IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE RIGHT TO BE FORGOTTEN: A COMPARATIVE ANALYSIS OF THE GDPR AND THE DPDPA

Bhargav Chaganti
LLM Scholar
School of Law,
Christ (Deemed to be University), Bengaluru, India

Abstract: The digital age has witnessed an explosion in personal data collection, raising concerns about individual privacy. The Right to be Forgotten (RTBF) empowers individuals to request the deletion of their personal data. The Digital Personal Data Protection Act of 2023 is India's answer to growing concerns over data privacy; it saw several challenges before its enactment. This paper compares the RTBF within the European Union's General Data Protection Regulation (GDPR) frameworks and India's Digital Personal Data Protection Act, 2023 (DPDPA). The paper explores the jurisprudence of RTBF in India and the EU. The paper analyses the provisions under GDPR and DPDPA concerning the Right to be Forgotten to understand how far the DPDPA provisions stand their ground. The country is still at a nascent stage in data protection. The strengths and weaknesses of DPDPA are yet to be truly realized as they have yet to come into force.

Index terms: Right to be Forgotten, DPDPA, Right to Privacy, GDPR, Right to Erasure.

INTRODUCTION

The digital age has brought about a period characterized by an unparalleled accumulation of personal data. Each instance of clicking, purchasing, and engaging online creates a digital footprint, which creates an extensive and intricate record of our lives. The widespread collection of data gives rise to significant inquiries on the protection of individual privacy and the ability to exercise control over personal information. The Right to be Forgotten (RTBF) is fundamental in this dynamic environment.

The Right to Privacy (RTBF) grants individuals the authority to demand the removal of their data from search engines and other internet platforms. This Right allows individuals to begin over, enabling them to move on from previous errors or irrelevant knowledge that might harm their current and future circumstances. The extensive memory of the Internet threatens our entitlement to be forgotten. The global population of internet users now stands at 5.35 billion, with projections indicating a growth to 7.9 billion by the year 2029[1]. Despite our efforts to remove material, copies may persist on the Internet. Particularly in the context of AI, they possess an immutable memory. Enforcing the Right to be forgotten, which grants individuals autonomy over their online history, poses challenges in the current era of digital technology.

This study explores the concept of the Right to Privacy (RTBF) about data privacy rules, focusing on a comparative analysis of the General Data Protection Regulation (GDPR) of the European Union (EU) and the Digital Personal Data Protection Bill, 2023 (DPDPA) of India. To identify gaps and areas for improvement in India's data protection laws, an analysis will be conducted on the scope, enforcement mechanisms, and limits of the Right to Privacy Framework (RTBF) in each framework. In India's efforts to traverse the intricacies of the digital era, it is crucial to have a solid Right to Privacy Framework (RTBF) in place. This

1Lexie Pelchen, Internet Usage Statistics in 2024, FORBES (Mar 1st, 2024) https://www.forbes.com/home-improvement/internet/internetstatistics/#:~:text=There%20are%205.35%20billion%20internet,the%20internet%2C%20according%20to%20Statista.

framework is necessary to guarantee individual autonomy over personal information and promote a harmonious equilibrium between privacy and other social concerns.

EVOLUTION OF RTBF: EUROPEAN UNION

The origin of this specific Right can be ascribed to the conceptualization of the 'Right to oblivion' or Droit a loubli in the French legal framework in 2010. The Right of Oblivion was designed to aid persons convicted of crimes and who had completed their prison terms by forbidding the public release of information regarding their criminal actions and personal life.

In ***AEPD and Mario Costeja González v. Google Spain SL, Google Inc***[2], the Court of Justice of the European Union (CJEU) rendered a decision in a case in 2014 involving Mario Costeja González, who asked Google to take down links to newspaper articles that mentioned his previous debts. As to the ruling of the CJEU, people have the Right to ask for links to be removed from search engine results if they contain excessive, irrelevant, or outdated information unless there is a robust public interest in maintaining it.

In 1998, Mario Costeja Gonz'lez, a Spanish man, faced financial difficulties and experienced a pressing need for financial resources. As a result, he continued to advertise a property for auction via a newspaper, which fortuitously migrated to the online platform. Unfortunately, the online presence of Mr. Gonz was not disregarded. The transaction's news was made available on Google after the individual successfully resolved their financial issue, therefore generating extensive discussion surrounding their potential bankruptcy status.

Consequently, this substantially damaged his reputation, prompting him to initiate legal proceedings. The litigation in question ultimately established the legal doctrine called the 'Right to be forgotten.' In a ruling against Google, the European Court of Justice confirmed that persons inside the European Union had the entitlement to demand the removal of their personal information from search results and public records databases under certain conditions. However, in 2019, the European Union court implemented a limitation on the ruling, asserting that Google is not legally bound to uphold the 'Right to be forgotten' internationally.

In ***Google LLC v. CNIL***[3], the CNIL, the French data protection authority, fined Google for failing to delist search results globally when complying with Right to be Forgotten requests. Google argued that delisting should only be applied within the EU. The case raised questions about the territorial scope of the Right to be forgotten and the balance between the Right to privacy and freedom of expression. In ***NT1 & NT2 v. Google LLC***[4], the UK High Court ruled in a case involving two individuals with criminal convictions but argued that their names should be removed from Google search results. The Court sided with Google, finding that the information was still relevant and in the public interest. This case highlighted the difficulty in balancing an individual's Right to be forgotten with the public's Right to access information.

ARTICLE 17 OF GDPR

Article 17[5] of the General Data Protection Regulation (GDPR) delineates the specific circumstances in which the Right to be forgotten is applicable. An individual has the entitlement to request the deletion of their data if the organization considers the personal data unnecessary concerning its original purpose for collection or processing. The legal basis for data processing inside the organization relies on an individual's permission, which the subject has later revoked. The justification for an organization's processing of an individual's data is grounded in legitimate interests.

Nevertheless, the individual raises a concern over this processing, and there is no undeniable and valid reason for the organization to continue with the processing. The individual is contesting the organization's handling of personal data for direct marketing. An entity mishandled the personal data of an individual. An organization must erase personal data to comply with legal regulations or demands.

The organization has engaged in processing a child's data to deliver information society services. However, an organization's Right to manage an individual's data may take precedence over their Right to delete their data from their memory. The General Data Protection Regulation (GDPR) outlines several situations that overrule the Right to erasure. In order to exercise the fundamental Right to freedom of expression and access

2Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González C-131/12.
3Google LLC v. CNIL C-507/17.
4NT1 & NT2 vs Google LLC [2018] EWHC 799 (QB).
5Article 17 of GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

to information, the data is employed. The data is being employed to comply with a legal mandate or obligation. The data is employed to carry out a task that is being carried out in the public interest or while exercising the official authority of an institution.

Efficient data processing is essential for achieving public health goals and is in line with the overall well-being of the general public. Data processing is a crucial component in implementing preventative or occupational medicine. It is important to note that this obligation is only relevant when the data is being managed by a healthcare professional legally obligated to uphold professional secrecy. The dataset includes substantial material relevant to public interest, scientific research, historical inquiry, or statistical analysis. The elimination of this element will undoubtedly obstruct or obstruct the advancement toward the desired goal of data processing. The data gathered is employed to construct a legal defence or advocate for other legal claims.

JURISPRUDENCE OF RTBF IN INDIA

In the case of ***KS Puttuswamy vs Union of India***[6], the Supreme Court of India acknowledged the Right to Privacy as a fundamental right. The Court noted that an individual's Right to have authority over their data and control their own life would also include their Right to govern their presence on the Internet. This laid the groundwork for acknowledging the Right to be Forgotten, which asserts that individuals have the Right to privacy and have the ability to determine whose information is accessible to the public. The subject has been discussed in various High Courts.

Sri Vasunathan vs. The Registrar General[7], the petitioner sought the removal of her daughter's name, which was propping up on specific search engines due to her involvement in a case of marriage annulment published online. The Court ruled that, despite the lack of a statute specifically addressing this case, it would only allow for the same in India given the growing significance given to people's rights to privacy and the establishment of laws about the Right to be forgotten in other jurisdictions, such as Europe.

The case of ***Dharmraj Bhanushankar Dave vs. the State of Gujurat***[8] gave a contrasting judgment in a comparable case where a person not guilty of any crimes had petitioned to have his name taken down from public domains. Here, the Gujarat High Court adopted a more positivist approach to reasoning, ruling that it could not find the publishing to violate the petitioner's fundamental rights in the lack of the required legislative support. As a result, it declined to enforce the petitioner's Right to be forgotten.

In the case of ***Kancherla Durga Prasad vs. State of Karnataka***[9], the Apex Court concluded that, given the social rejection they experienced as a result of being involved in a prior divorce, a couple who had been estranged had the Right to have their personal information removed from the Internet. This ruling will have a significant impact on future High Court decisions. It will have great persuasive power in any dispute involving the Right to be forgotten or even the broader Right to privacy that may arise in the future.

The petitioner in ***Jorawer Singh Mundy vs Union of India***[10] was an American citizen of Indian descent. In 2009, the individual in question faced allegations under the Narcotics Drugs and Psychotropic Substances Act of 1985 during his travel to India. Nevertheless, in 2011, he was exonerated from all accusations, and his exoneration was affirmed in 2013. The petitioner asserts that upon his return to the United States, he encountered discrimination and disadvantage due to the unrestricted accessibility of the judgments' contents on the Internet. The petitioner issued a legal notice to the relevant websites; however, only one website responded by removing the judgments, while the remaining websites were included as respondents. The petitioner kindly urges the Court to instruct the defendants to eliminate the ruling, safeguarding his entitlement to be eradicated from public view.

In the case of ***X vs YouTube Channel***[11], the Delhi High Court awarded protection to an actress who brought a lawsuit against the republishers of her obscene movies. The Court affirmed the actress's Right to be forgotten.

[6]KS Puttuswamy v Union of India, (2015) 8 SCC 735.
[7]Sri Vasunathan vs The Registrar General WP No.62038 of 2016.
[8]Dharmraj Bhanushankar Dave vs State of Gujurat SCA 1854/2015.
[9]Kancherla Durga Prasad vs State of Karnataka CRL.P. NO. 8912/2017.
[10]Jorawar Singh Mundy v Union of India (2021) SCC OnLine Del 2306.
[11]X v https://www.youtube.com/watch?v=iq6k5z3zys0, (2021) SCC OnLine Del 4193.

The High Court of Madras, in the case of ***Karthik Theodore vs the High Court of Madras***, ruled that defendants had the entitlement to have their names expunged from judgments or decrees, especially those that are publicly accessible and may be accessed through search engines. In reaching its determination, the Court observed that before the implementation of data protection law, it is incumbent upon the Court to safeguard individuals' privacy and reputational rights. The inclusion of an objective criterion in the legislature's enactment of the Data Protection Regime is recommended to address appeals for removing names of convicted individuals from criminal cases.

In the case ***Zulfiqar Ahman Khan vs Quintillion Business Media Pvt. Ltd. & Ors***[12], the plaintiff initiated legal proceedings by filing a lawsuit seeking an injunction against the defendant, a news website. The website above disseminated two narratives from two individuals who had survived allegations of sexual harassment perpetrated by the plaintiff. The plaintiff was identified as the culprit in these published reports. The plaintiff said that the dissemination of the narratives on the digital platform 'www.quint.com' by the first defendant resulted in significant psychological distress and emotional anguish experienced by the plaintiff. The individual argued that they should have been provided with advance notification before publishing the publications.

Nevertheless, via their failure to do so, the defendants disseminated biased narratives, eroding his standing. The removal of two articles purportedly libelous against Zulfiqar Khan by the Quintillion Business Media online portal Quint.com, which contained claims related to the #MeToo movement, was mandated by the High Court. The Court acknowledged the plaintiff's reputation, the Right to Privacy, and the Right to be Forgotten by mandating the removal of the contentious item. Moreover, any other news outlet or website was prohibited from republishing these assertions. In this instance, it was acknowledged that the entitlement to be forgotten or left undisturbed constituted an essential component of the Right to Privacy.

In the case of ***Subhranshu Rout vs State of Odisha***[13], the Orissa High Court, in the context of a bail application, proceeded to elucidate the concept of the Right to be forgotten and affirmed its applicability to people as a fundamental aspect of their Right to privacy.

RIGHT TO ERASURE UNDER DPDPA

The primary objective of the Digital Personal Data Protection Act of 2023 is to achieve a harmonious equilibrium between the rights of individuals and the public interest in processing digital personal data. Section 12[14] of the Act grants the data principal the Right to correct and erasure personal data. It states that data fiduciaries must respond to the data principal's request by updating, correcting, completing, or destroying the data. Additionally, it delineates that in the event of receiving a request for data deletion, it may only be granted if the objective of its acquisition is satisfied and legal obligations do not mandate data retention. As stated in Section 16(4)[15], the data principal is obligated to provide verified and authentic information.

In addition, Section 18(1)[16] of the Act outlines the circumstances in which this Right does not apply. These circumstances include when the data is necessary for carrying out judicial or quasi-judicial duties when the data is required for enforcing legal rights or claims, when data is processed to prevent, detect, investigate, or prosecute any offense or law violations, and when the data is processed by a person based in India under a contract outside the territory of India. In the section above, the second clause stipulates that the Union Government has the authority to exempt the application of the Act in cases where data is necessary for statistical purposes or the preservation or prevention of incitement to cognizable offenses about public order, security, sovereignty, integrity, and friendly relations with other states.

The legislation further includes provisions for creating the Data Protection Board as outlined in Section 19[17]. The primary responsibilities of this board include assessing adherence to the laws, imposing penalties on those who violate them, and executing tasks as instructed by the Central Government. According to the Criminal Procedure (Identification) Rules, the investigating authority can gather identifiable information such as biological samples and fingerprints. This information will be electronically or digitally kept for 75 years unless the individual is found not guilty, in which case it will be permanently destroyed. In certain instances, a Court

[12]Zulfiqar Ahman Khan v Quintillion Businessman Media Pvt. Ltd, (2019) SCC OnLine Del 8494.
[13]Subhranshu Rout vs State of Odisha 2020 SCC OnLine Ori 878.
[14]Section 12 of the Digital Personal Data Protection Act, 2023 (No. 22 Of 2023).
[15]Section 16(4) of the Digital Personal Data Protection Act, 2023 (No. 22 Of 2023).
[16]Section 18(1) of the Digital Personal Data Protection Act, 2023 (No. 22 Of 2023).
[17]Section 19 of the Digital Personal Data Protection Act, 2023 (No. 22 Of 2023).

or Magistrate can issue a directive to preserve details, provided the reasons for such retention are documented in writing. This regulation imposes a constraint on the entitlement to be forgotten and possesses the capacity to provide significant ramifications about the entitlement to privacy.

ANALYSIS OF RTE UNDER DPDPA

B. N. Sri Krishna Committee recommended that the Right to be Forgotten can be exercised if the data is misleading, humiliating, obsolete and embarrassing. This was incorporated in Section 20 of the Personal Data Protection Bill, 2019[18]. The subsequent drafts adopted this differently. The passing of the Digital Personal Data Protection Act (DPDPA) in 2023 signifies a notable advancement in tackling privacy issues and safeguarding data for individuals in India. It expands on the groundwork established by previous versions, considering the changing environment of data protection and international standards.

An outstanding aspect of the DPDPA is its strong focus on the fundamental Right to give permission. The system effectively grants data principals full authority over their data, guaranteeing that they cannot be processed without express authorization unless specific legal circumstances arise. These principles are consistent with the notion of informed and voluntary permission, which is a fundamental cornerstone of data protection on a global scale. In addition, the DPDPA grants individuals the Right to erasure, enabling them to seek to delete their data and enhance their authority over their digital presence.

The Act also provides a thorough approach to reporting data breaches. In contrast to earlier versions, which allowed for varying interpretations on the specific breaches that should be notified, the Data Protection and Privacy Act (DPDPA) stipulates that all instances of personal data breaches must be disclosed to both the Data Protection Board of India and the appropriate data principals. This guarantees openness and responsibility, empowering individuals to undertake essential measures in case of a violation.

In several ways, the DPDPA deviates from its predecessors. Significantly, it omits clauses about the entitlement to data portability and the entitlement to be erased. The omission of these rights in the DPDPA is a significant change from their inclusion in the 2018 and 2019 versions. This prompts inquiries on the degree to which data owners may exercise authority over their data and their capacity to transition between service providers smoothly.

Upon careful analysis of the DPDPA's influence on the Right to privacy as enshrined in Article 21 of the Indian Constitution, it becomes apparent that the legislation fortifies and enhances this fundamental constitutional entitlement. The Right to privacy is enshrined as a fundamental right in Article 21, and significant rulings by the Supreme Court, such as K.S. Puttaswamy v. Union of India and Navtej Singh Johar v. Union of India, have broadened its extent and acknowledgment.

The Data Protection and Privacy Act (DPDPA) is based on these fundamental values since it grants individuals enhanced authority over their data. It protects against unjustified monitoring, theft of personal information, and damage to one's reputation, all of which can be considered violations of the Right to Privacy. The DPDPA emphasizes the gravity of privacy violations by granting data principals the authority to pursue compensation in cases of harm resulting from data processing.

The DPDPA 2023 signifies a significant advancement in India's endeavours to safeguard privacy rights and govern data processing. Although it excludes specific elements from previous versions, it incorporates robust systems for obtaining consent, reporting breaches, and erasing data. Furthermore, it enhances the entitlement to privacy outlined in the Indian Constitution by advocating for openness, responsibility, and personal authority over personal information by changing international norms and significant legal rulings. However, it lacks regulatory measures to address harms arising from the processing of personal data, which were present in the earlier drafts. It relies on government notification without a comprehensive evaluation of data protection standards in each country with respect to cross-border data transfer regulation mechanism[19].

[18]Prerna Shree, *Oblivisci and the Right to be Forgotten in India*, DNLUSLJ, (2023).

[19]Sayantani Dutta, Does the DPDPA 2023 Strengthen the Right to Privacy in India?: A Constitutional Perspective, TSCLD (Oct 13, 2023) https://www.tscld.com/does-the-dpdpa-2023-strengthen-the-right-to-privacy-in-india-a-constitutional-perspective.

COMPARATIVE ANALYSIS OF GDPR AND DPDPA

SCOPE OF RTBF UNDER GDPR

According to Article 17 of the General Data Protection Regulation (GDPR), individuals considered 'data subjects' are entitled to seek to delete their data without any unnecessary delay. This request shall be quickly addressed if it meets the following conditions: The acquired data is no longer deemed essential for its original purpose—withdrawing permission without any legal basis for processing. The individual possessing the data expresses their objection to processing their data, and there are no valid overriding reasons (similar to the 'Certain lawful uses' outlined in the Act). Illegally processed data: Data to be deleted due to a legal requirement. According to Article 8(1)[20], data is gathered to provide information society services.

Moreover, according to Article 17(2)[21], it is mandated that the 'controller' delete the data if it becomes public and additionally provide instructions to other controllers with whom the data has been shared. According to Article 17(3)[22], there are exceptions to data needs in some situations. These exceptions include situations where the data in issue is necessary for the exercise of the Right to freedom of speech and information, compliance with legal obligations, the execution of a job in the public interest, or the exercise of official power by the regulator. The goal is to serve the public interest in public health, preserve information for public interest, scientific or historical study, or statistical analysis, and if deletion would make it impossible to process such information for legal claims.

SCOPE OF RTE UNDER DPDPA

The rights and duties of the data principal are codified in Chapter III of the Act. Gaining a comprehensive understanding of the extent of the rights and responsibilities of the data principal will assist in proposing suitable solutions for international compliance. According to Section 11[23] of the Act, the data principal is granted the Right to receive information from the Data Fiduciary. These rights include the ability to collect personal data from the data fiduciary, provided that consent has been freely given.

To exercise this Right, individuals can request the information in the specified manner: A comprehensive overview of the personal data being processed and the specific processing activity being carried out. This inquiry pertains to identifying further data fiduciaries and processors with whom the data has been shared, together with a comprehensive description of the shared data—additional details on the personal data and its handling.

According to Section 12 of the Act, individuals have the Right to rectify, complete, update, and delete their data provided they have consented. This Right may only be rejected if the data is necessary for a specific purpose or to comply with the law.

ANALYSIS OF GDPR and DPDPA

Merely examining the Indian legislation reveals that it broadly defines data protection. In contrast, the GDPR includes a comprehensive clause that addresses most of the "data subject's" concerns. Nevertheless, the primary distinction is in the absence of importance placed on the length of compliance in India, in contrast to GDPR's emphasis on safeguarding their 'data subject' from the consequences of excessive delay.

In addition, the Right to Erasure (RTE) under the General Data Protection Regulation (GDPR) is sufficiently comprehensive to encompass the illegal processing of data, namely data processing that occurs without the approval of the 'data subject.' In contrast, in India, the RTE only applies to digital personal data for which the data subject has provided consent for processing.

However, the extent of the Right to erasure (RTE) in India is restricted compared to that of the European Union (EU), primarily because of fundamental disparities in the definition of personal data. Within India, the phrase' data' only pertains to digitalized personal data or data that has been physically acquired and later transformed into a digital format. In contrast, inside the European Union, the term "personal data" pertains to information that will undergo automated processing, either in its entirety or in part. Furthermore, it encompasses personal information currently or will be included in a file system.

[20]Article 8(1) of GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
[21]Article 17(2) of GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
[22]Article 17(3) of GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
[23]Section 11 of the Digital Personal Data Protection Act, 2023 (No. 22 Of 2023).

CONCLUSION AND SUGGESTIONS

Although the General Data Protection Regulation (GDPR) and the Data Protection and Privacy Act (DPDP Act) have similar goals, they differ significantly in their strategy and technique. The General Data Protection Regulation (GDPR) exhibits more prescriptiveness than the Data Protection and Privacy Act (DPDP). The DPDP Act delineates specific core principles while allowing for resolving other implementation-related matters through later subordinate legislation. As the legislative process progresses, this approach has the potential to offer more flexibility and adaptability in addressing several facets of data security.

Entities that are currently obligated to adhere to the GDPR must be ready to make necessary modifications and fine-tune their operations to achieve compliance with the requirements of the DPDP Act. With the law's implementation, companies will be expected to strategically traverse the supplementary foundation and adjust their activities accordingly to conform to the newly established Indian framework.

The legal precedents worldwide are relatively unambiguous on this matter. Nevertheless, in the context of India, the acceptance of RTBF is limited to the scope of the Right to Erasure as outlined in Section 11 of the Act. The standards provided by the European Union's General Data Protection Regulation (GDPR) and the subsequent adherence by major multinational corporations (MNCs) might assist enterprises worldwide in adopting the most effective approach to safeguarding and handling data, even by the forthcoming legislation in India.

It is noteworthy that the assessment of an individual's Right to Benefit from Family (RTBF) is conducted during the request processing stage when corporations analyse the individual's RTBF about its exceptions since RTBF is not an unconditional entitlement. However, the core principle for operating protocols designed to protect client data successfully is the prompt handling of requests without any unnecessary delay. Therefore, it is of utmost importance for organizations to promptly complete such requests.

There are several concerns that might pop up once the Act comes into force. For now, the Act may not provide a comprehensive account on Data Protection, yet it is believed to be a start. Further research as the Act comes into force is recommended to realise the full potential of the merits and demerits. Implementation, awareness, clashes with right to information and freedom of speech and expression, technical challenges etc would have to tackled with in the future. Nevertheless, the Act being enacted is a step forward in realising the growing need for Data protection.

REFERENCES

Douwe Korff, *The Indian Digital Personal Data Protection Act, 2023, viewed from a European Perspective, SSRN, 1-58 (2023).*

Prerna Shree, *Oblivisci and the Right to be Forgotten in India*, DNLUSLJ, (2023).

Uta Kohl, *The Right to be Forgotten in Data Protection Law and Two Western Cultures of Privacy*, 72(3), International & Comparative Law Quarterly, 737-769 (2023).

Shabnam Ahmed Zaman, Saptarishi Prasad Sharma & Modhu Chanda Dey, *Right to Be Forgotten: Socio-Legal Study*, 4 INDIAN J.L. & LEGAL RSCH. 1 (2022).

Piyush Jha, *Right to Be Forgotten and Its Conflict with Freedom of Speech and Expression in India*, 4 INDIAN J.L. & LEGAL RSCH. 1 (2022).

Ashwinee Kumar, *The Right to be Forgotten in Digital Age: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & the GDPR*, 2, Shimla Law Review, 75-104 (2020).

Prashant Mali, *Privacy Law: Right to Be Forgotten in India*, 7 NLIU L. REV. 1 (2018).

Michael Douglas, *Questioning the Right to be Forgotten*, 40(2), Alternative Law Journal, 109 112 (2015).