LAW AND SOCIAL POLICY REVIEW

VOLUME 2 AND ISSUE 1 OF 2024

INSTITUTE OF LEGAL EDUCATION

LAW AND SOCIAL POLICY REVIEW

APIS - 3920-0015 | ISSN - 2583-8180

(OPEN ACCESS JOURNAL)

Journal's Home Page – https://lspr.iledu.in/

Journal's Editorial Page - https://lspr.iledu.in/editorial-board/

Volume 2 and Issue 1 (Access Full Issue on - https://lspr.iledu.in/category/volume-2-and-issue-1-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

LAW AND SOCIAL POLICY REVIEW

VOLUME 2 AND ISSUE I OF 2024

APIS - 3920-0015 | ISSN - 2583-8180

Published by

Institute of Legal Education

https://iledu.in

EXAMINING THE RELEVANCE OF THE RIGHT TO BE FORGOTTEN IN PROTECTING INFORMATIONAL PRIVACY IN DIGITAL AGE

AUTHOR - VIKAS KUMAR* & DR. AMAN MALIK**, RESEARCH SCHOLAR* & ASSISTANT PROFESSOR** AT DEPARTMENT OF LAW, JAGANNATH UNIVERSITY

BEST CITATION – VIKAS KUMAR & DR. AMAN MALIK, EXAMINING THE RELEVANCE OF THE RIGHT TO BE FORGOTTEN IN PROTECTING INFORMATIONAL PRIVACY IN DIGITAL AGE, *LAW AND SOCIAL POLICY REVIEW,* 2 (1) of 2024, Pg. 14-21, APIS - 3920-0015 | ISSN - 2583-8180

ABSTRACT

The Right to Be Forgotten (RTBF) has emerged as a crucial mechanism for protecting informational privacy in the digital age, where personal data is continually collected, stored, and shared across a vast array of online platforms. This right allows individuals to request the removal of their personal information from search engines, databases, and websites, thereby regaining control over their digital footprints. The RTBF is particularly relevant in an era where the permanence of online data can have long-lasting consequences for individuals' privacy, reputation, and personal autonomy. As digital technology advances, so too do the risks associated with the widespread availability of personal information, including identity theft, data breaches, and unwarranted surveillance. The RTBF offers a means of mitigating these risks by empowering individuals to limit the accessibility of their personal data, especially when it is outdated, irrelevant, or harmful. This research paper examines the role of the RTBF (RTBF) in securing informational privacy in India, a country where digital technology is rapidly expanding and the collection and dissemination of personal data have become pervasive.

Keywords: Informational Privacy, Right to Privacy, Right to be Forgotten.

INTRODUCTION

The current world is witnessing an unprecedented and rapid expansion of technology. Each passing day brings new technological innovations that are revolutionizing the way people live, work, and communicate. The current era of technological innovation has brought about an unprecedented expansion of data storage on the internet.[1] While this has brought significant benefits in terms of research, analysis, and innovation, it has also created new challenges related to privacy and security.

With the rapid advancements in technology, there have been growing concerns about the privacy and security of personal data. In this context, the "RTBF" has gained significant attention. The simple and the precise articulation of the RTBF is that it is right that empowers the individuals to request for the removal of his personal information from the web.[2] The concept is based on the idea that individuals have the right to control their personal data and can request its deletion under certain circumstances. The unprecedented growth of the technological innovation has brought the option for the collection and the storage of the huge amount of the data and need for the mechanism where the data of the individuals should be safeguarded at the most. A wide range of data including from the personal details to the professional details are available online and may continue to be present till time immemorial if not removed.

[1] Shankar Dubey, Technology and Innovation Manangement 134 (PHI Learning Private Limited, 2nd edn., 2019)

[2] Ashley Nicole Vavra, "Right to be Forgotten: An Archival Perspective" 81 JSTOR 100- 106 (2019)

LAW AND SOCIAL POLICY REVIEW
VOLUME 2 AND ISSUE I OF 2024
APIS - 3920-0015 | ISSN - 2583-8180
Published by
Institute of Legal Education
https://iledu.in

The collection and storage of such data can pose a risk to individuals' privacy, as it can be used for identity theft, fraud, or other malicious activities. In today's digital age, our personal information is more accessible than ever before. With just a few clicks, anyone can find out a wealth of information about us, including our names, addresses, phone numbers, and even our political affiliations and religious beliefs. While this level of access can be useful in many ways, it can also be deeply concerning, especially when it comes to our personal privacy.

Moreover, personal data that is stored online can have a lasting impact on individuals' lives, even after they have moved on from a particular situation or event. For example, a negative review or comment that is posted online can have long-lasting consequences for an individual's reputation and career. In such cases, the RTBF can enable individuals to request the removal of such information, thereby protecting their privacy and reputation.

This research work provides a critical analysis of the different facets of the RTBF and its conflict with other rights. The conflict between the RTBF and other fundamental rights is complex, and this research work aims to provide a critical analysis of the balance that must be struck between them. In doing so, the research work considers a range of factors, including the accuracy and relevance of the information, the public interest in accessing the information, and the potential harm to individuals that may result from the publication of certain information. This research work seeks to provide a critical analysis of these issues and contribute to the ongoing debate surrounding the RTBF and its relationship with other fundamental rights, including "Freedom of Speech and expression" .

CONCEPTUAL ANALYSIS OF THE INFORMATIONAL PRIVACY

In India, the right to privacy has evolved significantly through judicial pronouncements. The landmark judgment by the SCin **Justice K.S. Puttaswamy (Retd.) v. Union of India**[3] recognized the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21 of the Indian Constitution. This ruling has profound implications, extending privacy protections to various aspects of personal life, including bodily autonomy, sexual orientation, and data protection. The decision marked a shift towards acknowledging individual autonomy and dignity in an increasingly digital world, where the protection of personal information from unwarranted state or private interference has become paramount. This has led to ongoing debates and legislative efforts to balance privacy rights with other competing interests, such as national security and public interest, highlighting the dynamic and evolving nature of privacy law in India.

Informational privacy, a part and parcel of the Right to Privacy, refers to the right of individuals to control the collection, use, and dissemination of their personal data, particularly in the digital age where data flows freely and rapidly across various platforms. This concept encompasses a broad spectrum of concerns, including how personal information is gathered, who has access to it, and how it is used, stored, or shared. The rise of the internet, social media, and big data analytics has exponentially increased the amount of personal information that is collected and stored by both public and private entities, often without the explicit consent of individuals. This data can include everything from basic identifiers like names and addresses to more sensitive information such as financial records, health data, browsing histories, and even biometric details. The concept of informational privacy is rooted in the belief that individuals should have autonomy over their personal information, with the ability to decide what is shared and with whom. However, in practice, this autonomy is increasingly challenged by the pervasive and often opaque nature of data collection practices. Companies and governments

[3] AIR 2018 SC 1841

LAW AND SOCIAL POLICY REVIEW
VOLUME 2 AND ISSUE I OF 2024
APIS - 3920-0015 | ISSN - 2583-8180
Published by
Institute of Legal Education
https://iledu.in

frequently harvest personal data for various purposes, including targeted advertising, market research, surveillance, and even predictive modeling, which can lead to the creation of detailed profiles that are used to influence behavior or decision-making. The erosion of informational privacy poses significant risks, including identity theft, discrimination, manipulation, and the loss of anonymity. Moreover, once personal data is shared or leaked online, it can be difficult, if not impossible, to completely erase, leading to long-term implications for individuals' privacy and security. As technology continues to evolve, with innovations such as artificial intelligence and the Internet of Things further increasing the amount and granularity of personal data being collected, the importance of safeguarding informational privacy becomes even more critical. Ensuring that individuals can maintain control over their personal information in this rapidly changing digital landscape is essential for protecting not only privacy but also the broader principles of autonomy, dignity, and freedom that are foundational to democratic societies.

CONCEPT AND THE HISTORICAL ROOT OF RTBF

The entire concept of the RTBF do not has long past rather it is a innovation of the present time. It came into picture after the popularization of the Internet and the issue of the huge stroge of data on the online platform.[4] It empowers people to protect their reputations, safeguard their personal information, and maintain control over their digital identities. It is a critical component of modern privacy law. It recognizes the importance of individual autonomy.

Article 17 of the "General Data Protection Regulation (GDPR)" elaborates that "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay". [5]

The jurisprudential aspect of the RTBF refers to the legal principles and reasoning that underpin the recognition of this right. At its core, the RTBF is based on the idea that individuals have a fundamental right to privacy, and that this right should include the ability to control their personal information. This right is typically grounded in constitutional law, international human rights law, and data protection laws, among other legal frameworks. From a jurisprudential perspective, the RTBF has been shaped by a number of landmark cases in various jurisdictions around the world. These cases have helped to establish the legal principles and criteria that are used to determine when and how the RTBF should be applied. For example, in the case of ***Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*** [6] (2014), The European Court of Justice (ECJ) determined that people have the right to ask search engine companies to take down links to personal information that is unreliable, insufficient, unnecessary, or excessive. The European Court of Justice (ECJ) has determined that the aforementioned entitlement is grounded on the fundamental "Right to Privacy" and data protection of the individual concerned. Furthermore, the ECJ has emphasized that this right must be weighed against the right to freedom of expression and information.

The RTBF is a relatively new concept in India's legal framework. The Indian legal framework currently lacks a specific law on the RTBF. However, it is widely recognized in several counties and EU is one of them. The concept of the RTBF was first proposed in Europe in the early 2000s. In 2006, a Spanish lawyer named Mario Costeja González filed a complaint with the Spanish Data Protection Agency (DPA) against Google, asking that the search engine

[4] Keith Markham, A Practical Guide to General Data Protection Regulation 45 (Law Brief Publishing, 2nd edn., India, 2018)

[5] Cristina Casagran, Global Data Protection in Field of Law Enforcement: An EU Perspective 56 (Routledge, 1st edn., 2018)

[6] ILEC 060 (CJEU 2014)

LAW AND SOCIAL POLICY REVIEW
VOLUME 2 AND ISSUE I OF 2024
APIS - 3920-0015 | ISSN - 2583-8180
Published by
Institute of Legal Education
https://iledu.in

remove links to a newspaper article from 1998 that mentioned a debt he had previously settled. Costeja argued that the information was no longer relevant and that it was causing him harm.

The Spanish DPA initially decided against Costeja, but he appealed the judgement, and the matter eventually reached the European Court of Justice (ECJ). ***Google Spain v. AEPD and Mario Costeja González***[7] was a significant decision in which the ECJ ruled in 2014 that users have the legal capacity to ask search engine companies to delete references to their personal information from search results if it is "inadequate, irrelevant, or no longer relevant." This decision gave rise to the phrase "right to be forgotten" and driven a discussion about how to strike an equilibrium between personal privacy and freedom of speech. In 2019, the European Union court restricted the application of the 'RTBF' ruling to within the European Union, thereby stating that Google is not obligated to implement this right beyond the borders of Europe. The court's decision, which went against the recommendation of the Advocate General, sent shockwaves through the community. Although privacy campaigners welcomed the ruling, it was generally perceived as a blow to freedom of expression. This was due, in part, to the judgment's focus on an individual's "Right to Privacy"and data protection, which appeared to take priority over the rights of search engines and internet users to access and display information in search results. The court further suggested that information should only be made available in the public interest. Since the concept was first introduced in the landmark 2014 ruling by the European Court of Justice, it has influenced similar legislation around the world, including in India, where the country's SCrecognized the RTBF in a 2017 ruling. While the RTBF has developed and evolved in various countries, its origins can be traced back to the EU, where it continues to be a critical component of privacy law.

RTBF IS AN INTRINSIC PART OF RIGHT TO PRIVACY

The Constitution plays a crucial role in a democratic setup as it serves as the foundation and framework of the government and its institutions.[8] Constitution guarantees the protection of fundamental rights such as freedom of speech, religion, and association, and ensures that minorities and marginalized groups have equal representation and protection under the law. Fundamental Rights are the basic rights guaranteed to every citizen in a democratic country.[9] They are enshrined in the Constitution and serve as a shield to protect citizens from any arbitrary action by the state. These rights ensure that individuals have the freedom to express their opinions, practice their religion, and participate in the democratic process without fear of persecution. In many countries, including India and the United States, these rights form the cornerstone of the legal system and are considered essential for upholding justice and ensuring equality for all citizens.

The RTBF is not explicitly mentioned in the Indian Constitution. However, it is based on Article 21 of the Constitution, which guarantees the right to life and personal liberty, and includes the right to privacy.[10] Concept of "Right to Privacy" in India is a completely fascinating improvement that took inside the Indian constitutional jurisprudence is the extended dimension given to Article 21 by way of the judicial precedents in post-maneka generation.[11] Article 21 has emerged as of multidimensional nature having wide ambit and scope. The extension of the dimensions of Article 21 has been made feasible by giving a prolonged scope of the words such

[7] LEC 060 (CJEU 2014)

[8] H.M. Seervai, *Constitutional Law of India* 243 (Law and Justice Publishing Company, India, 4th edn., 2023)
[9] Das Saumendra, "Indian Constitution: An Analysis of the Fundamental Rights and the Directive Principles" 1 *Journal of Applied Research and Social Sciences* 42 (2014)
[10] The Constitution of India,art. 21
[11] Dr. J.P Yadav, Right to Privacy and Data Protection in Digital Era: Issues and Challenges 34 (Notion Press, 1st edn., 2023)

LAW AND SOCIAL POLICY REVIEW
VOLUME 2 AND ISSUE I OF 2024
APIS - 3920-0015 | ISSN - 2583-8180
Published by
Institute of Legal Education
https://iledu.in

as 'life' and 'liberty' defined in Article 21 of the Constitution. These particular terms given under Art. 21 are not to be examined narrowly. The apex court has clearly explained that as a way to treat a right as a Fundamental Right, it is not mandatory that it need to be expressly defined within the constitution as a Fundamental Right. The law enlarges its scope to fulfill the rapidly changing needs of the society. "Right to Privacy" belongs from those categories of right that got recognized after widening of the scope and ambit of Article 21 of The Constitution of India. "Right to Privacy" is not independently defined under any section of the Indian Constitution. But, this type of right has been discovered by the apex court from Article 21 and many other provisions of the Constitution

In the very same landmark judgment of ***Puttaswamy vs. Union of India***[12] (2017), the SCof India held that the "Right to Privacy" is a fundamental right under the Constitution. However, in this judgment one important aspect comes forward and that is RTBF. Justice Kaul, thus, acknowledged that RTBF is derived from Right to Privacy, however, would be weighed against other fundamental rights and larger public interests. The Court held that the RTBF can be exercised only in cases where the information is no longer relevant, accurate, or necessary, or where it causes harm to the individual's reputation or privacy.

LEGAL AND JUDICIAL PERSPECTIVE OF RTBF IN INDIA

In the Indian legal framework there are no laws specifically dedicated to the concept of RTBF. However few of the Judicial pronouncements address the issues and gives insight about the implementation of the Right. The judgment given by the SCand the High court clearly highlights the need for giving due recognition to this right and the problems that arises due to the absence of the proper law addressing the issue.

IT ACT, 2000 is one of the prominent legislation in the world of technology and it underwent several amendments to meet the demand of the time. The recent amendment of 2008 brings with it section 43A which talked about the concept of granting compensatition in the instances of data breach. This section clearly elaborated that if an organization is found responsible for the data breach than it has to provide compensation to the victim whose data has been breached. However it is pertinent to note that this section does not explicitly talks about the concept of RTBF.

Under Section 43A of the Information Technology Act 2000, companies that hold sensitive personal data but if fail to properly secure it, resulting in harm to an individual, may be required to provide compensation.[13] While the 'RTBF' isn't explicitly addressed in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 issued by the Indian government, the rules do establish a procedure for individuals to submit complaints to a designated Grievance Officer in order to have personal information removed from the internet, even without their consent.

On the other hand, Section 69A and Section 79 of the Information Technology Act, 2000, deal with the blocking and removal of certain types of content from the internet. These sections provide the government with the power to direct intermediaries to block access to certain types of content, including content that is considered to be obscene, defamatory, or a threat to national security. However, these provisions do not specifically provide for the RTBF. So while there are provisions in the Indian legal framework that relate to personal data protection and the removal of certain types of content from the internet, there is no specific legislation in India that explicitly recognizes the RTBF.

Digital Personal Data Protection Act, 2023 aims to strike a balance between individual rights

[12] (2017) 10 SCC 1

[13] The Information Technology Act, 2000 (Act 21 of 2000), s.43A

LAW AND SOCIAL POLICY REVIEW
VOLUME 2 AND ISSUE I OF 2024
APIS - 3920-0015 | ISSN - 2583-8180
Published by
Institute of Legal Education
https://iledu.in

and public interest in the processing of digital personal data. Section 13 of the Act grants data principals the right to request correction and erasure of their personal data. It mandates that data fiduciaries respond to such requests by updating, correcting, completing, or erasing the data. However, requests for data erasure can only be honored if the data's original purpose has been fulfilled and it is no longer required for legal purposes. Additionally, under Section 16(4), data principals are obligated to provide verifiable and authentic information.

Section 18(1) of the Act outlines specific exceptions to this right, indicating instances where it will not apply. These exceptions include situations where the data is necessary for judicial or quasi-judicial functions, enforcement of legal rights or claims, prevention, detection, investigation, or prosecution of offences or law violations, and when data processed outside India by a person within India is pursuant to a contract. Furthermore, the Union Government has the authority under the second clause of this section to exempt the Act's application for statistical purposes or to prevent incitement to cognizable offences related to public order, security, sovereignty, integrity, and friendly relations with other states.

Judicial Approach

In the Gujarat High Court case of ***Dharmaraj Bhanushankar Dave v. State of Gujarat***[14], the issue of the RTBF was addressed for the first time in India. The petitioner had filed a case seeking the removal of a published judgment in which they had been acquitted. However, the Court declined to issue an order for the removal of the judgement since the petitioner was unable to identify any specific legal provisions that had been breached. This lack of a legal framework meant that the petitioner was unable to seek any recourse.

In 2017, the SCof India, in the landmark case of ***Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors***[15], recognized the "Right to Privacy" as a fundamental right under the Indian Constitution. The court held that the "Right to Privacy" includes the right to control one's personal information and data. This judgment can be considered a significant step towards the recognition of the RTBF in India.

In the case of Name Redacted v. The Registrar General[16] **(2017),** The RTBF has been upheld by the Karnataka High Court, which acknowledged its alignment with regulations in Western countries. In cases that involve sensitive matters like assault or damage to a person's reputation, the preservation of the RTBF is deemed necessary to protect heir dignity and honor. In the case of X vs. Registrar General,[6] the Karnataka High Court acknowledged the RTBF in cases involving severe crimes against women. The court emphasized that if this right is not recognized in such instances, any perpetrator could easily exploit the victim's privacy in cyberspace without any consequences.

Zulfiqar Ahman Khan v. M/S Quintillion Business Media Pvt. Ltd and others[17], is a case against M/S Quintillion Business Media Pvt. Ltd. and others, seeking the removal of articles published about him on news website The Quint. In response, the Delhi High Court recognized the RTBF as well as the right to privacy, which are essential components of an individual's existence.

The High Court of Delhi, in the recent 2021 case of ***Jorawer Singh Mundy v. Union of India and Ors***[18]., ordered Google to take down the judgment that cleared a man of drug charges. The court ruled that the verdict's online presence could harm the man's employment opportunities, thereby recognizing the RTBF.

The concept of 'RTBF' was acknowledged by the Karnataka High Court in the matter of ***V. versus High Court of Karnataka***[19]. The intent of this legal matter was to safeguard the honour of the petitioner's daughter by expunging her name

[14] SCA No. 1854 of 2015]
[15] (2017) 10 SCC 1
[16] 2017 SCC OnLine Kar 424
[17] 2019 (175) DRJ 660
[18] W.P. (C) 3918/ 2020
[19] 2017 SCC OnLine Kar 424

LAW AND SOCIAL POLICY REVIEW
VOLUME 2 AND ISSUE I OF 2024
APIS - 3920-0015 | ISSN - 2583-8180
Published by
Institute of Legal Education
https://iledu.in

from the cause title, which had a chance to be easily available and inflict damage to her image. The court rendered a decision in favour of the petitioner, mandating the expunction of the name of the petitioner's daughter from the cause title and orders. The court underscored that this verdict is consistent with the customary practise in Western nations, where the 'RTBF' is frequently invoked in sensitive cases pertaining to women, particularly those related to rape or harm to a someone's modesty and reputation.

The Orissa High Court explored the application of the 'RTBF' in the case of ***Subranshu Raot v. State of Odisha***[20], as a potential solution for victims of sexually explicit images or videos that are frequently posted on social media to harass them.

RTBF: PROTECTING INFORMATIONAL PRIVACY

The RTBF plays a crucial role in protecting informational privacy by allowing individuals to request the removal of personal information from public access, particularly from search engines and digital platforms. This right is rooted in the broader right to privacy, which encompasses the ability of individuals to control the dissemination and accessibility of their personal data. In the digital age, where vast amounts of personal information can be easily accessed and shared, the RTBF offers a mechanism to limit the public's ability to access outdated, irrelevant, or harmful data that might otherwise continue to circulate online indefinitely. By enabling individuals to request the delisting or deletion of such information, the RTBF helps to safeguard against potential misuse, discrimination, or harm that could arise from the perpetual availability of personal data. This protection is particularly significant in cases where information, though accurate at the time of publication, no longer reflects the current circumstances or has become disproportionately intrusive. In this way, the RTBF aligns with the principles of informational privacy by reinforcing the notion that individuals should have the right to manage their digital identities and personal histories. It recognizes that the continued availability of certain information may infringe on one's privacy rights, especially when that information is no longer relevant to the public interest or when it disproportionately impacts the individual's reputation, career, or personal life. The RTBF thus acts as a counterbalance to the pervasive nature of the internet, offering a degree of control over personal data in an era where information can be easily and perpetually accessible, thereby contributing to a more nuanced and protective approach to privacy in the digital realm.

CONCLUSION

The RTBF is a complex issue that raises important questions about privacy, freedom of expression, and the appropriate balance between these competing rights. While the RTBF has been recognized in some jurisdictions, its implementation remains contentious and varies from country to country. Nevertheless, the growing importance of data protection and privacy rights means that the RTBF is likely to remain an important topic of debate and discussion in the years to come. It will be crucial to strike a balance between the "Right to Privacy" and the right to free expression while ensuring that the implementation of this right is transparent, fair, and serves the public interest.

Although there is currently no specific law in India that addresses the RTBF, past court rulings indicate a growing recognition of this right. Additionally, the Indian government has introduced the Personal Data Protection Bill, which aims to give individuals greater control over their personal information and aligns with the principles of the EU's General Data Protection Regulation. Although the notion of the RTBF is a progressive one, there must be a system in place to ensure that it is not an absolute right. It is important to note that much of the information in the public domain is part of public records. If all of this information were to be erased, it could disrupt the authenticity of

[20] BLAPL No. 4592 OF 2020

records and the information associated with them. Therefore, the RTBF must be balanced with the right to information and freedom of expression. It is advisable to monitor how this right interacts with other laws and regulations, such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021, which provide a mechanism for individuals to address grievances against information in the public sphere. The current trend suggests that India's legal framework on the RTBF is still evolving, and this could potentially mark a new era in the realm of privacy rights in a highly public world.

REFRENCES

BOOKS

- Shankar Dubey, Technology and Innovation Manangement 134 (PHI Learning Private Limited, 2nd edn., 2019)
- Keith Markham, A Practical Guide to General Data Protection Regulation 45 (Law Brief Publishing, 2nd edn., India, 2018)
- Cristina Casagran, Global Data Protection in Field of Law Enforcement: An EU Perspective 56 (Routledge, 1st edn., 2018)
- Dr. J.P Yadav, Right to Privacy and Data Protection in Digital Era: Issues and Challenges 34 (Notion Press, 1st edn., 2023)
- Dr. Bhupesh, How Indian Data Protection Law Should Look Like 45 (Notion Press, 2nd edn., India, 2020)
- Ravindra Kumar, The Right to Privacy in India: Concept and Evolution 34 (Lightning Source, 2nd edn., 2018)

JOURNALS

- Ashley Nicole Vavra, "RTBF: An Archival Perspective" 81 JSTOR 100- 106 (2019)

WEBSITES

- https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022
- https://www.livelaw.in/columns/digital-data-protection-bill-personal-data-protection-bill-pdp-bill-ministry-of-electronics-and-information-technology-rti-act-216722
- https://www.scconline.com/blog/post/2023/01/21/the-digital-personal-data-protection-bill-2022