to be forgotten can be found in the European Union's General Data Protection Regulation (GDPR). Article 17 of the GDPR enshrines the "Right to Erasure," granting EU citizens the right to request the deletion of personal data when it is no longer necessary, has been unlawfully processed, or if the data subject withdraws consent. The landmark case Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (2014) by the Court of Justice of the European Union (CJEU) was pivotal in establishing the right to be forgotten, requiring search engines to remove links containing personal data upon legitimate request.

In contrast, countries like the United States have been reluctant to embrace the right to be forgotten due to their emphasis on freedom of speech and the First Amendment. Here, the tension between individual privacy and the public's right to access information has been a significant barrier to implementing the right to be forgotten. As India drafts its data protection

[5] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.,* [2019] (1) SCC 1.
[6] Brien M.O. David, "Privacy Law and Public Policy", Published by Praegar Publication New York 1979.
[7] Basu D.D., "The Constitutional Law of India" Princeton University Press 3 Edition 1983.
[8] Boderin. A. Mashood, "International Human Rights and Islamic Law" Oxford University Press 2003.

laws, these international frameworks provide crucial insights into balancing privacy rights with other fundamental freedoms, making it imperative to craft legislation that respects individual autonomy while upholding transparency and accountability.[9]

III. LEGAL FRAMEWORK OF DATA PRIVACY IN INDIA

A. Constitutional Basis

The right to privacy in India found its strongest affirmation in the landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India, where a nine-judge bench of the Supreme Court unanimously declared the right to privacy as an intrinsic part of the fundamental rights guaranteed under Article 21 of the Indian Constitution. The court held that privacy is an integral part of the right to life and personal liberty, stating that every individual has the right to control their personal information.[10] This judgment laid the foundation for the legal protection of data privacy and set the stage for further legislative and judicial developments in this domain. The court, while recognising the need for data protection, emphasised that the right to privacy is not absolute and must be balanced against legitimate state interests and the public good.

B. Existing Laws

Currently, India's legal framework on data privacy is primarily governed by the Information Technology Act, 2000 (IT Act) and its accompanying rules, particularly the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Section 43A[11] of the IT Act mandates that anybody corporate handling sensitive personal data must implement reasonable security practices and compensate for any wrongful loss or gain resulting from a data breach. The Act defines "sensitive personal data" to include details such as passwords, financial information, medical records, and biometric data, among others.

Moreover, Section 72A[12] of the IT Act penalises individuals who disclose personal information without consent, imposing imprisonment of up to three years or a fine. Despite these provisions, the IT Act lacks comprehensiveness and specificity regarding data protection standards, rights,

[9] Bonnett John Colin and Roab D. Charles, "Policy Instruments in Global Perspective", ed. (2003).
[10] Chaubey R.K. "An introduction to cyber crime and law", 2009 reprint.
[11] Information Technology Act, 2000, Section 43A.
[12] Information Technology Act, 2000, Section 72A.

and remedies, often rendering it inadequate in addressing contemporary challenges related to data privacy.

C. Data Protection Act

To address these shortcomings, the Government of India introduced the Digital Personal Data Protection Act, 2023, which replaced the earlier versions of the data protection framework and brought the country's laws in line with global standards. This Act represents a comprehensive attempt to establish a legal framework for the protection of personal data in India, akin to the GDPR in the European Union.[13]

The Act introduces the concept of Data Principals (data subjects) and Data Fiduciaries (entities processing data), granting Data Principals rights such as the right to access, correct, transfer, and erase their personal data. Significantly, Clause 20 of the Act expressly addresses the Right to be Forgotten, allowing individuals to request the removal or restriction of access to their personal data when it is no longer necessary, unlawfully processed, or consent has been withdrawn. This provision empowers an individual to approach the Data Protection Board, which the Act proposes to establish as an adjudicatory body for resolving such disputes.[14]

However, the right to be forgotten is not absolute under the Act and is subject to certain limitations, including the public interest, the right to freedom of speech, and the maintenance of transparency. For instance, the retention of certain information may be warranted to comply with legal obligations or serve larger public interests, ensuring a balanced approach between privacy rights and other competing rights.

The Act also prescribes hefty penalties for data breaches, unauthorised processing, or failure to implement adequate security measures, reflecting the growing need to enforce data protection standards stringently. Despite its progressive stance, concerns have been raised about the potential for government exemptions from certain obligations, which could impact the effectiveness of data privacy protection.[15] While India's legal framework on data privacy is evolving, the emerging legislation, alongside judicial recognition, signifies a growing acknowledgement of the right to privacy and the right to be forgotten. These developments

[13] G. S. Bhargava, "Scoop Based on Phone-Tapping," Mainstream, 1996, pp. 19-20.
[14] Geoffrey Marshall, "The Right to Privacy - A Sceptical View," Mc. Gill LJ.
[15] Harbert Marcuse, One Dimensional Man, (1964).

mark a crucial step toward establishing a robust data protection regime, aligning India with international standards while catering to its unique socio-legal landscape.[16]

IV. JUDICIAL INTERPRETATION OF THE RIGHT TO BE FORGOTTEN IN INDIA

The Right to be Forgotten in Indian jurisprudence, while not explicitly codified in current legislation, has found recognition through a series of judicial pronouncements. The evolution of this right can be traced through landmark judgments, which have sought to balance the right to be forgotten with competing fundamental rights, such as the freedom of speech and the right to information.[17]

A. Key Case Laws

1. Justice K.S. Puttaswamy (Retd.) v. Union of India:

This landmark judgment by the Supreme Court of India played a pivotal role in shaping the discourse on the right to be forgotten. In this case, a nine-judge bench recognised the right to privacy as a fundamental right under Article 21 of the Indian Constitution. While the court did not explicitly mention the right to be forgotten, it laid the groundwork for it by recognising the individual's autonomy over personal data and the right to control its dissemination. The judgment emphasised that privacy encompasses the right to be left alone, which, in effect, hints at the possibility of erasing personal data in certain contexts.

The Supreme Court acknowledged that informational privacy is a critical aspect of an individual’s dignity, thus providing the foundational argument for the right to be forgotten. However, it also highlighted the need to balance this right with other societal interests, such as transparency and the freedom of the press.

2. X v. Union of India:

The Karnataka High Court was the first to directly address the right to be forgotten in India in this case. Here, the petitioner, a woman who had been acquitted of all charges in a criminal case, sought the removal of her name from court records available online. She argued that

[16] HigToss, "The Concept of Privacy", (1967) 2 Univ. of Ras. L.R. 418.
[17] Govind Mishra, "Privacy as Public Issue", Vidhura,June, 1981.

continued online availability of her details caused significant hardship and emotional distress, despite her acquittal. The High Court, recognising her right to privacy, ordered the redaction of her name, marking a significant acknowledgement of the right to be forgotten in Indian jurisprudence. This judgment was a pioneering step toward recognising the individual's right to disassociate themselves from events that might unduly stigmatise them, even after the legal process exonerated them.

3. Subhranshu Rout @ Gogul v. State of Odisha[18]:

In another notable case, the Orissa High Court took cognisance of the right to be forgotten. The petitioner, accused of sexually explicit acts, sought the removal of all references to him in the court orders available online. The court observed that the presence of his name could tarnish his reputation, despite the case being sub judice. The High Court acknowledged the need to protect individual privacy but refrained from granting complete anonymity, thereby indicating that the right to be forgotten must be balanced with the public's right to access judicial proceedings.

4. Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.[19]:

In this case, the Delhi High Court granted an interim injunction restraining the publication of articles that were found to infringe on the petitioner’s right to privacy. The Court noted that the right to be FORGOTTEN is intrinsic to the right to privacy, particularly when the dissemination of such information could have a long-lasting impact on an individual's reputation. Although the Court refrained from issuing a final order, it recognised that the right to privacy could necessitate the removal of content in certain circumstances, thus reinforcing the legitimacy of THE RIGHT TO BE FORGOTTEN within Indian legal discourse.

B. Challenges and Ambiguities

Despite these judicial acknowledgements, the implementation of the right to be forgotten in India is fraught with challenges and ambiguities. One of the primary challenges lies in balancing the right to be forgotten with the right to freedom of speech and expression under Article 19(1)(a) of the Indian Constitution. The right to be forgotten, if exercised

[18] *Subhranshu Rout @ Gogul v. State of Odisha,* [2020] SCC OnLine Ori 878.
[19] *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.,* [2019] SCC OnLine Del 8494.

unconditionally, could lead to the erasure of public records and potentially infringe on the public's right to know. For example, information that holds significant public interest, such as details about political figures, public authorities, or criminal activities, could be unjustifiably removed under the guise of the right to be forgotten.[20]

The right to information (RTI) under Article 19(1)(a)[21] further complicates the landscape, as it emphasises transparency and accountability, particularly concerning public figures or public records. The conflict between the Right to be Forgotten and RTI becomes evident when individuals seek the removal of information that may be crucial for public awareness, historical records, or matters of public safety.[22]

Another ambiguity lies in determining the scope and application of the right to be forgotten. Unlike the European Union's GDPR, which explicitly outlines the circumstances under which personal data can be erased, India lacks a statutory framework to guide its application. For instance, should the right to be forgotten be limited to search engine de-indexing, or should it extend to the removal of personal data from websites, databases, and social media? Indian courts have yet to provide a clear, uniform standard for such applications. Further, questions arise regarding jurisdictional enforcement, particularly in a digital world where data crosses borders effortlessly. In an era of transnational data storage, implementing the right to be forgotten would require not just national enforcement but international cooperation, a challenge not easily surmountable given the lack of consensus on privacy norms across countries.[23]

Indian courts have made significant strides in acknowledging the right to be forgotten; its implementation remains in a nascent stage, with numerous challenges ahead. The absence of comprehensive legislation on data protection means that much of the right to be forgotten's future in India will depend on evolving judicial interpretations and the eventual enactment of laws that balance privacy rights with the public's right to access information.[24] The need for a nuanced, case-specific approach is evident, ensuring that while the Right to be Forgotten is respected, it does not unduly infringe upon democratic principles of transparency and free

[20] I. P. Messey, "Constitutionalization of the Right to Privacy in India," in BPS Sehgal (ed.) Human Rights in India, (1995).
[21] The Constitution of India, Article 19(1)(a).
[22] Janusz Symonides, Human Rights Concepts and Standards, (2000).
[23] Jagdish Swamp, Tagore Law Lectures : Human Rights and Fundamental Freedoms, (1975).
[24] K. Pattibhi Rama Rao, "Right to Privacy : A New Fundamental Right," Andhra Law Times, 1999, Vol. 2, pp. 16-18.

speech.

V. COMPARATIVE ANALYSIS WITH INTERNATIONAL JURISPRUDENCE

A. European Union's General Data Protection Regulation (GDPR)

The European Union's GDPR stands as the most comprehensive legal framework for data privacy, explicitly recognising the Right to be Forgotten under Article 17[25]. This empowers data subjects to request the erasure of their personal data when it is no longer necessary for the purposes for which it was collected, or if consent has been withdrawn, among other conditions. One of the most significant cases that solidified the right to be forgotten in the EU is Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos [26](2014), popularly known as the "Google Spain" case.

In this landmark judgment, the Court of Justice of the European Union (CJEU) held that individuals have the right to request search engines to de-index links containing personal information if it is outdated, irrelevant, or excessive. The CJEU emphasised that the right to privacy outweighs the public's interest in accessing such information unless there is a legitimate reason for its retention. This decision imposed a legal obligation on search engines, making them 'data controllers' responsible for processing personal data in compliance with GDPR, thereby reinforcing the right to be forgotten as a fundamental aspect of data privacy.[27]

B. Approach of the United States

Contrary to the EU's approach, the United States does not have a codified Right to be Forgotten, largely due to its robust protection of the freedom of speech enshrined in the First Amendment of the U.S. Constitution. The U.S. legal system prioritises the right to free expression and public access to information over individual privacy concerns, even if it involves personal data. The absence of a centralised data protection law akin to the GDPR means that the right to be forgotten is not formally recognised within the American legal landscape.

In cases like Melvin v. Reid [28](1931), courts have, however, acknowledged the need to protect

[25] The Constitution of India, Article 17.
[26] *Google Inc. v. Agencia Española de Protección de Datos*, Case C-131/12.
[27] P. V. Kane, History of Dharamshastra, (1968).
[28] Melvin v. Reid, 112 Cal.App. 285, 297 P. 91 (1931).

individual reputation against the publication of private information. Despite this, U.S. jurisprudence typically leans towards transparency and upholding free speech, making it challenging for individuals to exercise any form of the right to be forgotten. The U.S. approach underscores the notion that once information enters the public domain, it becomes difficult to restrict its dissemination, reflecting a clear divergence from the EU's stance.

C. Indian scenario

India has formalised its data protection laws through the Digital Personal Data Protection Act, 2023, and has drawn valuable insights from these international models. The EU's GDPR offers a comprehensive and enforceable framework that balances individual privacy rights with public interest, something that Indian jurisprudence can adapt, ensuring clarity in the scope and application of the right to be forgotten. Simultaneously, the U.S. model serves as a reminder of the importance of protecting free speech, cautioning against the unrestrained use of THE RIGHT TO BE FORGOTTEN that could impede the right to information and expression.[29]

India's challenge lies in crafting a balanced approach that recognises the right to be forgotten while safeguarding democratic values, ensuring that data privacy laws effectively address individual rights without compromising on transparency and freedom of expression. This comparative analysis highlights the need for nuanced legislation, tailored to India's unique socio-legal environment, to create a framework that upholds both privacy and public interest.

VI. CONCLUSION

The evolving landscape of data privacy in India, particularly the Right to be Forgotten, underscores the nation's efforts to strike a balance between individual privacy and the broader societal need for transparency. The absence of a clear legal framework in India has created ambiguity, leading to inconsistent interpretations by courts. However, landmark judgments such as K.S. Puttaswamy v. Union of India have laid a foundational emphasis on privacy as a fundamental right, signalling a shift toward recognising the right to be forgotten as a legitimate claim.[30]

[29] Philip, Hanon, "From Politics to Reality : Historical Perspective of the Legal Service Corporation," 25 Emory Law Journal, 639-54 (Summer, 1976).
[30] R. Shamasastri, Kautilya's Artashastra, (1961).

Despite this progress, implement the right to be forgotten.[31] in a manner that aligns with the principles of freedom of expression and public interest remains a formidable challenge. The proposed Digital Personal Data Protection Act, 2023, attempts to address this gap, but it requires a more nuanced and well-defined structure to avoid conflicting with constitutional freedoms and the public's right to know. In conclusion, India's journey toward establishing a comprehensive right to be forgotten framework is a work in progress that necessitates a delicate balance. Ensuring that the right to privacy coexists with freedom of speech and access to information is paramount. Such an equilibrium will pave the way for a robust data privacy regime that respects individual autonomy without compromising democratic values.

[31] Richard Hixson, "Privacy in a Public Society : Human Rights in Conflict" (1987).