

In the Digital Age, the Right to be Forgotten: A Comparison of the Indian Personal Data Protection Act of 2018 and the GDPR

Srijit Nair*

Abstract

The term "right to be forgotten" refers to the legal right to be forgotten. Individuals have the right to have misleading, embarrassing, irrelevant, or obsolete personal information on the Internet erased, limited, delinked, removed, or amended. The European Court of Justice's ruling in the Google Spain case, which established it as a matter of EU law, brought this legal right to the fore. This "right" has existed in many forms around the world and is frequently based on a balance-of-rights analysis of the right to privacy vs. the right to free expression. In contrast, the new European version is based on a legal principle known as intermediary liability, which claims that Internet search engines are now deemed "data controllers" and, as such, are accountable for some online content management. This entitlement has brought attention to basic policy considerations as well as practical implementation challenges under the new European regime as it has evolved across Europe. Data protection necessitates extreme caution and care, not only because personal information is sensitive, but also because it is valuable. Individual information is collected. By far, the most important feature is the human right to privacy. Indian authorities have begun to look at data protection due to the country's reliance on the internet and technologically advanced equipment. The phrase "privacy" should not be confused with this. Protectionism and data security are terms that are used around the world. In a number of well-known texts, such as the Treaty on the Functioning of the European Union and the European Union's Fundamental Rights Charter. The European Union took a step forward by giving data protection legal significance with the 1995 Directive. Despite this, India is the world's largest IT services market and one of the largest IT service providers. It was possible to get help. Regrettably, Indian citizens are not treated with the same respect as European citizens. Topics are provided by legislators, but the Indian Supreme Court paved the way. Personal data protection must be recognized as a fundamental right. The 'Personal Data' section of the 2018 Protection Bill, on the other hand, is considered a detailed investigation into the concept of privacy. Data security is also crucial, especially when it comes to the "right to be forgotten".

Keywords: Right to be forgotten, right to erasure, GDPR, Indian data protection bill, 2018, privacy, data protection

*Author for Correspondence

Srijit Nair

E-mail: srijit.nair@law.christuniversity.in

Student, CHRIST (Deemed to be University), Delhi NCR,
Nandgram Rd, Marium Nagar, Sewa Nagar, Ghaziabad, Uttar
Pradesh, India

Received Date: May 02, 2022

Accepted Date: November 05, 2022

Published Date: December 10, 2022

Citation: Srijit Nair. In the Digital Age, the Right to be Forgotten: A Comparison of the Indian Personal Data Protection Act of 2018 and the GDPR. National Journal of Cyber Security Law. 2022; 5(2): 1–6p.

INTRODUCTION

We live in a digital age, where data storage, retrieval, and electronic information's global reach are normal, and the phrase "knowledge is power" has taken on new meaning. Because of clandestine monitoring, undeclared transfers, and the monetization of personal data through marketing, people want and demand greater regulatory measures. In the age of the World Wide Web, it is difficult to fully forget material posted on the Internet. While this data can be utilized for a variety

of purposes, if it is mishandled, it can be harmful to data subjects. Without the agreement of the interested party's reputation or intended use of unsolicited and unlicensed material on the Internet may have harmful consequences. Minor humiliation to social antagonism and melancholy are examples of undesirable outcomes. Because privacy cannot be guaranteed from the start, people must be able to remove information that has already been acquired. India's present data protection law, which does not recognize an individual's "right to be forgotten", is governed by the Information Technology Act of 2000 and its articles. The Personal Data Protection Bill: 2019 PDP Bill, based on the Report of the Justice B. N. Srikrishna Committee, finally intends to provide statutory protection to this right after much debate and judicial inconsistencies. Thanks to the PDP Bill, this is now officially recognized.

HISTORY

The European Court of Justice introduced a new right known as the "right to be forgotten" in a 2014 judgement, which allows data subjects to request that personal data or content posted on the internet be removed from online databases. It was implicitly recognized as a right for the first time in the 1995 European Union Directive on Data Protection. In 2016, the European Union established a new General Data Protection Regulation, which includes an express right to be forgotten and is expected to produce results in 2018. Although it has been criticized for infringing on freedom of expression, this right is founded on privacy and data protection principles. The right to be forgotten has been warmly received by the public; but, in the current situation, the critiques and worries about such a right remain relevant. It immediately opposes both the right to know and the freedom of speech of the people. This is particularly true in the United States, where the right to free expression and the rejection of censorship are both core beliefs. Many people also criticize the right, stating that it is meaningless because most countries already have defamation and libel laws in place. Neither the judiciary nor the legislature in India have taken a strong stance on the issue. Despite widespread recognition of the right to privacy judgement, important issues remain unresolved in the wake of India's drive to digitize sensitive data such as credit histories, biometrics, and other personal information. As a result, the goal of this study is to compare and contrast the right to be forgotten law emerging from a historic ruling by the European Union's Court of Justice on the creation of the EU's General Data Protection Regulations. The Personal Data Protection Bill 2018 presented by the Justice BN Srikrishna Committee incorporates another right known as the option to be neglected, which alludes to a singular's capacity to restrict, delink, eliminate, or correct the exposure of misleading, humiliating, or insignificant individual data on the web. Section 27 of the Bill states that it shall only be on the basis of a written request to the data fiduciary accompanied by reasonable information sufficient to satisfy the data fiduciary of the identity of the data principal making the request, and the data fiduciary shall acknowledge receipt of such request within the time period specified. Section 27(2) also states that the adjudicating officer (Data Protection Authority) must rule on the issue of disclosure as well as the conditions in which he believes such disclosure can trump citizens' right to free speech and information. The right to be forgotten is analogous to the right to privacy, which was recognized by the Supreme Court in the Puttaswamy case as an inherent aspect of Article 21 (right to life) of the constitution.

IMPORTANT FEATURES OF A BILL

Because the draught Bill is still in the executive branch and the European Union General Data Protection Regulation (GDPR) has emerged as the spearhead of data protection operations, it is preferable to consider the former in the context of the latter. Anatomic or root level investigation of basic title and provision, as well as the scanning orientation of the powers that be, will be the focus of the inquiry. The Bill's Section 27 addresses the all-powerful 'right of data principle', while the data 'fiduciary' is pulled into the final devoir of obligation. While compliance is not the most important aspect of data protection law, it is critical. What matters is that compliance is achieved, not what a data fiduciary's responsibilities are or how they should be carried out in order to fulfil them. Anatomic or root level investigation of basic title and provision, as well as the scanning orientation of the powers that be, will be the focus of the inquiry. Consider Subsection (1) of Section 27, which allows the data principal the right to limit or prohibit a data fiduciary from releasing personal information that has

already been provided with lawful authorization for a specific purpose. Subsection 2 restricts the scope of the privilege granted in the previous subsection (2).

Section 27 deals with two independent but related legal terms: 'restrict or prevent' and 'continuous disclosure' (1). 'Because this Bill would establish India's fundamental legal framework for data protection, we must also consider the practical implications of these two statements while keeping Section 27's simple title in mind.'

This concept has two elements in the context of data protection.

The first section focuses on further processing or profiling of personal data, while the second section discusses current personal data with the data fiduciary.

As a result, in this case, the provision has a double effect. Under subsection (1), the data fiduciary is barred from making continuous disclosures, and he should cease doing so after receiving a request in this regard. It should be stressed that, at least for the time being, we will not be addressing the clashing interests of the data principal's right to privacy and others' freedom of speech and expression. The Committee deviated from the genuine meaning established by EU legislators and the European Union Court of Justice in its report to the Indian government. In its report, the Committee constrained itself by attempting to link the right to be forgotten with an individual's ability to delete information (it merely means that the term "be forgotten" should be made anonymous to refer to the permanent erasure of data). When the Bill defines data fiduciaries in Section 3, it refers to both individuals and entities as data fiduciaries. In the report, the committee attempted to describe the right to be forgotten in only two ways. 'There is no conceptual reason why the data principal's unfairness judgement should prevail over the fiduciary's', the committee adds, but it does not specify what this 'principled rationale' is '...the spread of information may become extremely difficult to avoid in the event of a direct or subsequent public revelation of personal data'. According to the text, the objective of a publication often involves topics of public interest, and whether or not the disclosure is needed "may depend on the level of such public interest". The committee relied largely on criticisms of the Google Spain case judgement from the House of Lords, Justice Committee, and European Union Committee, but failed to cite the Google Spain case, which popularized the word "be forgotten" as a synonym for "erasure".

The Google Spain case is critical to understanding the jurisprudence of the right to "be forgotten", as well as the Committee's overall approach in this regard. A Spanish person protested to the Spanish Data Protection Authority (AEPD), as well as Google Spain and Google Inc., about a Catalan newspaper. When a user types in the name 'Mr. Costeza Gonzalez', he is directed to two pages of news headlines about a real-estate auction being held against him to recover the debt. Surprisingly, the story was first published in 1998, but the case was not filed until several years later. Mr. Gonzalez sought two immediate remedies in his complaint: one against the newspaper and the other against Google Spain & Google Inc. In response to the theories in the Sri Krishna Committee report, it would be good to present some verifiable facts about this topic, including the logic behind Google Spain's decision. The committee was unable to find any rational foundation for the data principal's personal assessment of unfairness having a greater influence than the fiduciaries in severing the conflicting legal framework when establishing its malicious suspicions. With all due deference to 'principled reasoning', the first line of thought would be fiduciary checks and balances on economic benefits and the means to obtain them, for example. In the Indian Data Protection Bill, a "data fiduciary" is defined as someone who has control over a natural person's personal data or with whom the natural person shares data. Businesses, firms, and other similar institutions that gather personal data for professional or commercial purposes are known as data fiduciaries.

Market stability is followed by market stability, which includes fostering a respect for competition law issues, a purpose-centric consent system, lawfulness and location of processing, respect for citizens' fundamental rights, and so on.

INDIAN PERSPECTIVE

In India, the right to be forgotten is yet unprotected by law. In Puttuswamy, however, the Supreme Court ruled that the right to privacy is a fundamental right. The Supreme Court concluded in the Puttaswamy case that an individual's "right to exercise control over his personal data and to be able to manage his or her own life" includes the "right to control his or her own existence on the Internet". Many High Courts have now explicitly recognized the right to be forgotten in their judgments, using international jurisprudence. A simple Google search could reveal a wealth of information on someone, compromising their reputation and dignity, as provided by Article 21 of the constitution. At a time when the judiciary is launching Phase III of its ambitious E-courts effort, rights like the right to be forgotten must be integrated into any technology solution designed for judicial data storage and management. On the 'Right to be Forgotten', the Gujarat High Court and the Karnataka High Court have taken opposite positions. In Dharamraj Bhanushankar Dave v/s State of Gujarat & the Gujarat High Court dismissed any such privilege. In this case, the petitioner filed a writ petition under Article 226 of the Constitution, asking the court to limit public exposure of a Hon'ble Court judgement dated October 30, 2007, which the respondent had published on the internet. The petitioner alleged that he was falsely accused of criminal conspiracy, murder, and other serious crimes. According to the Jamnagar Police Station, a report was submitted. The petitioner was eventually released by the Sessions Court, which was then upheld by the Gujarat High Court Division Bench. Despite the fact that the judgement was not made public, the respondent made it available on the internet, causing the petitioner's personal and professional life to be disrupted. The Gujarat High Court ordered that copies of the High Court's judgement could be provided to any party on the Assistant Registrar's authority. The Gujarat High Court also found that the petitioner had failed to show any violation of Article 21 of the Constitution, and hence the court did not recognize the 'Right to be Forgotten'. In the matter of Sri Vasunathan v/s The Registrar General & Ors, the Karnataka High Court acknowledged the 'Right to be Forgotten' on January 23, 2017. The petitioner asked that his daughter's identity be removed from a digital record of an order dated June 15, 2015. The verdict came after the petitioner's daughter filed a complaint against a guy for allegedly pressuring her to marry, forgery, and other offenses [1–5]. They also filed a civil suit to have their marriage certificate nullified, claiming that they were never lawfully married. After then, the parties reached an arrangement in which the petitioner's daughter agreed to abandon the father's criminal charges. As a result, the individual filed a motion under Section 482 of the Code of Criminal Procedure, 1973, to have the above-mentioned FIR quashed, which was granted by the Humble High Court in an order dated June 15, 2015.

The petitioner's daughter was designated as respondent no. 2 in the order, along with her name and identifying details. The petitioner argued in court that a name-based search on Google, Yahoo, and other search engines could result in the order dated June 15, 2015, being posted on the result page. The order dated June 15, 2015, could appear on the result page of Yahoo and other search engines.

Furthermore, the aforementioned injunction could jeopardize his daughter's connection with her spouse as well as her public image.

The Karnataka High Court, in a judgement dated June 15, 2015, ordered respondent to take the steps necessary to mask the name of the petitioner's daughter, taking into account the petitioner's reasons and recognizing the "Right to be Forgotten". If a certified copy of the aforementioned order is requested, the petitioner's name must be included [6–10].

"This would follow the trend in Western countries, where the "Right to be Forgotten" is used as a rule in delicate situations affecting women in general, as well as particularly sensitive cases such as rape or injury to an individual's modesty and reputation..."

This can be shown in situations where a rape victim has the right to have her past forgotten, while a criminal does not. The Data Protection Authority must decide whether to keep (right to information) or delete (right to be forgotten) online data (right to be forgotten). Because a journalist must wait for the

adjudicating officer's decision, the right to be forgotten may pose a threat to press freedom. As a result, criticizing public figures for their policies based on previous statements and actions will be limited; it is also possible that a citizen requesting such information is unsure whether to approach the Central Information Commission or the Data Protection Authority.

The state retains unrestricted right to gather and analyze data without the need for consent in the sake of national security [11, 12]. On the other hand, the national interest is never defined, leaving the application of the right to be forgotten to the government's discretion.

The right to be forgotten may meet with public records issues, posing a legal hurdle. Judgments, for example, have always been regarded as public papers and fall under Section 74 of the Indian Evidence Act of 1872's definition of a public document. Right to Access Official Public Records (RTBF) cannot be extended to official public records, including court records, according to a report issued by the Vidhi Centre for Legal Policy, because doing so would weaken public faith in the judicial system over time. Information in the Public Domain: It is like toothpaste in the digital era, material that has been released into the public domain cannot be taken back. What is the difference between an individual and a society?

The right to be forgotten creates a tension between individuals' right to privacy and society's right to knowledge and press freedom.

CONCLUSION

Creating a Reasonable Restriction on Privacy: In order to implement the right to be forgotten, a significant revision to the Constitution must include privacy as a criterion for justifiable restriction under Article 19.

How to Strike a Balance between Privacy and Data: As a result of framework development, the right to be forgotten may be reduced. Completing a project in the public interest or for the sake of public health; according to legal requirements; archiving for public good, scientific or historical study, or statistical purposes; or Claims are created, exercised, or defended in the legal system.

To make the right to be forgotten a reality, a significant constitutional change is required to include privacy as a justification for restriction under Article 19 of the Constitution. On the one hand, a balance must be struck between internet users' right to privacy and personal data protection (as guaranteed by Article 21 of the Indian constitution) and their freedom of information (as covered by Article 19). A comprehensive data protection law must address these concerns while avoiding conflicts between India's golden trinity of fundamental rights (Articles 14, 19, and 21). A complete debate is essential, given that the Personal Data Protection Bill 2019 has already been introduced in parliament.

REFERENCES

1. Swiss S, Jennings PJ, Aryee GV, Brown GH, Jappah-Samukai RM, Kamara MS, *et al.* Violence against women during the Liberian civil conflict. *JAMA*. 1998; 279(8): 625–9.
2. Solveig Vatnar, Stål Bjørkly. Victim of and Witness to Violence: An Interactional Perspective on Mothers' Perceptions of Children Exposed to Intimate Partner Violence. *Violence Vict*. 2011 Dec; 26(6): 830–52. Researchgate.net. Available from: https://www.researchgate.net/publication/221789673_Victim_of_and_Witness_to_Violence_An_Interactional_Perspective_on_Mothers%27_Perceptions_of_Children_Exposed_to_Intimate_Partner_Violence. [cited 2021 Dec 4].
3. Nirmita Panchal, Rabah Kamal, Cynthia Cox, Rachel Garfield. (2021 Feb 10). The implications of COVID-19 for mental health and substance use. [Online]. Kff.org. Available from: <https://www.kff.org/coronavirus-covid-19/issue-brief/the-implications-of-covid-19-for-mental-health-and-substance-use/> [cited 2021 Dec 4].
4. Innocenti U. (2020). Five ways governments are responding to violence against women and children during COVID-19. [Online]. Unicef.org. Available from: <https://blogs.unicef.org/>

- evidence-for-action/five-ways-governments-are-responding-to-violence-against-women-and-children-during-covid-19/ [cited 2021 Dec 3].
5. Fao.org. (2018). Developing gender-sensitive value chains – Guidelines for practitioners. Rome. [Online]. Available from: <https://www.fao.org/3/I9212EN/i9212en.pdf>. [cited 2021 Dec 4].
 6. AIR Online. AIR 1997 Supreme Court 3011. [Online]. Aironline. Available from: [https://www.aironline.in/legal-judgements/1997+\(7\)+JT+384](https://www.aironline.in/legal-judgements/1997+(7)+JT+384). [cited 2021 Dec 3].
 7. Kaur R, Garg S. Addressing domestic violence against women: an unfinished agenda. *Indian Community Med.* 2008; 33(2): 73–6.
 8. Gov.in. [Online]. [cited 2021 Dec 3]. Available from: <https://www.mha.gov.in/sites/default/files/>
 9. Joseph V, Deeya Ray. (2019 Nov 12). India: The right to be forgotten - under the Personal Data Protection Bill 2018. [Online]. Argus Partners. Available from: <https://www.mondaq.com/india/privacy-protection/860598/the-right-to-be-forgotten--under-the-personal-data-protection-bill-2018>. [cited 2022 Nov 15].
 10. Zubair Ahmad. (2022 Aug 23). Right to be Forgotten. [Online]. Manupatra. Available from: <https://articles.manupatra.com/article-details/Right-to-be-forgotten>. [cited 2022 Nov 15].
 11. Cleary Gottlieb. (2019 Mar 12). The Indian Personal Data Protection Bill 2018: a view through the lens of the EU GDPR. [Online]. Khaitan & Co. Available from: <https://www.clearygottlieb.com/-/media/files/india-personal-data-protection-bill-gdpr--final-31219-pdf>. [cited 2022 Nov 15].
 12. Burman A. (2020 Mar). Will India's proposed data protection law protect privacy and promote growth? [Online]. Carnegie India. Available from: https://carnegieendowment.org/files/Burman_Data_Privacy.pdf. [cited 2022 Nov 15].