



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

RIGHT TO BE FORGOTTEN AS A SUBSET OF RIGHT TO PRIVACY

AUTHORED BY - R.NAGESWARI & S.KALAIVANI¹

ABSTRACT

Evolution is considered as the basic development of humankind. In the ancient era, the storage of information was done through manual channels which later transformed into digital medium. If those data are stored for private usage, there is no conflict of interest or violation on any rights. Concern arose when any confidential matters on any individual were discussed in any public forum without his consent or information. It instantly inflicted his secluded life which is safeguarded as a preliminary right under our Constitution. Right to Privacy protects the solitary mind from arbitrary or unlawful interference of any state or non-state actors into the confidential or intimate matters of any individual. In the digital sphere where confidential information is shared online without proper authorization it is vital to protect the integrity, nobility, autonomy and liberty of any individual for which special enactments to safeguard them need to be implemented. It bolsters upon the concept that whatever is happening inside the four walls should remain inside the walls unless they voluntarily want to converse about the subject matter. Adhering to this principle the concept of “*Right to be Forgotten*” emerged wherein upon the request of any individual his name or any personal information will be removed from the internet or any publicly accessible databases. The principle of need to be Forgotten is a legal concept which aims to provide a balance between privacy and freedom of expression in the digital era and it gained prominence for the first time in European Court of Justice whereby the idiosyncratic particulars of individuals are specifically removed from search engines. This article highlights the basic concept, their complex phenomena, the legal precedents, the key challenges and provides a reasonable solution to protect individual privacy thereby upholding the democratic values in the emerging contemporary world.

¹ Nageswari R, Assistant Professor (VISTAS), PV Vaithiyalingam Rd, Velan Nagar, Krishnapuram, Pallavaram, Chennai, Tamil Nadu 600117
Kalaivani S, Assistant Professor (VISTAS), PV Vaithiyalingam Rd, Velan Nagar, Krishnapuram, Pallavaram, Chennai, Tamil Nadu 600117

KEYWORDS:

Digital Platforms, Data Protection, Right to Privacy, Right to be Forgotten, Confidential Information.

RESEARCH METHODOLOGY:

This is a Doctrinal form of research which is a library-based research or research within four walls. This research is done to check the validity of existing laws in society and in case there are any discrepancies suggestions are made to rectify the same. It includes a secondary source of data and includes a thorough analysis into the governing legal doctrines and principles within Indian Jurisprudence and even Internationally by evaluating cases, laid down precedents and relevant statutory enactments.

INTRODUCTION:

The privacy right encompasses an individual's ability to regulate the collection, use, and disclosure of their personal information. This personal information may include habits, activities, family details, educational background, communications, medical history, and financial records. Often equated with the "*right to be let alone*," as described by *Black's Law Dictionary*, privacy entails a person's freedom from unwarranted publicity or interference in matters unrelated to the public interest.

It includes:

- The right to safeguard the individual sovereignty of a person.
- The right to not let others hamper the property of anyone and protect from unnecessary public exposure or scrutiny.

Privacy is a fundamental liberty inherent to human existence. It extends to bodily integrity, personal independence, and the freedom to express, consent, dissent, move, and think without intrusion. This right serves as a safeguard against government or private actions that threaten individual privacy.²

The "*Right to be Forgotten*" allows the individual to do away with the confidential information pertaining to findings in any social media or on digital platforms for which they are unaware or not given proper assent to publish or distribute. Also referred to as the "*Right to Erasure*,"

² Riddhi Tripathi, "The Right to be Forgotten", available at: [The Right To Be Forgotten](#) (last visited on December 19, 2024).

this concept was first introduced by the European Union in May 2014. In India, there is currently no dedicated legislation recognizing the "*Right to be Forgotten*," though a bill addressing the issue is under parliamentary consideration. In the truancy of sturdy data protection laws that uphold the right to delete irrelevant or defamatory private data from online spaces, the "*Right to be Forgotten*" has garnered significant attention in India.³

CONCEPT AND EVOLUTION OF RIGHT TO PRIVACY:

The privacy of any individual was initially considered an insinuated right in India but eventually evolved into a fundamental right under the Indian Constitution. Increasing violations of this right by the State prompted the judiciary to take an active role in safeguarding it. Over time, Article 21 has been interpreted to include several dimensions, emphasizing the terms "*life*" and "*liberty*." The recognition of the right to privacy has significantly expanded the scope of Article 21.

In *M.P. Sharma v. Satish Chandra*⁴, an eight-judge bench of the Supreme Court addressed whether privacy was a fundamental right while dealing with the State's power to search and seize documents from the Dalmia Group. The Court ruled that the framers of the Constitution did not intend to establish a fundamental right to privacy, citing the absence of language similar to the Fourth Amendment of the U.S. Constitution. The bench rejected the notion of importing the concept of a right to privacy into search and seizure provisions, deeming such an interpretation as a "*strained construction*." This issue resurfaced a decade later in *Kharak Singh v. State of Uttar Pradesh*⁵, was presented before a six-judge bench of the Supreme Court. Once again, the Court dismissed the existence of a fundamental right to privacy. However, it struck down provisions allowing night visits by police, deeming them an infringement of "*personal liberty*." The case involved Kharak Singh, who was accused of dacoity but released due to insufficient evidence. The Uttar Pradesh Police placed him under surveillance based on Chapter XX of the state's Police Regulations, which Singh challenged infringing the rudimentary right of any individual under Articles 19(1)(d) and 21. The Court ruled that night-time domiciliary visits were unconstitutional, but it upheld the rest of the regulations. Importantly, the bench held that privacy was not considered as a basic right under Part III of the Constitution. However, in a dissenting opinion, Justice Subba Rao asserted that

³ Zubair Ahmad, "Right to be Forgotten", available at: [Right to be forgotten](#) (last visited on December 17, 2024)

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

⁵ *Kharak Singh v. State of Uttar Pradesh*, 1963 AIR 1295.

the right to privacy was integral to personal liberty, although it had not yet been explicitly recognized as a fundamental right in the Constitution. After eleven long years, the Supreme Court, in a three-judge bench decision in *Gobind v. State of Madhya Pradesh*⁶ acknowledged the existence of that Privacy is enshrined as a basic right under Part III and Article 21 of our Constitution even though it was not abruptly stated in the Article it can always be inferred upon. This marked the first significant recognition of the right to privacy, which had been debated for years. However, it emphasized that this right is not absolute and may be subject to reasonable restrictions. Such restrictions are to be assessed based on the facts of each case and the compelling state interest test. The Court integrated the right to privacy within the framework of fundamental rights, holding that its violation could be challenged if it contravenes the law. It derived the right to privacy from various fundamental rights, including the right to personal liberty, freedom of movement, and freedom of speech. The Court asserted that reasonable restrictions could be imposed only after laws or actions infringing privacy are subjected to scrutiny under the compelling state interest test.

In *R. Rajagopal v. State of Tamil Nadu*⁷, the scope of the right to privacy was further deliberated. This case is about the privacy rights of an accused prisoner. Justice B.P. Jeevan Reddy interpreted the Constitution alongside case law from the United States and the United Kingdom, concluding that, although not explicitly mentioned as a fundamental right, the right to privacy could be inferred from Article 21 of the Constitution.

Another pivotal case was *People's Union of Civil Liberties v. Union of India*,⁸ which addressed the issue of phone tapping. The Court ruled that tapping an individual's phone line infringes on their right to privacy, except in the most critical circumstances, such as national emergencies. The judgment highlighted that, while the right to privacy is protected as a fundamental right, it primarily acts as a limitation on the State's actions and does not necessarily shield individuals from intrusions by private entities.

The *Justice K.S. Puttaswamy v. Union of India*⁹, was a landmark judgement which significantly changed the entire structure and provided a new paradigm to the principle of

⁶ *Gobind v. State of Madhya Pradesh*, 1975 AIR 1378.

⁷ *R. Rajagopal v. State of Tamil Nadu*, 995 AIR 264.

⁸ *People's Union of Civil Liberties v. Union of India*, AIR 1997 SC 568

⁹ *Puttaswamy v. Union of India*, AIR 2017 SC 4161

Privacy rights. On August 24, 2017, a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right under the Indian Constitution. This case was propagated during the challenge to the Aadhaar scheme, where the Attorney General had argued that the Constitution did not guarantee a fundamental right to privacy. Initially heard by a three-judge bench, the matter was referred to a larger bench and eventually escalated to a nine-judge bench. The Court's decision underscored the importance of liberty, dignity, autonomy, and privacy. It overruled previous judgments in *M.P. Sharma* and *Kharak Singh*¹⁰, affirming that the right to privacy is an integral part of the right to life and personal liberty under Article 21, as well as a component of the guarantees in Part III of the Constitution. The Court emphasized that the right to privacy forms part of the "Golden Trinity" of Article 14 (Right to Equality), Article 19 (Right to Freedom), and Article 21 (Right to Life and Personal Liberty), thereby solidifying its place as a fundamental right.¹¹

EVOLUTION OF RIGHT TO BE FORGOTTEN:

The "*right to erasure*," commonly referred to as the "*right to be forgotten*," is enshrined in Article 17 of the General Data Protection Regulation (GDPR) of 2016. The origins of this right trace back to French law, which recognizes *le droit à l'oubli*, or "*the right of oblivion*." Under this principle, rehabilitated individuals who have served their sentences can object to the publication of information about their convictions and incarceration. This concept evolved into modern data protection laws, eventually being incorporated into the European Union's Data Protection Directive of 1995. Under this directive, individuals could request the removal of certain internet information due to its incomplete or inaccurate nature.

Nearly two decades later, the Court of Justice of the European Union (CJEU) delivered a landmark judgment in *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*¹² in 2014. This case firmly established the "*right to be forgotten*" for EU citizens, asserting that personal privacy outweighs the free flow of data within the EU. The judgment was widely praised and paved the way for the inclusion of this right in the GDPR of 2016. The *Google Spain* case arose when Mario Costeja González sought two forms of relief: first, the deletion or alteration of an article in a Spanish newspaper,

¹⁰ *M.P. Sharma and Kharak Singh*, 963 AIR 1295

¹¹ *Ibid* F. No. 2

¹² *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12

and second, the removal or concealment of links in Google search results that connected to the article. Costeja argued that the case referenced in the article had been resolved years ago, and retaining public access to such outdated information was irrelevant and unjustified. The Spanish Data Protection Agency (AEPD) supported Costeja's claim against Google, ruling that search engine operators process personal data and are therefore subject to data protection laws. When Google contested the decision before the CJEU, the key question was whether search engine operators were obligated to protect personal data by removing links to third-party websites containing outdated or irrelevant personal information. The CJEU affirmed this obligation, ruling that search engine operators must delist links to such information from search results, even if the information remains lawful and accessible on the original websites. The court clarified that the right to erasure stems from the right to privacy. However, it emphasized that this right must be exercised with certain qualifications, particularly when data processing conflicts with the relevant legal directives. The *Google Spain* decision was groundbreaking, as it established the "right to be forgotten" as a vital aspect of privacy rights. The judgment also introduced the right to delist or de-index links while addressing the potential misuse of this right, ensuring safeguards were in place to prevent abuse.¹³

RIGHT TO BE FORGOTTEN UNDER EUROPEAN UNION DIRECTIVE:

The "Right to be Forgotten" as discussed earlier was first recognized by the Court of Justice of the European Union (CJEU) in the landmark *Google Spain v. Agencia Española de Protección de Datos* judgment. This right was acknowledged as an aspect of data subjects' right to privacy, specifically concerning the processing of personal data by internet search engines in response to delisting requests under Articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union (the Charter).

Following this recognition in CJEU case law, the "Right to be Forgotten" was formally codified in Article 17 of the General Data Protection Regulation (GDPR), titled "Right to erasure ('right to be forgotten')." in which subsection (1) allows the individuals the right to request the erasure of their personal data without unnecessary prolongment under certain conditions. These include situations where the data are no longer visibly available for the public as the purposes for which they were collected or processed are no longer viable or in other cases where the consent has

¹³ Nikhil Aswani, "The Right to be Forgotten and its Enforcement in India", available at: [Nikhil-IJLDAI.pdf](#) (Last Visited on December 20, 2024)

been withdrawn or is obtained by unlawful means or methods. The right to be forgotten extends beyond publication by news outlets or search engines and applies to other contexts, such as requests to remove personal information from public registers. Under Article 17(2) of the GDPR, permits the controller to erase personal data which was made public and ensures that while doing so he must take reasonable steps considering available technology and implementation costs and provide a prior intimation to other controllers who are processing the data that the subjected data has been requested to erasure and henceforth there will be no links, copies, or replications of this data.

Additionally, the GDPR outlines criteria for balancing the right to be forgotten with other competing interests, such as freedom of expression and access to information. These obligations were clarified further by the CJEU after the GDPR's enforcement. The Court provided guidance on the interpretation of Article 17 obligations for search engine operators, considering fundamental rights protected by Articles 7 and 8 of the Charter on one side and Article 11 (freedom of expression and information) on the other.¹⁴

BALANCING RIGHT TO BE FORGOTTEN AND ARTICLE 19(1) OF INDIAN CONSTITUTION:

The right to be forgotten has consistently faced significant criticism for potentially curbing the freedom of speech and expression. The core issue lies in balancing two competing rights: an individual's right to enforce their right to be forgotten, an inherent aspect of the right to privacy, and the public's right to freedom of speech and expression, which includes the right to information and the right to know.

A key concern regarding the right to be forgotten is enabling individuals to express themselves freely without fear that their current statements will negatively impact them in the future. The principle behind enforcing this right is arguably more about protecting free speech than restricting it.

Critics argue that the right to be forgotten is inherently restrictive of the freedom of speech and expression guaranteed by constitutions in countries like the United States and India, which

¹⁴ "Right to be Forgotten", ECtHR and CJEU Case Law 2024, *available* *at:* fra.europa.eu/sites/default/files/fra_uploads/fra-2024-factsheet-right-to-be-forgotten_en.pdf (Last Visited on December 20, 2024)

have robust legal frameworks protecting these rights. These criticisms suggest that enforcing the right to be forgotten directly contradicts such freedoms. To address this conflict, a balanced approach is recommended, where the judiciary evaluates each case on its merits to determine which right privacy or free speech holds greater weight in the specific context.

In India, the right to privacy is not explicitly mentioned in the Constitution as a fundamental right under Part III. However, the judiciary has recognized it as an intrinsic part of Article 21 Right to Life and Personal Liberty¹⁵. This recognition began with Justice Subba Rao's groundbreaking dissent in the *Kharak Singh case*¹⁶, which gave a liberal interpretation of Article 21 and laid the groundwork for privacy jurisprudence. This idea expanded significantly with the landmark judgment in *Justice K.S. Puttaswamy (Retd.) case*¹⁷, where the Supreme Court's nine-judge bench comprehensively discussed privacy and extended its scope under Article 21.

Conversely, Article 19(1)(a) of the Constitution explicitly guarantees the freedom of speech and expression, subject to reasonable restrictions outlined in Article 19(2). These restrictions are exhaustive and allow the state to enact laws limiting free speech for specific purposes. In *Shreya Singhal v. Union of India*¹⁸, the Supreme Court held that vague and overly broad restrictions, such as those in Section 66-A of the IT Act, 2000, are unconstitutional. The court ruled that such provisions could have a "chilling effect" on free speech, emphasizing that restrictions must be narrowly defined.¹⁹

When the CJEU recognized the right to be forgotten, free speech advocates criticized the decision, arguing that it amounted to censorship. This issue was further examined in the case of *Olivier G v. Le Soir*²⁰. In this Belgian case, a newspaper was sued for publishing its archives online, which included a report revealing the full name of a truck driver involved in an accident. The driver argued that he had been convicted and subsequently rehabilitated, requesting that the information be removed from the internet. The court ruled in his favor, affirming the right of erasure in instances where a significant passage of time or disproportionate harm justified

¹⁵ The Constitution Of India (As of 1st May, 2024), S. 21

¹⁶ Ibid, F.No. 5

¹⁷ Ibid, F.No. 9

¹⁸ *Shreya Singhal v. Union of India*, AIR 2015 SC 1523

¹⁹ Ibid, F.No.13

²⁰ *Olivier G v. Le Soir*, 29 April 2016, n° C. 15.0052. F

such action. Additionally, General Comment No. 34 of the *United Nations Human Rights Committee (UNHRC)* emphasized that the protections under Article 19 of the *International Covenant on Civil and Political Rights (ICCPR)*, which safeguards freedom of expression, also apply to online platforms.²¹

RIGHT TO BE FORGOTTEN IN INDIA:

India lacks a specific data protection law, leading to reliance on case-by-case judicial intervention. In *Sri Vasunathan v. The Registrar-General*²², the Karnataka High Court acknowledged the relevance of the right to be forgotten in sensitive cases, such as those involving women or incidents that affect personal reputation. The court directed that the petitioner's daughter's name be removed from earlier court orders to protect her reputation and societal standing. Justice Sanjay Kishan Kaul has also expressed support for the right to be forgotten, emphasizing an individual's right to control their personal data and online existence.

However, contrasting views have emerged in *Dharamraj Dave v. State of Gujarat*²³, the Gujarat High Court noted the absence of a legal framework for removing judgments from online platforms like Google or Indian Kanoon, ruling that such actions did not violate Article 21. These cases highlight the need for a comprehensive legal framework to address the right to be forgotten in India.

In the *Justice K.S. Puttaswamy case*,²⁴ the Supreme Court acknowledged the principles of the *European Union's General Data Protection Regulation (GDPR)*, which defines the right to be forgotten. Key considerations included:

- 1. Children's Data:** Recognizing the digital footprints of children and allowing parents or individuals to request the removal of personal information linked to childhood mistakes.
- 2. Personal Growth:** Supporting individuals' ability to move forward without being perpetually tied to past errors, allowing for personal evolution.
- 3. Balancing Rights:** Ensuring that the right to privacy does not entirely erase history, balancing it with freedom of expression and the public's right to information.

²¹ Swati Pandita and Lovely Sharma, Right to be Forgotten: A Study with Special Reference to India, *available at: 4850700.pdf* (Last Visited on December 20, 2024)

²² *Sri Vasunathan v. The Registrar-General*, W.P. No. 62038/2016

²³ *Dharamraj Dave v. State of Gujarat*, SCA No. 1854 of 2015

²⁴ Id, F.No. 9

The right to be forgotten implies that individuals can request the removal of data that is no longer relevant, necessary, or accurate. However, it does not extend to erasing information essential for public interest, scientific research, public health, or legal claims. While this right supports privacy and individual autonomy, it must be carefully balanced to avoid excessive profiling or unjust censorship of past events.²⁵

SIGNIFICANCE OF PERSONAL DATA PROTECTION BILL 2023:

Personal data refers to any information that pertains to an identified or identifiable individual. Both businesses and government entities process personal data to facilitate the delivery of goods and services. Such processing enables the understanding of individual preferences, which can be leveraged for purposes like customization, targeted advertising, and creating recommendations. Additionally, personal data processing can assist law enforcement efforts. However, unchecked processing poses risks to individuals' privacy as a fundamental right potentially leading to harms such as financial loss, reputational damage, and profiling.

At present, India does not have a dedicated data protection law. The use of personal data is primarily governed by the Information Technology (IT) Act, 2000. In 2017, the central government established a Committee of Experts on Data Protection, chaired by Justice B. N. Srikrishna, to address data protection issues in India. The Committee presented its report in July 2018.

Based on the Committee's recommendations, the Personal Data Protection Bill, 2019, was introduced in the Lok Sabha in December 2019. The Bill was subsequently referred to a Joint Parliamentary Committee, which submitted its report in December 2021. However, the Bill was withdrawn from Parliament in August 2022. A Draft Bill was then released for public consultation in November 2022. Finally, in August 2023, the Digital Personal Data Protection Bill, 2023, was introduced in Parliament²⁶ which eventually became an Act on August 11, 2023. This Act was implemented to regulate the processing of digital personal data, ensuring a balance between individuals' rights to safeguard their personal data and the necessity of

²⁵ Prashanth Mali, Privacy Laws: Right to be Forgotten in India, *available at*: [Volume-VII-17-33.pdf](#) (Last Visited on December 20, 2024)

²⁶ "The Digital Personal Data Protection Bill, 2023", *available at*: [Legislative Brief : The Digital Personal Data Protection Bill, 2023](#) (Last visited on December 20, 2024)

processing such data for legitimate purposes, along with related or incidental matters.²⁷

SUGGESTIONS:

- A Comprehensive legislative framework for data protection in India should explicitly be included for the *Right to Be Forgotten (RTBF)* to ensure internet invisibility for providing robust data privacy for Web users.
- The specific law can be implemented by making amendments to the already existing laws by keeping in view the fundamental rights of the Constitution thereby ensuring a detailed conditions to erase the date when it has become outdated, irrelevant or cause any harm to the individual reputation of the person.
- Implement an effective judicial and administrative to system address the requests promptly without causing any undue delay for appeals.
- Create Public Awareness by launching campaigns to educate citizens about adherence to data protection norms and highlighting the importance of safeguarding their personal information.
- The organization should conduct Data Minimization Practices by collecting the data for predefined periods and delete the obsolete and redundant data in regular intervals.
- Personal Software Apps should be pre installed in every mobile or any electronic device at low or no cost to remove date easily.

Practices like use of anonymous and pseudonymous names, signs or symbols can be used to protect their personal data while enabling legitimate users.

- Adequate protection needs to be focused on Vulnerable Groups like children, women, old age and persons with mental disabilities by ensuring erasure of their digital footprints linked to their accounts or their past mistakes.
- Incorporation of the laws should be always in consideration of International standards for consistency and easy compliance.
- Implement strict accountability mechanisms to ensure organizational compliance and Impose penalties for non-compliance or misuse of personal data and Conduct regular evaluations to identify challenges and refine policies.

²⁷ “The Digital Data Personal Data Protection Act (No.22 of 2023)”, available at: [Digital Personal Data Protection Act 2023.pdf](#) (Last visited on December 20, 2024)

CONCLUSION:

The **Right to Be Forgotten (RTBF)** is an essential and evolving component of the broader **Right to Privacy**, designed to address the distinct challenges posed by the digital age. It grants individuals the ability to reclaim control over their personal data, ensuring that obsolete, irrelevant, or harmful information does not indefinitely compromise their dignity and autonomy. Grounded in the principles of self-determination and human dignity, RTBF expands traditional privacy protections into the digital sphere, tackling the rapid proliferation of online data and its potential for exploitation.

However, implementing RTBF raises significant questions about balancing individual rights with the public's right to information and freedom of expression. Despite these complexities, RTBF highlights the necessity of adapting privacy laws to contemporary realities. In a world where digital footprints can have enduring and widespread consequences, RTBF offers a progressive framework for protecting individual privacy. By integrating RTBF into broader privacy regulations, legal systems can foster a fairer and more respectful digital landscape, ensuring privacy remains a cornerstone of human rights in the modern era.

