OPEN ACCESS

Volume: 5

Issue: 2

Month: May

Year: 2026

ISSN: 2583-7117

Published: 09.05.2026

Citation:

Mishal Ann James "Digital Privacy and The Right to Be Forgotten: Managing Public Access and Individual Rights in The Modern Internet Era" International Journal of Innovations in Science Engineering and Management, vol. 5, no. 2, 2026, pp. 169-176.

DOI:

10.69968/ijisem.2026v5i2169-176

Digital Privacy and The Right to Be Forgotten: Managing Public Access and Individual Rights in The Modern Internet Era

Mishal Ann James[1]

[1]*Asst. Professor, Agnel School of Law, Vashi, Navi Mumbai*

Abstract

The advent of the digital age has ushered in unprecedented access to information, revolutionising communication, and knowledge sharing. However, this same technology has also raised profound concerns about individual privacy and the right to control personal data. At the heart of this complex issue lies the concept of the "Right to be forgotten". The "right to forget" refers to the already intensively reflected situation that a historical event should no longer be revitalized due to the length of time elapsed since its occurrence; the "right to be forgotten" reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them. This paper examines the Right to be Forgotten within the broader context of digital privacy, focusing on the challenge of balancing individual privacy rights with public access to information with a detailed review on the legal frameworks governing Right to be Forgotten, including the European Union's General Data Protection Regulation (GDPR), and explores the practical implications of these regulations and other global data protection laws, assessing their impact on privacy and transparency. Through case studies and comparative analysis, the paper examines the practical implications of Right to be Forgotten, its effectiveness in different jurisdictions, and the challenges associated with implementing privacy protections in a globalized digital landscape.

Keywords; Right to be Forgotten, Digital Privacy Rights, General Data Protection Regulation (GDPR), Personal Data Protection, Privacy and Public Access to Information.

INTRODUCTION

The "Right to Forget" refers to the already highly contentious situation in which a historical event should no longer be revived due to the passage of time since its occurrence; the "right to be forgotten" reflects an individual's request to have certain data deleted so that third parties cannot trace them. As a result, the right to be forgotten is founded on an individual's autonomy in becoming a right holder in relation to personal information over time; the further back the information's origin, the more probable personal interests will triumph over public interests.

The right to be forgotten is an emerging legal concept that allows individuals to control their online identities by requesting Internet search engines to remove certain results. It gained prominence after the **Google Spain SL v. Agencia Española de Protección de Datos** ruling, commonly known as the Google Spain ruling, where the EU Court of Justice detailed the protection arising from the existing right to erasure. Specifically, the court established that users can ask search engines to delist certain URLs from search results when searches are conducted using their name, if the content on the web pages in the results includes information that is "inadequate, irrelevant or no longer relevant, or excessive."

This right was later included as the Right to Erasure under the General Data Protection Regulation (GDPR) of the European Union, granting individuals the right to request the deletion of their personal data by organizations. Article 17 of GDPR allows individuals to request the deletion of personal data when it is no longer necessary for the purposes for which it was collected, when they withdraw consent, or when they object to the processing of their data.

The right to be forgotten is firmly embedded in EU law through the GDPR. It aims to give individuals control over their personal data and ensure that outdated or irrelevant information is not perpetually accessible online.

In contrast to the EU, the U.S. has not adopted a comprehensive right to be forgotten. Privacy and data protection laws in the U.S. are more fragmented and tend to focus on specific sectors rather than a broad right to data erasure.

While the California Consumer Privacy Act, effective from January 1, 2020, provides some rights related to personal data, including deletion, it does not offer a right to be forgotten in the same comprehensive sense as the GDPR.

India's approach to data privacy and protection has undergone significant transformation in recent years, driven by the growing importance of digital data and the internet. The Right to Be Forgotten (RTBF) has emerged as a crucial concept globally, and India is beginning to address this within its legal framework, reflecting the need for enhanced data privacy protections.

The Personal Data Protection Bill (PDPB), introduced in 2019, represents a major step towards a comprehensive data protection regime in India. While the bill does not explicitly mention RTBF, it encompasses several provisions related to data subject rights, such as the right to correction and erasure of personal data, which align with the principles underlying RTBF. The bill is designed to regulate data processing activities, consent, and breach notifications, setting the stage for future data privacy regulations.

To oversee compliance with data protection laws, the PDPB proposes the establishment of a Data Protection Authority of India (DPA). The DPA would handle complaints, enforce regulations, and ensure that data subjects' rights are upheld. Although RTBF is not explicitly detailed in the PDPB, the principles embedded in the bill suggest a framework where such rights could be integrated as the legislation evolves.

In 2017, the Supreme Court of India affirmed the right to privacy as a fundamental right under Article 21 of the Indian Constitution in the landmark case ***Justice K.S. Puttaswamy (Retd.) v. Union of India***.[1] This ruling underscored that privacy is a core component of personal liberty and life, laying a constitutional foundation that could support arguments for incorporating RTBF into Indian law. While this decision did not specifically address RTBF, it reinforces the broader context of privacy rights.

Indian High Courts have started to engage with data privacy issues, though RTBF has not yet been a central focus. The principles derived from these cases may influence future legal interpretations and the potential adoption of RTBF in India.

Implementing RTBF in India presents several practical challenges. The global nature of the internet complicates the enforcement of data removal, as ensuring comprehensive deletion from all relevant platforms and jurisdictions is technically demanding. Additionally, there are significant administrative hurdles in effectively managing and processing RTBF requests.

Balancing RTBF with freedom of expression and public access to information is crucial. The framework for RTBF must carefully navigate the tension between individual privacy and public interest, particularly in cases involving public figures or issues of significant societal concern.

RTBF IN INDIA: LEGAL FRAMEWORK

RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT: PUTTASWAMY CASE (2017)

The landmark Puttaswamy case (2017) established privacy as a fundamental right under the Indian Constitution. According to the Supreme Court of India, privacy is an essential component of the right to life and personal liberty under Article 21. This ruling constituted a significant shift in Indian constitutional law, recognizing privacy as a fundamental component of human dignity and personal autonomy.

Recognizing privacy as a basic right has consequences for the Right to be Forgotten (RTBF). While the Puttaswamy case did not directly address RTBF, the principles established support arguments for personal data ownership and privacy, which are consistent with RTBF concepts. The case highlights the necessity for legislative frameworks that protect individuals' rights to control and erase personal information.

[1] Justice K.S. Puttuswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).

BALANCING ARTICLE 21 (RIGHT TO LIFE AND PERSONAL LIBERTY) WITH ARTICLE 19 (FREEDOM OF SPEECH)

In Indian constitutional law, Article 21 guarantees the right to life and personal liberty, while Article 19 provides for the freedom of speech and expression. Balancing these rights is crucial in the context of RTBF and privacy.

Article 21 (Right to Life and Personal Liberty): This article ensures that individuals have the right to live with dignity and control over their personal data. It supports the notion that privacy, including control over one's personal information, is essential to a dignified life.[2]

Article 19 (Freedom of Speech and Expression): This article protects the freedom of speech and expression, including the public's right to access information. This freedom must be balanced against privacy rights, especially in cases where personal data removal requests might impact public access to information.[3]

The challenge lies in balancing these rights. On one hand, Article 21 supports privacy and personal data control, while on the other hand, Article 19 ensures freedom of expression and access to information. Courts and legislators must navigate this balance, ensuring that RTBF provisions do not unduly restrict freedom of speech while upholding individual privacy rights.

The Puttaswamy case (2017) affirmed the Right to Privacy as a fundamental right in India, supporting principles related to the RTBF. Balancing this right with the freedom of speech under Article 19 requires careful consideration to ensure that privacy is protected without unduly limiting public access to information.

STATUTORY PROVISIONS

Information Technology 2000 and its Amendments

The Information Technology Act, 2000 (IT Act) primarily addresses issues related to electronic commerce, digital signatures, and cybersecurity. It does not explicitly provide for the Right to be Forgotten (RTBF) but includes provisions related to data protection and privacy.

Key provisions are:

Section 43A: This section mandates that companies possessing sensitive personal data must implement reasonable security practices to protect such data. Failure to do so can result in compensation for damage caused.[4]

Section 72A: This section addresses the breach of confidentiality and privacy by individuals who are entrusted with personal information. It provides for penal action in cases where personal data is disclosed without consent.[5]

Subsequent amendments to the IT Act, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, further detail requirements for data handling and protection. However, the act and its rules do not directly address RTBF, focusing more on data security and privacy rather than the specific right to data removal.

ROLE OF DPDP ACT, 2023

The Digital Personal Data Protection Act (DPDPA) of 2023, commonly referred to as the DPDP Act is the data privacy legislation of India. The law is a meticulous blend of recognition of the rights of individuals and the need for processing of data.

Ever since the famous Puttaswamy judgment recognized the right to privacy as a fundamental right, digital privacy has been a hot topic in the country. Now that the DPDP Act has received the assent of the President, India is ready to enter its digital privacy era.

The DPDP Act introduces a formal right to erasure of personal data, which aligns with the RTBF principles. Individuals can request the deletion of their personal data when it is no longer necessary for its intended purpose or when consent is withdrawn. The act strengthens individuals' rights over their personal data, including the right to access, correction, and erasure. It requires data fiduciaries (organizations that handle personal data) to comply with these rights, providing a statutory basis for the RTBF. The DPDP Act establishes the Data Protection Board of India to oversee compliance, handle grievances, and adjudicate disputes related to data protection and privacy, including RTBF requests.[6]

[2] INDIA CONST. art.21.
[3] INDIA CONST. art. 19.
[4] The Information Technology Act, 2000 No. 21, Acts of Parliament (2002) India.
[5] The Information Technology Act, 2000 No. 21, Acts of Parliament (2002) India.
[6] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) Acts of Parliament (2023)India

The DPDP Act 2023 significantly enhances the statutory framework for data protection in India by explicitly incorporating the RTBF, aligning with international standards and addressing gaps left by the IT Act.

While the Information Technology Act, 2000 laid the groundwork for data protection and privacy, it did not directly address the RTBF. The Digital Personal Data Protection Act (DPDP) 2023, however, explicitly incorporates the RTBF, providing a comprehensive framework for data erasure and enhancing individuals' control over their personal data.

JUDICIAL INTERPRETATIONS

K.S. PUTTASWAMY V. UNION OF INDIA (2017)

In this landmark judgment, the Supreme Court of India recognized the Right to Privacy as a fundamental right under Article 21 of the Indian Constitution. The case involved a challenge to the constitutionality of the Aadhaar scheme, which required biometric and personal data collection.

The significance is that the court's ruling established that privacy is integral to the right to life and personal liberty, thereby setting a constitutional basis for various privacy-related rights, including the RTBF. The judgment marked a significant shift in Indian jurisprudence, affirming that privacy is a fundamental right, which could influence future discussions on data protection and the RTBF.

Following the 2017 judgment, this case further explored aspects of privacy, particularly in relation to data protection. Although it primarily focused on the Aadhaar scheme's implications, the discussions extended to broader privacy issues, including data security and individual rights over personal information.

The court recognized that the Right to be Forgotten is an aspect of privacy, emphasizing that individuals have the right to control their personal information and seek its removal under certain conditions. This case underscored the importance of protecting personal data and reinforced the idea that privacy encompasses the right to remove or control one’s personal data.

JUSTICE K.S. PUTTASWAMY (RETD.) VS. UNION OF INDIA & ORS. (2019): RTBF AS AN ASPECT OF PRIVACY

The 2019 case, often referred to as Puttaswamy II, built upon the Supreme Court's 2017 decision in the original Puttaswamy case. This case continued to address issues of privacy, particularly in the context of data protection and the implementation of the Aadhaar biometric identification system. It explored the intersection of privacy with other constitutional rights and data protection laws.[7]

The petitioners argued that the Aadhaar system infringed upon privacy rights, including the right to be forgotten. They contended that individuals should have control over their personal data, including the right to request its deletion when it is no longer necessary or relevant.

The Supreme Court reiterated that the right to privacy is a fundamental right under Article 21 of the Constitution, as established in the 2017 Puttaswamy judgment. This affirmation provided a strong constitutional basis for privacy-related claims, including RTBF. By reinforcing privacy as a fundamental right, the court supported the argument that individuals should have control over their personal data, including the right to request its removal. This laid the groundwork for recognizing RTBF as an aspect of privacy.

The court acknowledged that privacy encompasses various aspects, including data protection. This includes the right to be forgotten, which allows individuals to seek the deletion of their personal data under certain conditions. The judgment highlighted the need for a robust legal framework to protect privacy and manage data effectively. It underscored that the right to be forgotten is part of the broader right to privacy and should be implemented in a manner that aligns with constitutional guarantees.

The court recognized the need to balance privacy rights with other fundamental rights, such as freedom of speech and expression. This balancing act is crucial for implementing RTBF, as it involves removing personal data without unduly infringing upon public access to information. The judgment suggested that any RTBF provisions must be carefully regulated to ensure they do not excessively restrict freedom of expression or hinder legitimate public interests.

The 2019 ruling influenced subsequent data protection legislation in India, including the Digital Personal Data Protection Act (DPDP) 2023. By affirming privacy and RTBF as integral rights, the court's decision provided

[7] Justice K.S.Puttaswamy(Retd) vs Union Of India AIR 2018 SC 237 (India)

impetus for creating comprehensive data protection laws that include RTBF provisions.

The Justice K.S. Puttaswamy (Retd.) vs. Union of India & Ors. (2019) case was pivotal in establishing the Right to be Forgotten (RTBF) as an aspect of privacy under the Indian Constitution. By reaffirming privacy as a fundamental right, the Supreme Court supported the inclusion of RTBF within the broader framework of privacy rights. The judgment highlighted the need to balance privacy with other rights, influenced subsequent data protection legislation, and emphasized practical considerations for implementing and enforcing RTBF. This case marked a significant development in recognizing and upholding the right to data protection and privacy in India.

SHREYA SINGHAL V. UNION OF INDIA (2015)

The case challenged the constitutionality of Section 66A of the Information Technology Act, 2000, which criminalized online content deemed "offensive" or "annoying" and allowed for the arrest of individuals posting such content. This provision was criticized for being overly broad and infringing upon the fundamental right to freedom of speech and expression.[8]

The Supreme Court struck down Section 66A, ruling that it was unconstitutional. The court found that the provision was too vague and lacked adequate safeguards, which could lead to arbitrary and excessive restrictions on free speech.

The judgment highlighted the importance of balancing privacy with freedom of speech and expression. Although it did not directly address RTBF, it set a precedent for how data protection laws must navigate between individual rights and public interests.

By striking down the broad restrictions on online content, the case emphasized the need for precise and reasonable limitations on data and content management. This principle is crucial for RTBF, which involves removing personal data while respecting the broader public's right to information.

INDIAN MEDICAL ASSOCIATION V. V.P. SHANTHA (1995)

The case dealt with issues of medical negligence and the disclosure of patient information. The petitioner argued that the medical practitioners failed to maintain the confidentiality of medical records and caused harm by breaching privacy. The Supreme Court addressed the standards of care required from medical professionals, focusing on their obligation to maintain patient confidentiality and handle personal data responsibly.[9]

This case is significant in establishing the importance of privacy in handling personal medical information. While it did not address RTBF directly, it underscored the necessity of protecting sensitive personal data, which is a key aspect of RTBF.

The ruling reinforced the concept that privacy is a crucial component of personal dignity and autonomy, thereby supporting the broader argument for the RTBF. It highlights the need for stringent data protection standards in sensitive fields.

GOOGLE LLC V. UNION OF INDIA (2021)

This case involved Google's handling of data removal requests and compliance with Indian data protection laws. The focus was on how international tech companies manage RTBF requests in accordance with local regulations and their obligations to remove personal data when requested. The case examined Google's compliance with Indian legal standards for data removal and the practical challenges faced by multinational companies in implementing RTBF provisions. The court's decision addressed the alignment of international data practices with Indian laws.

This case is pivotal in understanding how RTBF principles are applied across borders. It addressed the challenges multinational corporations face when complying with local data protection laws, offering insights into practical RTBF implementation.

The ruling contributed to clarifying the expectations for RTBF compliance, particularly for global companies operating in India. It emphasized the need for clear procedures and legal frameworks to manage data removal requests effectively.

These cases collectively contribute to the broader understanding of the Right to be Forgotten (RTBF) and data

[8] Shreya Singhal vs U.O.I AIR 2015 SC 1523 (India).
[9] Indian Medical Association vs V.P. Shantha & Ors 1996 AIR 550(India).

protection and also illustrates the evolving nature of privacy rights and data protection in India, highlighting the ongoing need to balance individual rights with broader societal interests.

COMPARATIVE ANALYSIS OF THE RIGHT TO BE FORGOTTEN (RTBF)

EUROPEAN UNION

GDPR AND THE COSTEJA RULING:

The GDPR, effective from May 25, 2018, sets a robust framework for data protection in the EU. Article 17 of the GDPR, commonly known as the "Right to Erasure" or RTBF, allows individuals to request the deletion of their personal data when it is no longer necessary for the purposes for which it was collected, when consent is withdrawn, or when the data is processed unlawfully.[10]

Costeja Ruling in the 2014 landmark decision, the European Court of Justice ruled that search engines are responsible for removing links to outdated or irrelevant information about individuals upon request. The ruling established that individuals have the right to request the removal of links to pages containing personal data that is no longer relevant, effectively embedding the RTBF into the EU legal framework.[11]

ENFORCEMENT MECHANISMS AND PRACTICAL OUTCOMES:

Enforcement is carried out by national Data Protection Authorities in each EU member state. These authorities are responsible for handling complaints, conducting investigations, and ensuring compliance with GDPR provisions, including RTBF.

The GDPR and Costeja ruling have led to significant practical outcomes. Search engines and online platforms are required to implement RTBF requests, though the process can be complex. There have been numerous cases where the scope of RTBF has been tested, leading to ongoing debates about its limitations and the balance with other rights, such as freedom of information.

B. UNITED STATES

FIRST AMENDMENT CHALLENGES AND LACK OF FORMAL RTBF:

The U.S. Constitution's First Amendment guarantees freedom of speech and press, which often conflicts with RTBF principles. In the U.S., there is no federal law equivalent to the GDPR's RTBF, and privacy rights are generally considered secondary to free speech and information dissemination.

Unlike the EU, the U.S. does not have a comprehensive RTBF framework. The absence of such a right is partly due to the strong emphasis on freedom of expression and the belief that data removal can infringe upon public access to information.[12]

ALTERNATIVE MECHANISMS:

California Consumer Privacy Act (CCPA) enacted in 2018, the CCPA grants California residents' certain privacy rights, including the right to access, delete, and opt-out of the sale of their personal data. While not a direct equivalent of RTBF, it offers similar provisions related to data deletion within the scope of consumer privacy.[13]

Various U.S. states have enacted privacy laws with provisions for data deletion, but these are often limited in scope and do not provide a comprehensive RTBF similar to the GDPR. For instance, some states have specific laws for medical records or online consumer data, but these are not as broadly applicable as the GDPR's RTBF.[14]

COMMON LAW JURISDICTIONS:

UNITED KINGDOM:

Post-Brexit, the UK has retained GDPR principles through the Data Protection Act 2018, which includes provisions for the RTBF. The UK's implementation aligns

[10] GDPR art. 17
[11] Hillary C. Webb, People Don't Forget: The Necessity of Legislative Guidance in Implementing a U.S. Right to Be Forgotten, 85 GEO. WASH. L. 1318, 1319(2017).
[12] Wolford, B. (2018). Everything You Need to Know About the 'Right to be Forgotten' *(Aug 19, 2024*, 9:25 PM) (https://gdpr.eu/right-to-be-forgotten/.
[13] California Consumer Protection Act, 2018
[14] Intersoft Consulting (2018). *General Data Protection Regulation (GDPR) – Final text neatly arranged*. (Aug 19, 2024, 9:30 PM) General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/right-to-be-forgotten/.

with GDPR requirements, allowing individuals to request the removal of their personal data under similar conditions.[15]

The UK's approach reflects the EU model, with enforcement handled by the Information Commissioner's Office (ICO). The RTBF is applied in practice, though there are debates about its impact on freedom of expression and media reporting.

CANADA:

Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's PIPEDA includes provisions for individuals to access and request corrections to their personal data, but it does not explicitly provide a RTBF. Privacy rights under PIPEDA are less comprehensive regarding data removal compared to the GDPR.

Recent discussions and legislative developments, such as the Digital Charter Implementation Act, 2020, suggest that Canada may explore more robust data protection measures, potentially including RTBF-like provisions in the future.

CONCLUSION

The Right to be Forgotten is a significant advancement in data privacy, giving people more control over their personal information. While the EU has implemented a comprehensive RTBF framework under the GDPR, other regions, such as the United States and Canada, are still developing their methods. In India, the DPDP Act 2023 is a significant step toward incorporating RTBF principles into its legislative framework, mirroring a global trend toward improved data protection. Balancing RTBF with other rights, like as free speech, remains a significant concern that must be carefully considered in legislative and judicial situations.

The Right to be Forgotten (RTBF) faces notable challenges, particularly in balancing privacy with freedom of speech, as mandated by Article 19(1)(a) of the Indian Constitution. The tension between removing personal data and maintaining public access to information can lead to potential censorship and restrict public scrutiny. Enforcement issues include subjective judgments on data relevance, inconsistencies due to global jurisdiction, and resource constraints for managing RTBF requests. Developing precise legal frameworks and effective implementation mechanisms is crucial to navigate these complexities and ensure fair application.

The European Union's General Data Protection Regulation (GDPR) establishes a robust framework for the Right to be Forgotten (RTBF) under Article 17, which specifies conditions for data deletion. Individuals can request removal if their data is no longer needed for its original purpose, if consent has been withdrawn, or if processing is unlawful. Data controllers are obligated to act on these requests without undue delay and ensure compliance with the GDPR. This regulation has set a global benchmark, influencing other countries to adopt similar data protection laws. The GDPR also ensures a balance by not granting an absolute RTBF; it weighs this right against other fundamental rights, such as freedom of expression and public interest, ensuring that data removal requests are fair and contextually justified. This comprehensive approach promotes a consistent and practical application of data protection principles worldwide.

The future of the Right to be Forgotten in India requires a delicate balance between safeguarding individual privacy and ensuring transparency. The recent enactment of the DPDP Act signifies a big step forward in data protection by putting RTBF concepts into Indian legislation. However, successful adoption will necessitate overcoming technological hurdles, guaranteeing effective enforcement, and balancing private and public interest.

As India navigates these complications, continuous judicial interpretations, legislative changes, and public awareness campaigns will all play important roles in determining the future of RTBF. The goal will be to create a legislative and regulatory environment that protects individual privacy while protecting transparency and freedom of information.

REFERENCES

PRIMARY SOURCES

1. Constitution of India, 1950 Acts of Parliament (1950). India.
2. The Information Technology Act, 2000 No. 21, Acts of Parliament (2002) India.
3. The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) Acts of Parliament (2023) India

[15] Hillary C. Webb, People Don't Forget: The Necessity of Legislative Guidance in Implementing a U.S. Right to Be Forgotten, 85 GEO. WASH. L.1308, 1309-1311 (2017).

4. California Consumer Protection Act, 2018
5. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González EU:C: 2014:317 (Google Spain)
6. General Data Protection Regulation, 2018
7. Indian Medical Association vs V.P. Shantha & Ors 1996 AIR 550(India).
8. Justice K.S.Puttaswamy (Retd) vs Union Of India AIR 2018 SC 237 (India)
9. Shreya Singhal vs U.O.I AIR 2015 SC 1523 (India).

SECONDARY SOURCES

1. M P Jain, Indian Constitutional Law. (7th ed., Lexis-Nexis Butterworth Wadhwa Publications, Nagpur, 2016)
2. D. D. Basu Commentary on The Constitution of India, (8th ed., Lexis Nexis Butterworth Wadhwa Publications, Nagpur, 2008)
3. Hillary C. Webb, People Don't Forget: The Necessity of Legislative Guidance in Implementing a U.S. Right to Be Forgotten, 85 GEO. WASH. L. REV. 1304, [xii] (2017).
4. Prashant Mali Privacy Law: Right to Be Forgotten in India Privacy Law: Right to Be Forgotten In India. 1-2 (2022).
5. Jamal (2022). *Right To Be Forgotten: Meaning, Evolution, And Its Legality In India*.
6. Ajay Pal Singh; Rahil Setia, Right to be Forgotten - Recognition, Legislation and Acceptance in International and Domestic Domain, 2018, NULJ. (2018).

ONLINE RESOURCES

1. Ahmad, Z. (2022). Articles – Manupatra. articles.manupatra.com. https://articles.manupatra.com/article-details/Right-to-be-forgotten