International Research Journal of Commerce and Law
Volume 13 Issue 04, April 2025 ISSN: 2349-705X Impact Factor: 8.893
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

RIGHT TO BE FORGOTTEN: A SUBSET OF RIGHT TO PRIVACY

Dr. Poonamdeep Kaur[1] , Ms. Prerna[2]

[1]Assistant Professor, Department of Laws, Guru Nanak Dev University, Regional Campus, Jalandhar, Punjab,144012, India.

[2]Research Scholar, Department of Laws, Guru Nanak Dev University, Amritsar, Punjab, 143005, India.

Email: Poonam1246@gmail.com , Prernadogra99@gmail.com

ABSTRACT

The Right to be Forgotten (RTBF), a key component of data protection law, has gained a lot of attention in the digital age. As a part of the Right to Privacy, it allows individuals to request the removal of personal information from online platforms to protect their privacy, dignity, and digital identity. This paper critically investigates the philosophical and legal foundations of RTBF in the Indian context, where its history is interwoven with broader privacy rights law. The Supreme Court's recognition of the Right to Privacy as a basic right in *K.S. Puttaswamy v. Union of India* paved the way for RTBF, emphasising the importance of privacy protection in a fast digitising society.

Judicial interpretation of RTBF in India emphasises its growing importance in mitigating the problems connected with the constant availability of online information. In *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.*, the Delhi High Court recognised RTBF and imposed an interim injunction against the republication of defamatory content, emphasising the need of protecting individual dignity. This case was a watershed point in Indian jurisprudence since it recognised RTBF while balancing it against other constitutionally given rights, such as freedom of expression and the right to know. Courts have emphasised that RTBF rulings must balance opposing interests in order to maintain justice and avoid excessive information suppression.

Legislative changes, particularly the Digital Personal Data Protection Act of 2023, have influenced the RTBF discussions in India. This act gives individuals the right to request the correction or erasure of personal data, bringing Indian data protection regulations in line with international norms like the GDPR. Despite this improvement, there are still difficulties regarding the application of RTBF in circumstances involving public interest, historical value, or journalistic freedom, leaving much to judicial discretion.

The study claims that RTBF is critical for protecting individual privacy in the digital age, but it requires strong judicial norms and legislative clarity to be effective. This study adds to the continuing discussion about privacy, data protection, and the balancing of individual and collective rights in emerging democracies by positioning RTBF within India's constitutional and socio-legal frameworks.

Introduction - Tracing the Origin

The Right to Be Forgotten (RTBF) is a legal concept that allows people to request that personal information be removed, de-indexed, or erased from the internet, particularly from search engines and online platforms, if it is deemed outdated, irrelevant, or harmful to their reputation or privacy. The right owes it existence to the rapid use of technology. The right is based on the idea of providing people more control over their digital identities and guaranteeing that the persistence of information on the internet does not jeopardise their life and dignity.

The concept of the Right to be Forgotten, also known as the Right to Erasure, emerged in the digital era following a significant ruling by the European Union Court in 2014. This ruling was part of the well-known case of Google Inc. v. Agencia Española de Protección de Datos, involving Mario Costeja González. The European Court of Justice concluded that individuals have the right to request search engines to de-index personal information that is no longer relevant or required under data protection laws particularly if it infringes upon their privacy. This decision, codified in the European Union's General Data Protection Regulation (GDPR) under Article 17, became a global reference point for RTBF discussions. Article 17 of the GDPR specifies certain situations under which an individual can apply for the erasure of his personal data. Specifically, individuals have the right to have their data erased under the following conditions:

1. The data is no longer required for the purposes for which it was initially collected or processed.

2. The organization is basing its data processing on the individual's consent, and the individual chooses to withdraw that consent.

3. The organization cites legitimate interests as the reason for processing, the individual raises an objection to this, and there is no compelling reason for the organization to continue processing the data.

4. The organization is processing personal data for direct marketing and the individual objects to this activity.

5. The organization has unlawfully handled the individual's personal data.

6. The organization is obligated to delete personal data to comply with a legal mandate.

7. The organization has processed personal data belonging to a minor to provide online services.

These conditions highlight the framework established to allow individuals to regain authority over their personal data in a rapidly evolving digital landscape.

RIGHT TO BE FORGOTTEN A SUBSET OF RIGHT TO PRIVACY

The right to privacy in India has evolved greatly throughout time, influenced by legal interpretations, constitutional conflicts, and sociological shifts. Although not officially stated in the Indian Constitution, the right to privacy is drawn from the fundamental rights guaranteed in Part III of the Constitution. Its evolution reflects India's efforts to strike a balance between individual liberties and governmental interests in a fast changing sociolegal environment.

1. **Early Developments in Indian Jurisprudence**
   In India, disputes about personal freedom and political authority led to the establishment of privacy as a legal right. Early legal frameworks, such as the Indian Penal Code of 1860, implicitly recognised privacy in provisions dealing with trespass, defamation, and communication confidentiality. However, privacy remained an underdeveloped idea in Indian law until the mid-twentieth century.
2. **Privacy as a Fundamental Right : Initial Resistance**
   The first notable case addressing the question of privacy was ***M.P. Sharma v. Satish Chandra***. The Supreme Court determined that privacy is not a basic right, citing the lack of clear constitutional protections. Similarly, in ***Kharak Singh v. State of Uttar Pradesh.*** the Court rejected the concept of privacy as a basic right, but it did strike down the practice of domiciliary visits as a breach of personal liberty under Article 21.
3. **The Turning Point: Progressive Interpretation**
   The concept of privacy underwent a revolutionary transition in the late twentieth century, fuelled by court activism and cultural awareness. Courts began to interpret Article 21 of the Constitution, which guarantees the right to life and personal liberty, in a more expansive and inclusive manner. In ***R. Rajagopal v. State of Tamil Nadu***, often known as the "Auto Shankar case," the Supreme

Court recognised that the right to privacy is implied in Article 21. The Court ruled that the right to privacy includes the protection of an individual's personal information from being published without their agreement, a significant step forward in Indian privacy law.

4. **The Puttaswamy Judgment: Privacy as a Fundamental Right**

The key case that established privacy as a basic right in India was ***Justice K.S. Puttaswamy (Retd.) v. Union of India***. A nine-judge bench of the Supreme Court unanimously ruled that the right to privacy is inextricably linked to the right to life and personal liberty under Article 21 and is also protected by Articles 14 and 19. This case reversed previous precedents such as ***M.P. Sharma and Kharak Singh***, broadening the definition of privacy to include personal autonomy, bodily integrity, data protection, and informational privacy. It also laid the groundwork for contesting privacy-infringing laws and practices, such as the Aadhaar program's obligatory biometric data collecting.

5. **Privacy in the Digital Age**

With the advent of technology and widespread use of the internet, privacy concerns in India have shifted towards data protection, surveillance, and digital rights. The Supreme Court has addressed privacy issues in cases involving the Aadhaar scheme, social media regulation, and surveillance laws like the Information Technology Act, 2000.

The Personal Data Protection Bill, first introduced in 2019, aims to codify privacy rights in India by regulating the collection, storage, and use of personal data. Inspired by global frameworks like the European Union's GDPR, the bill seeks to establish a comprehensive legal regime for data protection while balancing privacy with national security and economic development. In the year 2024, by the passing of the Digital Personal Data Protection Act 2023, the government has expressly provided the citizens the Right to erasure of their personal data under section 12 of the Act though not specifically using the word the Right to be Forgotton, on the lines of Article 17 of the European Union's General Data Protection Regulation (GDPR). The evolution of the right to privacy in India illustrates the dynamic interplay between constitutional interpretation, technological advancements, and societal change. From being denied recognition in the early years to becoming a fundamental right through the Puttaswamy judgment, privacy in India has grown to encompass diverse aspects of personal liberty and autonomy. As India continues to grapple with challenges in data protection, surveillance, and technological governance, the right to privacy remains a crucial pillar of its democratic framework.

There is a significant distinction between the Right to be Forgotten and the traditional Right to Privacy. The Right to Privacy focuses on taking legal action against individuals or entities that infringe upon one's personal information, specifically targeting the offending parties. In contrast, the Right to be Forgotten involves the comprehensive and lasting removal of specific information from the internet, making it inaccessible to users worldwide, regardless of their location. Furthermore, the Right to be Forgotten is distinct from the right to correct misinformation or assert the truth, which falls under legal protections concerning claims of libel and slander. Essentially, the Right to be Forgotten operates as a mandated omission, aiming to render certain information increasingly difficult to find and access in the digital realm.

CHALLENGES IN IMPLEMENTING THE RIGHT TO BE FORGOTTEN (RTBF) IN INDIA

Implementing the Right to Be Forgotten (RTBF) in India involves several challenges that span legal, technological, ethical, and economic issues. These challenges must be addressed to ensure that the right is effectively enforced while balancing other competing rights and interests.

A. LEGAL CHALLENGES

1. ***Absence Of A Clear Statutory Framework:*** India does not yet have a particular statute concerning RTBF. While private rights are recognised in the Right to private (Article 21 of the Constitution), no separate statute defines the scope and processes for RTBF. This lack of clear legal rules creates doubt about how the right should be implemented and leaves persons without a clear path to seek remedy.
2. ***Inconsistent judicial interpretations:*** The Indian judiciary has failed to develop standard norms governing RTBF. As courts interpret private rights in various settings, the legal criteria for enforcing RTBF change. For example, balancing privacy with conflicting rights, such as freedom of speech and the right of the public to know, makes developing a uniform strategy challenging. Inconsistent interpretations result in legal consequences that are confusing and unpredictable.
3. ***Lack Of An Enforcement Mechanism:*** While privacy rules exist, India lacks a recognised regulatory authority to handle RTBF requests. The implementation of RTBF is scattered due to a lack of a central authority and clearly defined enforcement measures. Many internet platforms, particularly multinational corporations, may ignore or postpone compliance with RTBF-related Indian court judgements, complicating enforcement.

B. TECHNOLOGICAL CHALLENGES

1. ***Issues With De-indexing And Data Deletion:*** One of the most critical technological concerns is the persistence of internet data. Even when a request is made to remove or de-index specific material, this is frequently insufficient. Data may be cached, preserved, or mirrored across several platforms, search engines, and social media, making total erasure impossible. This problem is exacerbated by the growing rate of digital material sharing and storage, which makes full de-indexing or deletion a difficult and resource-intensive job.
2. ***Cross-border Jurisdiction Issues:*** Enforcing RTBF is especially difficult because of the internet's worldwide reach. Online data is frequently stored on servers located outside of India, making it harder to enforce Indian data removal rules. Global IT corporations may operate under distinct legal frameworks in different nations, therefore an RTBF request filed in India may be ineffective in other jurisdictions. Furthermore, some corporations may fail to comply with Indian court rulings owing to differences in rules in their home countries, complicating efforts to enforce the right on a worldwide basis.
3. ***Lack of Standardised Procedures:*** There is presently no globally agreed technique for online platforms to handle RTBF requests. Each platform may take its own strategy, resulting in variance in how requests are handled. Because of the lack of defined technological criteria, certain systems may be unable to properly handle data removal, while others may struggle to meet legal requirements. This lack of standardisation causes inefficient implementation and further delays in handling RTBF claims.

C. ETHICAL AND SOCIAL CHALLENGES

1. ***Concerns Over Censorship:*** One of the most serious ethical problems with RTBF is its possible use as a weapon for censorship. Individuals can ask for the removal of factual but unpleasant or embarrassing material that could alter public records and history. This raises the prospect that persons in positions of authority would utilise RTBF to hide material that could affect their image or career, undermining openness and accountability.
2. ***Impact On Free Expression:*** The Right to Be Forgotten may conflict with freedom of expression, especially in the media or public discourse. Individuals may find something inconvenient, yet it is nonetheless of public interest or vital for open debate. The widespread usage of RTBF may result in a chilling effect, in which people or media outlets are unwilling to voice ideas or report on

sensitive matters for fear of having their material erased. This may hamper the free flow of ideas and social discourse on crucial issues.

3. ***Distortion of Historical Record:*** Excessive removal of online information could affect the preservation of historical records. Important events, controversies, and political decisions are often documented online. If historical content is removed under RTBF, future generations may be deprived of crucial context that helps them understand past events. This raises concerns about potential revisionism, where individuals may erase or alter inconvenient facts, leading to the loss of collective memory.

D. ECONOMIC CHALLENGES

1. *Implementation Costs for Private Entities:* The expense of implementing RTBF is a considerable problem for private enterprises, particularly small and medium-sized ones. Platforms would need to set aside resources to create and maintain systems capable of handling data removal requests, ensuring compliance with RTBF requirements, and managing any legal issues. These costs might become prohibitively expensive, particularly for smaller technology businesses that may lack the capacity to properly comply with RTBF.

2. *Legal And Regulatory Costs:* Businesses who do not follow RTBF laws face serious financial consequences. Companies that fail to comply with RTBF-related decisions may risk fines or legal action, which would increase their operational expenses. Furthermore, firms will need to engage legal experts and implement compliance systems to address RTBF demands, increasing their regulatory burden. This can put a burden on financial resources, particularly for startups and smaller technology enterprises functioning in an increasingly complicated regulatory environment.

3. *Balancing RTBF with Innovation:* Enforcing RTBF may conflict with the innovation-driven nature of digital platforms. Social media sites and search engines rely heavily on user-generated data to power their revenue models. Implementing tight data removal processes may limit their capacity to innovate or provide personalised services like targeted advertising or suggestions. Balancing privacy protection with the need for corporate innovation is a difficult task, especially when it comes to the economic viability of data-driven businesses.

COMPARISON WITH OTHER COUNTRIES

United States

The United States has no explicit RTBF statute. The privacy rules in the United States are fragmented, with sector-specific requirements (for example, HIPAA for healthcare data and COPPA for children's data). RTBF is not usually recognised as a fundamental right under US law, and the First Amendment frequently takes precedent over privacy concerns in regards of data and speech. There is no federal mandate for RTBF in the United States, therefore enforcement falls to individual states or sectoral regulations. The Federal Trade Commission (FTC) enforces some privacy safeguards but does not have a mandate for RTBF. The United States prioritizes free expression and the ability to access information, which frequently limits the use of RTBF. There is no widespread legal acknowledgment of this right, and efforts to adopt RTBF encounter.

Brazil

Brazil's General Data Protection Law (LGPD), enacted in 2020, incorporates provisions similar to the GDPR, including the right to data deletion. Individuals have the right under the LGPD to request that obsolete, irrelevant, or improperly processed data be removed, which is consistent with RTBF principles. Brazil's National Data Protection Authority (ANPD) is in charge of implementing data protection regulations, including RTBF. Noncompliance with data protection requirements may result in penalties and punishments from this body. Brazil's approach to RTBF is based on the EU's GDPR, which provides a complete framework for both people and corporations. The LGPD, like the European model, strives to strike a balance between data protection and economic interests.

European Union

The General Data Protection Regulation (GDPR) is the cornerstone of RTBF in the EU. Article 17 of GDPR grants individuals the right to request the deletion of personal data when certain conditions are met. The EU framework provides clear guidelines and is enforceable across all member states. The GDPR includes provisions for cross-border enforcement, allowing for the removal of data even if the data controller is outside the EU, though enforcement remains complex for non-EU-based platforms. The EU's RTBF approach is comprehensive and legally robust, with a strong emphasis on data protection and privacy rights.

It has become a global standard for RTBF implementation, offering a structured legal framework for individuals to exercise this right.

United Kingdom

After Brexit, the United Kingdom retained key principles of the European Union's General Data Protection Regulation (GDPR) by introducing its own version, the UK GDPR, under the Data Protection Act of 2018 (DPA 2018). The UK GDPR includes the Right to Be Forgotten (RTBF), which allows individuals to request the deletion of personal data under specific circumstances, such as when the data is no longer necessary, was processed unlawfully, or when consent has been withdrawn. This right provides individuals with greater control over their personal information in the digital age.

The Information Commissioner's Office (ICO) is responsible for enforcing the RTBF in the UK. It plays a critical role in ensuring compliance with the UK GDPR, offering guidance on data protection laws and imposing fines or penalties for noncompliance. Although the UK operates independently from the EU, its approach remains closely aligned with the GDPR, maintaining a robust legal framework to balance privacy rights and public interest while enabling individuals to safeguard their digital identity.

Australia

Australia does not have a formal Right to Be Forgotten (RTBF) statute, but it does provide privacy protections under the Privacy Act of 1988. This legislation includes provisions for the modification and deletion of personal data, though these measures are narrower in scope compared to the RTBF as recognised in jurisdictions like the European Union. Individuals may request corrections or deletions of data that is inaccurate or outdated, but there is no comprehensive framework granting the right to request erasure of personal information.

The Office of the Australian Information Commissioner (OAIC) is responsible for enforcing privacy regulations in Australia. The OAIC primarily focuses on resolving privacy complaints and ensuring compliance with the Privacy Act rather than enforcing a formal RTBF. The emphasis in Australian privacy law is on data access and rectification, granting individuals the ability to view and correct their personal data, rather than broad rights for erasure or de-indexing. While Australia offers robust data protection measures, its approach does not formally recognise or prioritise RTBF.

International Research Journal of Commerce and Law
Volume 13 Issue 04, April 2025 ISSN: 2349-705X Impact Factor: 8.893
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

THE RIGHT TO BE FORGOTTEN – A CASE STUDY OF TAIWAN'S LEGAL APPROACH

Introduction

The Right to Be Forgotten (RTBF) is a relatively recent notion in privacy legislation that enables persons to seek the deletion of personal information that is no longer relevant or essential. The right is based on data protection and privacy rules, which allow individuals to retake control over their digital traces. However, this right frequently conflicts with other fundamental rights, such as free expression and the public's right to know, making its implementation a complex and contentious matter in many jurisdictions. This chapter looks at a major case in Taiwan involving the RTBF, focussing on its legal consequences, the court procedure, and the balancing of privacy and free speech.

Case Background

In a prominent instance, Mr. A, a former public figure, attempted to assert his Right to Be Forgotten following the online disclosure of information about his involvement in a match-fixing scandal. Mr. A requested that specific search results for his name be removed from Google's search engine, claiming that they injured his reputation and no longer served the public interest. However, both Taiwan's first and second instance courts denied Mr. A's motion, citing the factual correctness of the material as well as the data's public nature.

Opinion of Taiwan Supreme Court

The Taiwan Supreme Court reviewed the case and agreed with the lower courts on the factual disputability of the content in question under Article 11 of the Personal Data Protection Act (PDPA). However, the Supreme Court determined that the lower courts did not fully evaluate essential aspects in establishing whether the search engine's conduct went beyond the "necessary scope of purpose" in data collecting and processing. These factors include:

- The nature of the search engine's service.
- The impact of deleting the search results on public access to information.
- The public significance of the disputed content at the time of publication.
- The degree of harm to Mr. A's privacy.
- The extent of Mr. A's role as a public figure.

The Supreme Court emphasised that these components required more scrutiny, as lower courts may have disregarded them in their decision-making. As a result, the matter was sent to the Taiwan High Court for re-adjudication.

Taiwan High Court's Judgment on Remand

Upon re-examination, the Taiwan High Court considered various factors before ruling on Mr. A's request to delete the search results. Notably, the court assessed the nature of the online content, the public's right to know, and the balance between public interests and the plaintiff's privacy rights.

Obscene Online Article: One of the search results in question was an online article that used derogatory language towards Mr. A. The article provided no factual allegations, but rather expressed emotional displeasure. The High Court found that such content was more about emotional expression than factual reporting. The court found that removing this article would not violate the public's right to know because it lacked any significant informational value. The court also stated that the match-fixing scandal was no longer newsworthy since the event had lost commercial and public importance. As a result, the deletion of this article was justified under Article 11 of the PDPA.

Remaining Search Articles: The remaining search results focused on factual information about Mr. A's role in the match-fixing case, his fraudulent representations about his age and education, and general impressions of the occurrence. The court decided that these findings were relevant to public interests and satisfied the public's right to know. In addition, a public court judgement validated the data's factual accuracy. The court determined that keeping these search results did not cause Mr. A significant injury because the information was publicly available and met the public's informational needs.

The court finally found in favour of Google, stating that the majority of the search results did not exceed the "necessary scope" of data processing under the PDPA, with the exception of the inflammatory article, which should be erased.

The case of Mr. A provides a critical study of Taiwan's Right to Be Forgotten, demonstrating the difficulty of balancing individual privacy with the public's right to access information. Taiwanese courts agreed that the RTBF is a protected right, but limited its application. The legal principles developed in this case reflect thorough examination of matters such as public interest, factual accuracy, and the individual's function as a public figure.

While Taiwan has made strides in recognizing the RTBF under the Personal Data Protection Act, the case highlights the challenges of enforcing this right, particularly when it comes into conflict with free speech and the public's right to know. In Mr. A's case, the courts prioritized maintaining access to truthful, public information while affording privacy protections only when the content no longer served public interests or was harmful to the individual.

CONCLUSION

The Right to Be Forgotten (RTBF) is a significant aspect of privacy law in the digital age, reflecting the tension between an individual's right to privacy and the public's right to access information. This research paper has explored the RTBF from different perspectives, with a focus on the Indian perspective and a comparative analysis with other global jurisdictions.

The RTBF has become an increasingly important concern in India, particularly with the advent of digital platforms and the growing demand for data protection. Although the Indian Constitution provides the right to privacy, there is currently no comprehensive legislative structure to handle the RTBF. The proposed Personal Data Protection Bill (PDPB) aims to close this gap by giving individuals more control over their personal data. However, there are still issues in combining the RTBF with free speech and the public's right to know, particularly in a country with different sociopolitical circumstances and a lively media ecosystem.

This article highlights the many approaches to the RTBF by examining issues, legislative frameworks, and case studies from nations such as the European Union, the United States, Brazil, Taiwan, and others. The EU's rigorous General Data Protection Regulation (GDPR) provides the most complete blueprint for RTBF implementation. The United States, on the other hand, traditionally values free expression over privacy, making RTBF allegations more difficult to make. In contrast, nations like as Brazil and Taiwan have taken more balanced measures, acknowledging the relevance of both private and public interest concerns.

The research also discussed the legal, technological, ethical, and economic challenges that hinder the smooth implementation of RTBF, especially in countries like India, where there is an urgent need for clear and uniform legal standards. These challenges include issues of data de-indexing, cross-border jurisdiction, and concerns about censorship. Additionally, economic considerations, such as the cost of compliance for private entities, play a critical role in shaping the practical application of RTBF.

In conclusion, while the Right to Be Forgotten holds significant promise as a tool for protecting individual privacy in the digital age, its implementation requires a careful, balanced approach. As digital information continues to expand and the line between public and private life becomes increasingly blurred, the RTBF will continue to be a central issue in privacy law. For countries like India, a nuanced legal framework that considers both privacy rights and the public interest is essential for ensuring that the RTBF is applied fairly and effectively, promoting both individual dignity and freedom of expression in the digital age.

REFERENCES

A. BOOKS

1. Franz Werro, A comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia (Springer, 2020).
2. Md. Zishan Khan, Right to be forgotten in India: Evolution and Present position (Kindle edition)
3. Paul Lambert, *The right to be forgotten* (Bloomsbury Professional Law ,2023)
4. Uta Kohl, *The right to be forgotten in Data Protection law and two western culture of privacy* (Cambridge University Press , 2023)

B) JOURNALS

1. Dr.Jyoti J. Mozika , "**.** Integrating the Right to be Forgotten in the Indian Legal Framework in the Light of Experiences from the European Union" XII *Indian Journal of Law and Justice* (2024)

2. Swaathi R., "The right to be forgotten in India: Balancing privacy and free speech"IV *Journal of Legal research and Juridical Sciences*(2025)

3. Bhargav Chaganti, " The right to be forgotten: A comparative analysis of the GDPR and the DPDPA" XII *International Journal of Creative Research Thoughts* (2024)

4. Dr. Arti & Debaditya Das**,** RIGHT TO BE FORGOTTEN IN INDIA– A CRITICAL ANALYSIS" 52 *Industrial Engineering Journal* (2023)

5. Harikartik Ramesh & Kali Srikari Kancherla, "Unattainable Balances: The Right to be Forgotten" IX *NLIU Law Review*(2023)

6. Poorvaja Subramanian & Anjali ViswanaathanI," Erasing The Past: The 'Right To Be Forgotten' In India - Progess, Pitfalls And Prospects"6 *International Journal for Multidisciplinary Research* (2024)

C) CASES

1.Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

3. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

4. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

5. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

6. Shi Jiang-Xin v. Google International LLC, 103 Su Zi No. 2976 (Taipei District Court, 2015).

7. Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd, 2019.

D) BAREACT/STATUES

1. The Bharatiya Nyaya Sanhita, 2023

2 The Bharatiya Nagarik Suraksha Sanhita, 2023

3 The Bharatiya Sakshya Adhiniyam, 2023

4 The Constitution of India

5. European Convention on Human Rights and Fundamental Freedoms, 1950, Art. 8.

6. General Data Protection Regulation, Art 17.

7. The Information Technology Act, 2000

8. The Digital Personal Data Protection Act, 2023.

E) NEWSPAPER

1. Aaratrika Bhaumik, On the 'right to be forgotten' from judicial records -Explained, *The Hindu*(Aug 07,2024).

2. Sofi Ahsan, Right to be forgotten: govt position, court rulings, and laws elsewhere, *The Indian Express*(Dec 27,2021)

3. Krishna Das Rajagopal, Right to Privacy is "intrinsic to life and liberty," rules SC, *The Hindu*(Nov 25,2022)

4. Krishna Das Rajagopal, SC Verdict on right to privacy: Judges demolish Centre's stand that privacy is elitist concept, *The Hindu*(Aug 24, 2017)