INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 6 [2025] | Page 247 – 256

RIGHT TO BE FORGOTTEN: A COMPARATIVE LEGAL ANALYSIS OF ARTICLE 17 OF EU'S GDPR VIS-A-VIS SECTION 12 OF INDIA'S DPDP ACT,2023

-Roushan Kumar

ABSTRACT

This paper examines the evolving legal doctrine of the Right to Be Forgotten (RTBF) in both European and Indian contexts, exploring its conceptual foundations, legal interpretations, and practical implications in the digital era. It traces the origin of RTBF from European jurisprudence, particularly the Google Spain case and Article 17 of the EU General Data Protection Regulation (GDPR), highlighting its role in empowering individuals to reclaim control over outdated or irrelevant personal data. The paper juxtaposes this with Section 12 of India's Digital Personal Data Protection (DPDP) Act, 2023, which, though a progressive development, lacks the explicit articulation and enforcement mechanisms seen in EU law. Through a comparative lens, the study analyses key differences in scope, applicability, and institutional support. It further contextualizes the RTBF through landmark Indian and international cases, such as *Jorawar Singh Mundy*, *Subhranshu Rout*, and *Google Spain*, shedding light on how courts balance privacy rights against freedom of information. Finally, the paper discusses the global implications of RTBF, its impact on technology companies, and the pressing need for legal reform in India to ensure data protection aligns with global norms. The RTBF is presented not just as a privacy tool, but as a vital means of restoring autonomy and dignity in an increasingly permanent digital world.

INTRODUCTION

An Indian Forest officer (IFS) moved Delhi High Court invoking his "right to be forgotten" to remove certain articles which related to a case in which He was acquitted[1]. The doctrine of the "right to be forgotten" was first explained and established by the Court of Justice of the European Union (CJEU) in the Google Spain case in 2014[2]. The Right to be Forgotten(RTBF) is a legal concept that allows individuals to request the removal of their personal data from public access, especially online, when certain conditions are met. It is rooted in the idea that people should have control over their personal information, particularly when it is no longer relevant, necessary, or accurate. The right to be forgotten is increasingly important in the digital age, where information can be stored, shared, and accessed indefinitely. It holds significant value because it allows people to remove outdated, irrelevant, or harmful personal data from public access, Ensures individuals maintain control over their digital identity, Gives individuals the chance to move on from past mistakes or outdated events especially relevant for rehabilitated offenders, students, or people previously involved in controversial incidents, Enhances a person's ability to decide what happens to their data and reduces dependency o platforms or third parties to protect privacy, It prevents long-term damage from negative search results, old news, or past behaviour especially important in cases of revenge porn, defamation, or misinformation, but most importantly it forces tech companies to accountable in how they collect, store, and display personal information which helps in establishing more ethical data practices. In addition to the above mentioned points it also offers us a legal route to seek erasure or de-indexing of harmful content which adds to the arsenal of data protection rights, alongside consent, correction, and access.

LEGAL AND CONCEPTUAL FRAMEWORK

ORIGIN OF RIGHT TO BE FORGOTTEN

The origin of the right to be forgotten can be traced back to the Virginia da Cunha case[3]. Virginia da Cunha was an Argentine model and musician which sought injunctions against Yahoo and Google for search results linking her name to several erotic and pronographic websites. The Supreme Court of Argentina concluded that the search engines were not liable for the results that were produced, and

[1] https://www.thehindu.com/news/cities/Delhi/ifs-officer-moves-delhi-hc-to-remove-online-content-under-right-to-be-forgotten/article67679923.ece
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131
[3] Don't shoot the Messenger: Civil Liability for ISPs after Virginia da Cunha v. Yahoo- Argentina & Google Inc.

the use of filters to block search results would amount to prior censorship. Another important piece in the origin of the right to be forgotten is France's right to oblivion[4](le droit à l'oubli') which talks about the right that gives people the legal means to obtain their right to forget over the Internet through limiting the retention of personal digital data and the possibility of its abolition. The groundwork for the right to be forgotten was laid by European Union's data protection directive(1995)[5], 95/46/EC, this directive served as cornerstone EU law protecting individuals regarding the processing of personal data and the free movement of such data. The directive applied to the processing of personal data by individuals or organizations whose activities were governed by the EU. It madaged that each EU member state establish an independent national body to oversee the processing of personal data and aimed to facilitate the free movement of personal data within the EU by harmonizing national laws. But most importantly, the directive allowed the individuals to request correction or deletion of inaccurate or outdated personal data. In addition, to the above mentioned points, The Google Spain case[6], is considered one of the landmark cases with respect to the right to be forgotten, the case relates to the above mentioned directive of EU 95/46/EC, it was held that an Internet search engine operator is considered the controller in respect of the processing that carries out of personal information which appears on web pages published by third parties, namely the (1) finging, (2) indexing, (3) temporary storing, and (4) making it available to web users in a particular order. As such, search engine operators have to comply with the obligations provided for by that directive in particular by removing information connected to a person published by third parties from the list of results displayed following a search made on the basis of a person's name. The Google Spain case along with the other mentioned directives and cases laid the groundwork for the implementation of the European Union's General Data Protection Regulation.

ARTICLE 17 OF EU'S GENERAL DATA PROTECTION REGULATION

Article 17 of chapter 3 of EU's GDPR talks about Right to erasure[7] (right to be forgotten). The article says,(1) The data subjects have the right to obtain from the controller the erasure of personal data concerning themselves without undue delay and the controller have the obligation to erase personal data without undue delay where one of the following grounds applies:

[4] A revision of the attitude of the French punitive legislation on the idea of the right to digital oblivion by Dr. Muaath Al-Mullah
[5] https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng
[6] https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en
[7] https://gdpr-info.eu/art-17-gdpr/

a) The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1)[8], or point (a) of Article 9(2)[9], and where there is no other legal ground for the processing;
c) The data subject objects to the processing pursuant to Article 21(1)[10] and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)[11];
d) The personal data have been unlawfully processed;
e) The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) The personal data have been collected in relation to the offer of information society services referred to in Article 8(1)[12].

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a) For exercising the right of freedom of expression and information;
(b) For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

[8] https://gdpr-info.eu/art-6-gdpr/
[9] https://gdpr-info.eu/art-9-gdpr/
[10] https://gdpr-info.eu/art-21-gdpr/
[11] https://gdpr-info.eu/art-21-gdpr/
[12] https://gdpr-info.eu/art-8-gdpr/

(c) For reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2)[13] as well as Article 9(3)[14];

(d) For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)[15] in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) For the establishment, exercise or defence of legal claims.

ARTICLE 12 OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Article 12 of chapter 3 of Digital Personal Data Protection Act[16] talks about the right to correction and erasure of personal data.

(1) A Data Principle shall have the right to correction completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(2) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal,

(a) Correct the inaccurate or misleading personal data;

(b) Complete the incomplete personal data; and

(c) Update the personal data.

(3) A data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the data of such Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

[13] https://gdpr-info.eu/art-9-gdpr/
[14] https://gdpr-info.eu/art-9-gdpr/
[15] https://gdpr-info.eu/art-89-gdpr/
[16] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

COMPARATIVE ANALYSIS

SCOPE AND APPLICABILITY

Article 17 of the EU GDPR grants individuals the right to have their personal data erased by a data controller under certain conditions and it applies to any organization (whether in the EU or outside, if they target EU residents) that collects, stores or processes personal data. While section 12 of India's DPDP Act, 2023 grants individuals (called Data Principals) the right to correct, complete, update, and erase their personal data. Its focus is on giving people control over their data held by Data Fiduciaries. From the above points one thing is clear while article 17 of EU GDPR is very broad and has a global reach (EU citizens' data anywhere) while section 12 of DPDP act is focused mainly on Indian and Indian data subjects[17]. The DPDP act applies only to "digital personal data" whereas the GDPR applies to personal data even if that data is non-digital. In addition, personal data that is made publicly available is exempt from DPDP obligations. The DPDP act identifies a class of data fiduciaries as SDFs (significant Data Fiduciary) based on (a) volume and sensitivity of personal data processed; (b) risk to the rights of the data principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the state; and (f) public order, and applies additional obligations to those SDFs. There is no equivalent concept under the GDPR[18]. The DPDP act has consent managers who are entities registered with the Data Protection Board under the DPDP act and act on behalf of data principals to review, provide, manage, and withdraw consent whereas the GDPR has no equivalent concept under the GDPR[19]. Processing personal data for the performance of a contract is not a legal basis under the DPDP act. Unless an exemption is granted by the subordinate rules that are yet to be framed, this exclusion differs significantly from GSPR[20].

CASE STUDIES

JORAWAR SINGH MUNDY V UNION OF INDIA

[17] https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf
[18] Ibid
[19] Ibid
[20] Ibid

In this case, the Delhi High Court addressed the emerging "Right to be Forgotten" issue in India. Jorawar Singh Mundy, an American citizen, sought the removal of online records relating to a narcotics case from which he had been acquitted, arguing that the continued availability of such information harmed his reputation. The court recognized the right to be forgotten as part of the fundamental right to privacy under Article 21 and directed websites like Indian Kanoon to de-index the judgment concerning his name, balancing his privacy rights against the public's right to access judicial records. This case marked an important step in developing India's approach to digital privacy and online reputation management[21].

SUBHRANSHU ROUT V STATE OF INDIA

In the following case, the Orissa High Court addressed crucial concerns around digital privacy and victims' rights in the context of sexual offenses. The petitioner, Subhranshu Rout, was accused of raping a woman, recording the incident without her consent, and uploading the video to a fake Facebook account created in her name. While considering his bail application, the Court strongly emphasized the need to protect the victim's privacy and dignity, ultimately rejecting the bail plea due to the serious and damaging nature of the offense. Importantly, the Court discussed the emerging concept of the "Right to be Forgotten," observing that once sensitive information is uploaded online, it becomes almost impossible to completely erase it, comparing it to "toothpaste" that cannot be put back into the tube. The Court stressed that Indian law needs to recognize and operationalize the "Right to be Forgotten," especially to allow victims of sexual violence to reclaim control over their digital identities and avoid repeated victimization through online exposure. This case thus highlighted the urgent need for stronger digital privacy protections and became a significant early judicial acknowledgment of the importance of the "Right to be Forgotten" in India's legal landscape[22].

GOOGLE SPAIN SL AND GOOGLE INC. V AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZALEZ

The following case, decided by the Court of Justice of the European Union(CJEU) in 2014, is a landmark judgment that formally established the right to be forgotten under EU law. The case arose

[21] W.P.(C) 3918/2021

[22] https://www.scconline.com/blog/post/2020/12/07/orissa-hc-read-how-high-court-emphasised-the-need-of-right-to-be-forgotten-in-cases-of-objectionable-photos-and-videos-of-victims-on-social-media/

when Mario Costeja Gonzalez, a Spanish citizen, requested that Google remove links to a 1998 newspaper article about a real estate auction connected to his past social security debts, arguing that the information was outdated and no longer relevant. While the article itself was legally published, Gonzalez argued that continued indexing by Google harmed his reputation. The CJEU ruled in his favour, holding that search engines like Google are "data controllers" and therefore subject to EU data protection laws. The Court emphasized that individuals have the right, under certain conditions, to request removal of personal data from search engine results, particularly when the information is no longer relevant, excessive, or infringes upon their privacy. Importantly, the ruling clarified that this right does not depend on whether the information is accurate or legally published- it focuses on its ongoing relevance and impact on the individual's rights. The decision marked a turning point in data privacy law by recognizing individual's right to control their digital presence and balancing it against public interest and freedom of expression[23].

LIMITATION AND CHALLENGES

Section 12 of the Digital Personal Data Protection Act, 2023 does not explicitly use the term "Right to be Forgotten". It provides a right to request erasure or restriction of continued disclosure only after the purpose of data processing is fulfilled, or consent is withdrawn[24]. Whereas Article 17 of the GDPR explicitly establishes the Right to Erasure, including when data is no longer necessary, or the data subject objects to processing[25]. The right must be balanced with freedom of speech, especially for public records, journalism, or legitimate interests. In Karmanya singh v Union of India[26] and recent High Court decisions, court emphasize that RTBF must not override transparency or public interest. While the EU's GDPR applies extraterritorially that is non- EU companies targeting EU residents must comply. India's DPDP lacks such global reach and has limited scope of enforcement, especially in cross-border data scenarios. In India, enforcement depends on the effectiveness of the Data Protection Board, which is yet to be fully functional. RTBF is new to Indian legal jurisprudence. Unlike the EU where the CJEU has developed a body of law, Indian cases are fragmented and lack Supreme Court clarification[27].

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131
[24] Digital Personal Data Protection Act, 2023, section 12(2).
[25] https://gdpr-info.eu/art-17-gdpr/
[26] Karmanya Singh Sareen v Union of India and Anr. (2017 SCC Online SC 434)
[27] K.S. Puttaswamy v Union of India, (2017) 10 SCC 1.

IMPLICATIONS AND FUTURE PERSPECTIVE

HOW RTBF SHAPES GLOBAL DATA PROTECTION NORMS

China introduced a formal legal framework, the "Personal Information Protection Law of the People's Republic of China" (PIPL)[28]. The enactment of this law filled a legal gap and made detailed provisions regarding the collection, storage, use, transfer, and deletion of personal information. The law explicitly outlines that individuals have a range of fundamental rights over their data, including the right to know, the right to decide, the right to access and copy, the right to rectify or supplement, and the "right to be forgotten". In Switzerland, the "right to be forgotten", known as right to erasure, is recognized under the Swiss Federal Act on Data Protection(FADP)[29]. While in the USA, a New York senator in 2017 and assemblyman David Weprin introduced a bill proposing that individuals be allowed to require search engines and inline speakers to remove information that is "inaccurate", "irrelevant", "inadequate", or "excessive", that is "no longer material to current public debate or discourse" and is causing demonstrable harm to the subject.

POTENTIAL REFORMS NEEDED IN THE DPDP ACT

The DPDP act, though a significant step for data privacy in India, requires key reforms to enhance its effectiveness and align with global standards like the EU GDPR. Crucial improvements include explicitly recognizing the Right to be Forgotten, strengthening data fiduciary obligations, ensuring the independence of the Data Protection Board, and expanding user rights such as data portability and objection to processing. The Act should also provide clarity on cross-border data transfers, adopt a more nuanced approach to children's data by lowering the age of consent, and introduce mechanisms for individual compensation in case of violations. Furthermore, strict timelines for grievance redressal and enforcement are needed to make these rights practically enforceable and meaningful.

IMPACT ON TECH COMPANIES, SEARCH ENGINES AND MEDIA ORGANISATIONS

The RTBF significantly impacts these companies by imposing new obligations on how personal data is managed and disclosed. For search engines lke Google, RTBF means they must de-index links

[28] https://personalinformationprotectionlaw.com/
[29] https://www.pwc.ch/en/insights/regulation/data-deletion.html

upoi=n valid user requests when data is outdated, irrelevant, or no longer necessary, as affirmed in the landmark Google Spain v. AEPD. This places a substantial compliance burden, with Google having processed over 1.5 million such requests by 2020. For technology abd social media companies such as Meta or X, the RTBF necessitates the creation of robust data deletion systems and the removal of personal content across platforms, including from backups, aligning with GDPR. However, these platforms face challenges in ensuring global consistency, especially given the lack of RTBF frameworks in countries like the U.S. For media organizations, RTBF raises concerns around editorial freedom and archiving, as individuals may seek to anonymize or erase references from previously published reports. While GDPR Article 17(3)(a) provides exceptions for freedom of expression, Indian courts, such as in *Subhranshu Rout v. State of Odisha* (2020), have also begun recognizing the tension between privacy and public interest. Globally, the need to balance RTBF with freedom of the press, transparency, and the right to information remains a core challenge, especially for organizations operating across multiple legal jurisdictions with differing privacy norms.

CONCLUSION

The Right to Be Forgotten (RTBF) is no longer a theoretical concept but an evolving and increasingly essential element of data privacy in the digital age. As individuals' personal lives become permanently archived online, the need to reclaim control over one's digital identity becomes more urgent. While the European Union has led the way in shaping a robust legal framework through Article 17 of the GDPR, India's DPDP Act marks an important but still maturing step toward similar protections. The comparative analysis reveals both ambition and limitations within the Indian framework—particularly in scope, enforcement, and conceptual clarity. Landmark cases like *Jorawar Singh Mundy* and *Subhranshu Rout* reflect a growing judicial recognition of the RTBF, even as legislative mechanisms continue to evolve. International developments—from China's PIPL to emerging proposals in the United States—show a global momentum toward embedding digital dignity into law. However, balancing the RTBF with freedom of expression, journalistic integrity, and public interest will remain a nuanced and jurisdiction-specific challenge. Going forward, meaningful reforms in India's DPDP Act—such as explicitly incorporating RTBF, ensuring independent enforcement, and enabling cross-border protection—will be crucial. Ultimately, the RTBF is not just about deleting data, but about enabling second chances, preserving autonomy, and restoring fairness in a world where the internet never forgets.