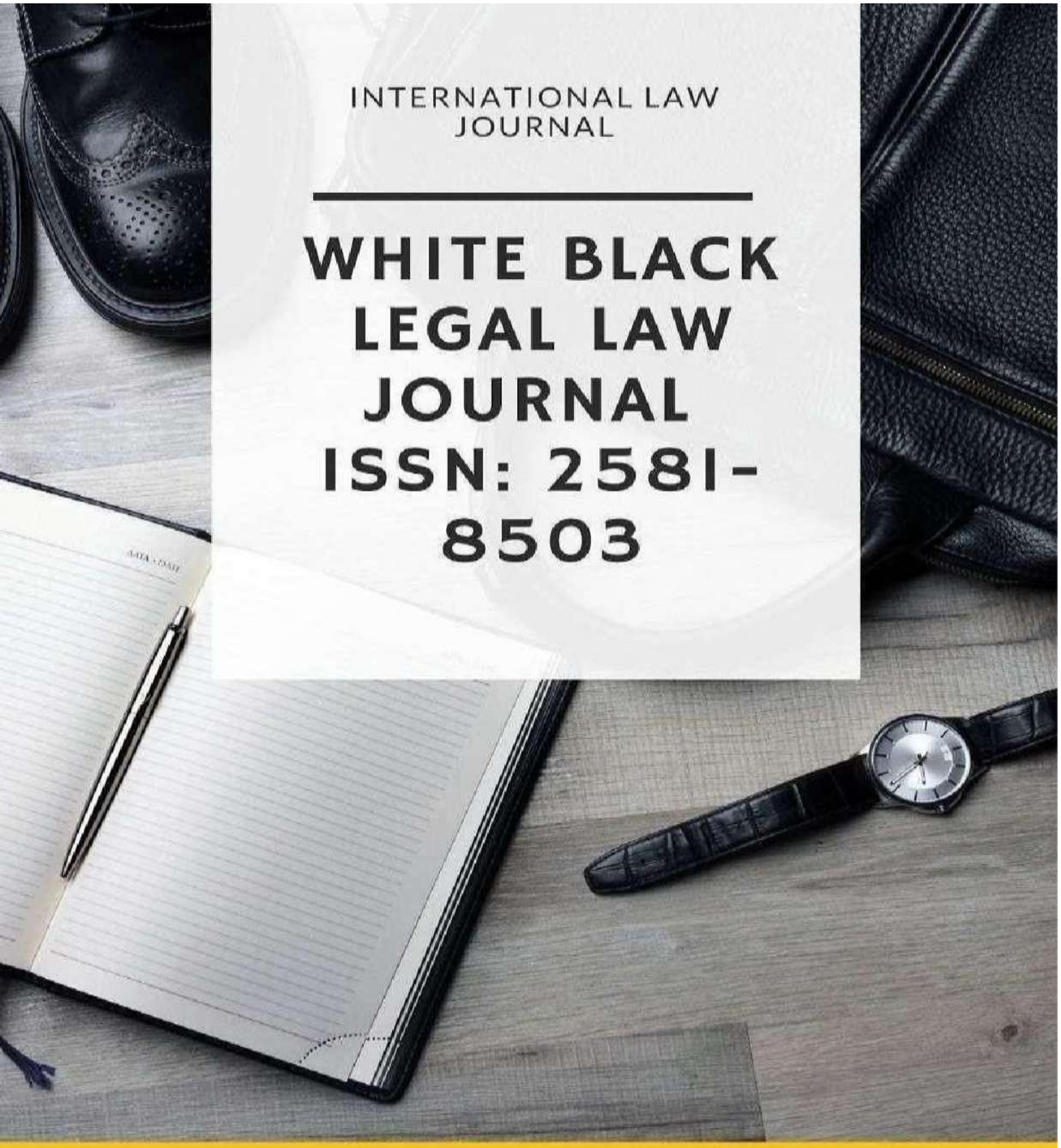

INTERNATIONAL LAW JOURNAL

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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

CONSTITUTIONAL CROSSFIRE: GDPR'S 'RIGHT TO BE FORGOTTEN' MEETS FIRST AMENDMENT & INDIAN LAW

AUTHORED BY - AKANSHI TANEJA
L.L.M (Constitutional And Administrative Law)
O.P. Jindal Global University, Sonipat

Introduction

The inherent conflict between the fundamental right to freedom of speech and expression and the right to privacy, especially the "Right to Be Forgotten" (RTBF), has been significantly exacerbated by the digital age. The unprecedented scope and permanence of personal data collection, processing, and storage made possible by technological advancements is the cause of this escalation. People in today's technological world leave a "long-lasting digital footprint," which implies that past errors, unrelated information, or even legally processed data may sit online indefinitely and potentially damage a person's reputation, dignity, and prospects for the future.[1]

The RTBF, which is predominantly codified in the General Data Protection Regulation (GDPR) of the European Union, emerged as a crucial legal concept in response to these obstacles. In a bid to give people greater autonomy over their online presence, it permits them the right to request that personal data be deleted from online platforms when it is no longer vital, or processed legally.

However, the public's right to information and freedom of speech are directly at loggerheads with this right. Critics dread censorship or the "total erasure of history" as a result of the RTBF's potential abuse to suppress lawful public records. In the global digital landscape, striking a balance between these conflicting interests—individual autonomy and the public's right to know remains a difficult and continuous task.

[1] **Geraldine Mbah**, *Data Privacy and the Right to be Forgotten*, 16 World J. Advanced Res. & Rev. 1079 (2022), https://doi.org/10.30574/wjarr.2022.16.2.1079.

Global divergence comparing the polar opposites of US vs EU

EU (GDPR)

Article 17 of the General Data Protection Regulation[2] (GDPR), which was introduced in 2018 and is often considered as the gold standard for privacy laws, explicitly sets forth the RTBF, a fundamental legal concept. When private information is no longer essential, relevant, or processed legally, people can request that it be removed from online platforms under the RTBF. This right, which has its roots in ideas like the French "le droit à l'oubli" (right of oblivion), has historically permitted ex-offenders to protest the disclosure of their prior convictions.

Google Spain SL v. Agencia Española de Protección de Datos[3] was a landmark case that established that search engines must remove links to personal information that is no longer relevant or up-to-date upon a valid request. This proved that search engines handle RTBF requests in their capacity as data controllers. The ruling affirmed that in the digital age, corporations are increasingly responsible for upholding human rights and that fundamental rights, such as the right to be forgotten, take precedence over commercial interests.[4]

GDPR emphasizes data minimization and storage limitations, requires stringent consent for data collection and usage, and imposes severe penalties for non-compliance, up to €20 million or 4% of annual global turnover. By establishing a stronger individual right to erasure, the EU approach essentially views privacy as superseding the free flow of data "as a rule." This framework has had a major impact on data protection laws around the world.

US (First Amendment) approaches.

The US does not have a federal law that expressly grants the Right to Be Forgotten, unlike the EU. Privacy claims are frequently superseded by the First Amendment, which protects freedom of the press and of speech. Upholding the protection of truthful information, even if it is embarrassing or connected to criminal history, as long as it was obtained lawfully, US courts have historically been hesitant to impose regulations on search engines that would limit their discretion.

---

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) 1, 33–36.

[3] Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ECLI:EU:C:2014:317 (May 13, 2014)

[4] Yulia Razmetaeva, *The Right to Be Forgotten in the European Perspective*, 10 TalTech J. Eur. Stud. 30 (2020), https://doi.org/10.1515/bjes-2020-0004.

This position stems from America's strong marketplace of ideas approach to free speech and emphasis on negative liberties, or freedom from governmental coercion. The European RTBF "represents the biggest threat to free speech on the Internet," according to critics.

Even though residents of some states, such as California, have the right to request the deletion of their data under the California Consumer Privacy Act (CCPA)[5], the CCPA does not apply to search engines or publicly accessible records, underscoring the scope difference with the GDPR.

Legal experts are still debating how to implement a US version of RTBF without violating free speech rights because the US believes that giving private companies the authority to decide what information should be deleted sets a problematic precedent.

Right to Erasure vs. Right to Know: India's Evolving Legal Battlefield

India's path to embracing and balancing the Right to Be Forgotten is a result of a combination of external factors and particular domestic difficulties. Although the nation has made great progress in recognizing privacy as a fundamental right, the conflict between free speech and privacy remains a constant challenge to its developing legal system.

The Development of India's Right to Privacy Early Indian constitutional rulings, like M.P. Sharma v. Satish Chandra[6] (1954) and Kharak Singh v. State of Uttar Pradesh[7](1964), gave the concept of privacy little recognition at first because it was not stated clearly as a fundamental right. With the groundbreaking Justice K.S. Puttaswamy v. Union of India[8] (2017) ruling, which categorically affirmed privacy as an essential component of the Right to Life and Personal Liberty [9] of the Indian Constitution, this drastically changed. This decision implicitly laid the foundation for the RTBF as an extension of privacy by establishing the constitutional framework for personal autonomy and data protection. The Court acknowledged that information on the internet is permanent and that people should be able to manage their online

[5] Cal. Civ. Code §§ 1798.100–1798.199 (West 2020) (as amended by the California Privacy Rights Act (CPRA), 2020).
[6] Sharma v. Satish Chandra, (1954) SCR 1077 (India).
[7] Kharak Singh v. State of U.P., AIR 1963 SC 1295 (India).
[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[9] India Const. art. 21.

presence.

India has gradually tackled privacy issues in the digital era through its legislative efforts: ◦ The Information Technology Act, 2000[10], was the nation's inaugural significant cybersecurity and privacy law, but it has been criticized for being out of date and insufficient for contemporary issues.[11] The "right to forgotten" was specifically mentioned in the Personal Data Protection Bill, 2019 under Clause 20[12], which defines it as the data principal's right to limit or forbid the ongoing release of personal data. The GDPR served as the inspiration for this bill, which sought to create a Data Protection Authority (DPA) and require user consent.

A major milestone was reached with the Digital Personal Data Protection Act, 2023[13] (DPDP Act), which developed from the bills in 2019 and 2022. It received approval in August 2023 with the goal of establishing greater accountability for organizations that handle data both domestically and internationally, with a focus on the rights to privacy, accountability, and transparency. The terms "data fiduciary" (an organization in charge of processing data), "data processor," and "data principal" (the people whose data is processed) are defined in the Act. It specifies rules for cross-border data transfers, requires express consent for data processing, and enforces severe sanctions for noncompliance. These laws were greatly influenced by the BN Srikrishna Committee[14], which was established in 2017 and recommended a framework for data protection that included the idea of RTBF and saw the relationship between customers and service providers as fiduciary. Constitutional Tensions and Judicial Interpretations, the implementation of RTBF in India is still developing despite legislative advancements, and it frequently faces conflict between the rights to freedom of speech and expression i.e. Article 19(1) (a)[15] and privacy i.e. Article 21. To balance these conflicting interests, Indian courts have taken a case-by-case approach:

Cases Giving Credit for RTBF:

The Delhi High Court recognized the RTBF as an integral component of the right to privacy and the right to be left alone under Article 21 in Zulfiqar Ahman Khan v. M/S Quintillion

[10] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[11] Dr. Tanveer Kaur, *Right to Privacy in Digital Age: A Study with Indian Context*, 14 Eur. Econ. Letters 4 (2024), http://eelet.org.uk.
[12] Personal Data Protection Bill, cl. 20, Bill No. 373 of 2019 (India).
[13] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
[14] Dr. Arti Aasha, *Right to Be Forgotten in India - A Critical Analysis*, 52 Indus. Eng'g J. No. 1, at 4 (2023)
[15] *Constitution of India*, art. 19 (1) (a)

Business Media Pvt. Ltd[16]., directing the removal of critical articles about the petitioner from a news website.

In Subhranshu Rout v. State of Odisha[17] (2020), the Orissa High Court recognized the need to safeguard the petitioner's privacy and future well-being by providing relief to a petitioner whose expunged criminal record was available online and impairing his rehabilitation. In order to preserve privacy and dignity, the Delhi High Court permitted a person to ask for their name to be removed from a public judgment in X v. Union of India[18] (2021). In Vishal v. The Registrar General[19] (2022), the Karnataka High Court recognized the significance of RTBF for out-of-date or irrelevant information that could damage a person's reputation.

The court held that the right to be forgotten applies in delicate cases involving women in Sri Vasunathan v. The Registrar General &Ors[20], ordering the removal of a petitioner's daughter's name from a cause title due to reputational harm.

Cases Rejecting/Limiting RTBF:

In Dharamraj Bhanushankar Dave v. State of Gujarat[21], the Gujarat High Court declined to recognize the RTBF, ruling that there was no legal basis to stop the publication of an acquitted criminal's judgment and that doing so did not violate Article 21.

Although it acknowledged exceptions for victims of rape and other sexual offenses where identities must be protected, the Madras High Court more recently held in Karthick Theodre v. Registrar General[22] that the "right to be forgotten cannot exist in the sphere of administration of justice, particularly in the context of judgments delivered by Courts." This demonstrates that the RTBF typically does not protect court decisions.

The RTBF in India is frequently subject to restrictions and is not always absolute. According to the Puttaswamy ruling, the PDP Bill, and most likely the DPDP Act, RTBF cannot be used

[16] Zulfiqar Ahman Khan v. Quintillion Bus. Media Private. Ltd., 2023 SCC On Line Del 800 (India).
[17] Subhranshu Rout v. State of Odisha, 2020 SCC OnLine Ori 878 (India).
[18] X v. Union of India, 2021 SCC OnLine Mad 2096 (India).
[19] Vishal v. Registrar Gen., 2022 SCC OnLine Del 3304 (India).
[20] Sri Vasunathan v. Registrar Gen., 2017 SCC OnLine Mad 10082 (India).
[21] Dharamraj Bhanushankar Dave v. State of Gujarat, 2017 SCC OnLine Guj 1002 (India).
[22] Karthick Theodre v. Registrar Gen., 2021 SCC OnLine Mad 2096 (India).

if the data is needed for:

- The exercise of fundamental rights under Article 19
- The performance of legal obligations and responsibilities.
- The execution of responsibilities pertaining to public health and interest; ◦ Information protection for public use;
- For historical, statistical, or scientific reasons.
- The formulation, implementation, or defence of legal claims.

The absence of a strong digital infrastructure for data removal, the question of jurisdiction over platforms with foreign headquarters, and a lack of public knowledge regarding digital privacy rights are additional obstacles to the implementation of RTBF in India. The possibility that RTBF could be abused for censorship or to censor important information, like criminal records or investigative journalism, thereby undermining accountability and transparency is another ongoing ethical worry. While India recognizes both privacy and free speech as fundamental rights, its legal framework struggles to balance them, requiring a tailored approach.

The Right to Freedom of Speech and Expression, which is protected by Article 19(1)(a)[23] of the Indian Constitution, frequently clashes with the RTBF's goal of protecting individual privacy. Access to information is a component of freedom of expression and is necessary for an open and knowledgeable society. There may be conflict between the public's right to know and an individual's privacy, dignity, and reputation when certain personal information is made freely available. For instance, even if it is required for the person's rehabilitation or dignity, requests to delete information about their prior criminal history or public behaviour may violate the principles of transparency.

The Puttaswamy ruling itself stated that the right to privacy is not unqualified and is subject to a number of limitations, such as the exercise of fundamental rights under Article 19, the satisfaction of legal obligations, the public interest, public health, scientific or historical research, statistical purposes, or the creation, performance, or defence of legal claims. Indian courts resolve this conflict by taking a case-by-case approach, balancing the right to privacy of the individual with the public interest in information access. Determining whether information removal is warranted and whether it unnecessarily restricts free speech in a

[23] India Const. art. 19, cl. (1)(a).

democratic society depends heavily on judicial scrutiny

Determining "public interest," defining "outdated" data, and resolving conflicts with RTI and freedom of speech laws are some of the difficulties in putting RTBF into practice. Additionally, there is worry that RTBF might be abused to stifle important information, like critical viewpoints or investigative journalism, undermining democratic principles.

Freedom of expression encompasses the public's right to access information, which is essential for an open and knowledgeable society, but RTBF seeks to protect individual privacy by permitting the removal of personal data from online platforms. This creates an inherent conflict[24]. In the 2017 case of Justice K.S. Puttaswamy v. Union of India[25], the Supreme Court of India established the constitutional foundation for the Right to Privacy by recognizing it as a fundamental right under Article 21. Nevertheless, there are limitations on this right, such as the ability to exercise fundamental rights under Article 19, the public interest, and legal accountability.

There is a serious concern that RTBF might be abused to cover up corruption or previous crimes. The critics contend that implementing requests for data removal goes against fundamental rights like information access and freedom of speech.[26]

Search engines and news organizations have voiced worries that RTBF might be used to censor valid public records, which could lead to a "memory hole" effect that modifies historical accuracy. Investigative reports and news archives are frequently used as vital sources by journalistic organizations; eliminating them could jeopardize accountability and transparency. There is a chance that the RTBF will be used as a weapon to stifle critical viewpoints or investigative journalism, which would undermine democratic principles like the right to information and freedom of speech. The judiciary is essential in examining RTBF requests to make sure they don't hinder proper reporting, especially when it comes to journalistic content. The Supreme Court invalidated Section 66A of the Information Technology Act[27] in Shreya

[24] Aakansha Bhardwaj, *Right to Be Forgotten in India: Balancing Privacy and Public Interest*, 7 Indian J.L. & Legal Res.
[25] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[26] ibid
[27] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, S. 66A (India)

Singhal v. Union of India[28] , highlighting the value of free speech in the digital era and establishing a precedent for shielding it from capricious limitations.

Another major issue is the conflict between a person's right to privacy and the public's right to know. Indian courts usually take a case-by-case approach, balancing the right to privacy of the individual with the public interest in information access[29]. To ensure accountability and transparency in public life, public figures and politicians are frequently subject to a higher threshold for data removal requests. Transparency principles may be violated by requests to delete information about a person's prior public behaviour. Conflict arises for the RTBF when people, including criminals, want their records expunged from the public domain. In the past, convicted criminals who had completed their sentences and received rehabilitation were able to protest the publication of their conviction facts and incarceration under the French legal doctrine known as the "right of oblivion" (le droit à l'oubli)[30].

However, the First Amendment in the United States protects the publication of a person's criminal history. The Gujarat High Court first rejected the RTBF in Dharamraj Bhanushankar Dave v. State of Gujarat[31]. After being exonerated of criminal charges, the petitioner attempted to stop a non-reportable judgment from being published online, claiming it would endanger his personal and professional life. However, since no legal justification was offered to stop it, the High Court determined that the publication did not violate Article 21. "Ordering the removal of a judgment is an extreme step that goes against the universal right to information," Chief Justice D.Y. Chandrachud has added. [32]

On the other hand, in certain situations, Indian courts have recognized the RTBF. In Subhranshu Rout v. State of Odisha (2020), the Orissa High Court ruled that data should be deleted from the internet, providing relief to a petitioner whose expunged criminal record was visible online and influencing his chances of rehabilitation.

In State of Punjab Vs. Gurmeet Singh and Ors[33], the Supreme Court stated that anonymity

[28] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[29] Tanveer Kaur, *Right to Privacy in Digital Age: A Study with Indian Context*, 14 Eur. Econ. L. (2024)
[30] Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88 (2012
[31] Dharamraj Bhanushankar Dave v. State of Gujarat, 2017 SCC OnLine Guj 2493 (India).
[32] Arti Aasha & Debaditya Das, *Right to Be Forgotten in India—A Critical Analysis*, 52 Indus. Eng. J. No. 1, 2023.
[33] State of Punjab Vs. Gurmeet Singh and Ors

could reduce the likelihood of social exclusion for victims of sexual assault, suggesting that RTBF would be beneficial for these victims as well as other people who might have unintentionally committed crimes. The severity of the offense, the amount of time since conviction, and the public interest in reducing recidivism are some of the variables that are taken into account when evaluating RTBF requests pertaining to criminal records.

With notable exceptions for victims of sexual offenses whose identities are protected, the Madras High Court held in Karthick Theodre v. Registrar General[34] that the right to be forgotten cannot exist in the administration of justice, especially with regard to court judgments. This suggests a legal differentiation between confidential data and public court records. The Puttaswamy ruling itself stated that the public interest and the creation, prosecution, or defense of legal claims are two examples of limitations on the right to privacy. Determining "outdated" data, resolving conflicts with RTI and freedom of speech laws, and objectively assessing "public interest" are all necessary for the implementation of RTBF. Additionally, there is worry that RTBF might be abused to stifle important information, like critical viewpoints or investigative journalism, undermining democratic principles.

Case Studies & Contemporary Relevance in India

In the context of non-consensual intimate imagery (NCII), the Subhranshu Rout case[35] offers a convincing judicial engagement with the right to be forgotten (RTBF), while carefully navigating Article 19(1)(a) concerns about free speech. While not explicitly stating an absolute right, the Odisha High Court impliedly acknowledged RTBF as a remedy for gender-based privacy harms when it ordered the removal of revenge porn from online platforms, highlighting the need for proportionality in content takedowns. This ruling exemplifies the larger conflict between the public's desire for digital transparency and individual privacy (Article 21), especially when it comes to cases involving sexual violence and dignity. Subhranshu Rout takes on greater significance in the current digital environment, where deepfakes and NCII are common, showing how courts can give victim protection top priority without completely censoring content. But since India's DPDP Act, 2023 avoids explicit RTBF recognition, the lack of a structured RTBF doctrine raises unanswered concerns regarding long-term content moderation and platform liability. As a result, the decision represents a jurisprudential turning

[34] ibid
[35] Subhranshu Rout v. State of Odisha, WP (C) No. 11118 of 2020, (Odisha H.C. 2020) (India).

point that strikes a balance between the dangers of excessive speech restrictions in an age of algorithmic amplification and gender justice.

In India's developing jurisprudence on the "right to be forgotten" (RTBF) and its conflict with freedom of speech and expression (Article 19(1)(a)), the Jorawar Singh Mundy v. UOI[36] (2023) case marks a turning point. While recognizing RTBF as a component of the right to privacy (Article 21), the Delhi High Court rejected an absolute right to erasure, stating that the right to information (Article 19(1)(a) & 19(2)), free speech, and the public interest must all be balanced. The case highlights the moral and legal conundrum that arises in the digital age when people try to disassociate themselves from inaccurate or biased information while the public, media, and researchers insist that historical records and transparency are essential. This ruling establishes a precedent for future cases involving reputation, privacy, and open justice and emphasizes India's cautious approach in an era of permanent digital footprints, departing from the GDPR's more stringent RTBF framework. As data privacy laws (DPDP Act, 2023) take shape and courts must balance the delicate balance between individual dignity and democratic discourse, the ruling is still especially pertinent today.

Ritesh Sinha v. State of Uttar Pradesh[37] (2019) 8 SCC 1 serves as an example of how the Indian judiciary's changing position on privacy rights deviates significantly from the GDPR's strict protections when state interests are involved. The Supreme Court subordinated individual privacy claims under Article 21 to the state's investigative powers in this landmark decision, approving the mandatory collection of voice samples under Section 311A of the CrPC[38]. The majority's logic, which placed a higher priority on the effectiveness of criminal justice than biometric privacy, is in direct opposition to the GDPR's categorical limitations on the processing of biometric data (Article 9)[39], and it further muddies India's still-developing RTBF jurisprudence. Notably, Justice Nariman's dissent highlighted the ongoing conflict between civil liberties and state power in India's constitutional framework by outlining an unyielding view of privacy that was more in line with Puttaswamy's core beliefs. Legislatively, this

[36] Jorawar Singh Mundy v. Union of India, W.P.(C) 3918/2021, 2023 SCC OnLine Del 1786 (Del. H.C. 2023) (India).
[37] Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1 (India).
[38] Code of Criminal Procedure, 1973, No. 2, Acts of Parliament, 1974, s. 311A (India).
[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 9, 2016 O.J. (L 119) 1, 35–37.

jurisprudential dissonance is expressed in Section 17(2)(a) of the DPDP Act[40], which codifies the deference to executive authority held by the Ritesh Sinha majority by carved out extensive exemptions for state surveillance. Thus, the case exemplifies India's contextual balancing approach, which favors state interests in contested domains while avoiding absolutism regarding free speech (as defined by the U.S. First Amendment) and privacy maximalism (as defined by the EU).

Claims of Censorship vs. Government Takedown Requests (IT Rules 2021): In India, social media sites like Facebook, Twitter, and WhatsApp are essential to contemporary communication and have come under fire for their data privacy policies. End-to-end encryption, which protects user privacy, and government requests for data access in criminal and national security investigations are at odds. Regulations like the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which were introduced by the Indian government, mandate that platforms track the source of specific messages. Opponents contend that this action compromises user privacy and encryption. Platforms must maintain user trust while striking a balance between privacy, transparency, and national legal requirements.

There is absolutely no denial to the misuse of data and widespread surveillance in India. The possible abuse of surveillance technologies is demonstrated by incidents such as the Pegasus spyware controversy, in which it was claimed that politicians, journalists, and activists were being monitored by spyware, which took advantage of security flaws to obtain private information without authorization. Critics contend that constitutional protections like the right to privacy are compromised by the lack of openness and judicial supervision in the use of such instruments. A stark example of data misuse is the Cambridge Analytica scandal[41], in which millions of Facebook users' personal information was obtained without their consent for political profiling, sparking worries about election meddling and public opinion manipulation. These instances highlight the continuous discussion about whether government actions amount to censorship and suppression or are legitimate attempts to counter false information.

Tech Giants & Compliance Challenges: The operational dilemma faced by Google, Meta, and

[40] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023, s. 17(2)(a) (India)
[41] Julia Angwin & Hannes Grassegger, *Facebook's Privacy Struggles*, N.Y. Times (Mar. 28, 2018), https://www.nytimes.com/2018/03/28/technology/facebook-privacy-scandal.html.

other intermediaries in India epitomizes the jurisprudential clash between the right to be forgotten (RTBF) and freedom of expression (Article 19(1)(a)). While Indian courts have incrementally recognized RTBF in cases like Jorawar Singh Mundy (2023) and Subhranshu Rout (2020), tech platforms remain caught between competing imperatives: complying with local takedown orders, adhering to global free speech norms (e.g., the First Amendment in the U.S.), and mitigating reputational risks. The absence of a statutory RTBF framework under India's DPDP Act, 2023 exacerbates this uncertainty, forcing platforms to adopt ad hoc moderation policies that lack transparency. The discretionary nature of these takedowns is highlighted by recent conflicts, such as courts ordering the delisting of criminal records Dharamraj Bhanushankar Dave v. State of Gujarat[42] while rejecting pleas from public figures in Zulfiqar Ahman Khan v. Quintillion Business Media[43]. This patchwork approach poses important questions in an era of algorithmic governance: Can platforms fairly strike a balance between democratic discourse and privacy harms? Should contextual judicial reasoning be superseded by automated compliance? Clearer guidelines on the RTBF's application, exclusions, and procedural protections are desperately needed as India's digital economy expands, lest privatized content moderation skew constitutional rights.

RTBF is one of the high standards for data protection set by the General Data Protection Regulation (GDPR) of the European Union. According to the 2014 Google Spain case[44], search engines are data controllers and are required to eliminate links to out-of-date or unnecessary personal data from search results in the EU under specific guidelines.

Google processed millions of RTBF requests as a result of this decision. However, Google first rejected a French data protection organization's (CNIL) order to implement these delisting requests across all of its global domains, arguing that "the Internet would only be as free as the world's least free place" if it were granted. Later, Google changed its stance to block access to deleted URLs using geolocation.

The difficulties of implementing RTBF in various jurisdictions were then highlighted when the

[42] ibid
[43] ibid
[44] Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, EU:C:2014:317 (Court of Justice of the European Union 2014).

Court of Justice of the EU decided in Google v. CNIL[45] (2019) that RTBF does not have global applicability, meaning Google was only required to remove search results within the EU. Tech companies are in a difficult position because of this: they have to deal with the GDPR's stringent compliance requirements in Europe, India's constitutional recognition of privacy, and the USA's protections for free speech.

On August 11, 2023, India passed the Digital Personal Data Protection Act, 2023 [46](DPDP Act), which aims to increase accountability for companies doing business in India, such as internet providers, mobile applications, and companies that collect, store, and process data. Additionally, it has an extraterritorial scope, which includes digital personal data processing activities conducted overseas that are related to profiling Indian citizens or providing goods or services to individuals in India. This law will further complicate the global operations and data handling policies of tech giants by imposing new compliance requirements.

Right to Be Forgotten: Should India Mirror the EU, Embrace US Free Speech Absolutism, or Forge a Third Way?"

1. Reasons in Favor of GDPR-Style Protections- The General Data Protection Regulation (GDPR) of the European Union, which went into effect in 2018, is regarded by many as the benchmark for privacy regulations. It created the Right to Be Forgotten (RTBF) as a fundamental clause in Article 17, giving people the ability to ask for the removal of personal information if it is no longer required for its intended use, if consent is revoked, or if data processing is illegal.

   In a data-driven economy, robust privacy protections are essential: Concerns regarding privacy have increased dramatically in India's developing digital economy as a result of data breaches, digital surveillance, and technology breakthroughs. Privacy was upheld as an essential component of the Right to Life and Personal Liberty (Article 21) in the historic Justice K.S. Puttaswamy v. Union of India (2017) ruling. There are serious risks associated with the commodification and proliferation of personal data by social media platforms, e-commerce websites, businesses, and governments. These risks include the potential for misuse for political, targeted, or financial gain without sufficient safeguards or user consent. The risks of unrestricted data collection and the

[45] Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), Case C-507/17, EU:C:2019:772 (Court of Justice of the European Union 2019).
[46] ibid

potential for privacy violations to affect democratic processes and individual dignity are brought to light by incidents such as the Pegasus spyware controversy and the Cambridge Analytica scandal[47]. A strong framework for protecting personal data and resolving these issues would be provided by implementing GDPR-style protections. On August 11, 2023, India's recently passed Digital Personal Data Protection Act, 2023 (DPDP Act) went into effect. Its goal is to increase accountability for organizations that handle data in India. It also has an extraterritorial scope, meaning that data processing abroad that involves Indian citizens is covered. Principles like user consent and sanctions for data breaches are shared by the DPDP Act and GDPR.

Prevents outdated or irrelevant information from damaging a person's reputation- With every picture, status update, and tweet having the potential to live forever in the cloud, the internet's persistent memory makes it extremely difficult to escape one's past. As demonstrated by the Mario Costeja González case[48], which gave rise to the idea of RTBF in Europe, this can seriously harm a person's reputation. Information that is out of date or unrelated can seriously damage someone's reputation, cause embarrassment, or undermine their chances of rehabilitation or self-respect. The RTBF gives people the legal right to manage their online history and make sure their online persona appropriately represents who they are today. In order to preserve privacy and dignity, the Delhi High Court in X v. Union of India[49] (2021) and the Orissa High Court in Subhranshu Rout v. State of Odisha[50](2020) have recognized RTBF as an essential component of the right to privacy, providing relief for the removal of expunged criminal records or names from public judgments.

2. Reasons in Favor of US-style Free Speech Priority Unlike the EU, the US does not have a federal law that grants RTBF. Rather, privacy claims are frequently subordinated to the First Amendment, which protects freedom of the press and of speech. US courts have generally decided that people's right to have their data deleted is subordinated to the public interest in having access to accurate information.

   Essential for public accountability, investigative journalism, and democracy: A broad RTBF is opposed on the grounds that it poses a serious risk to online free speech.

[47] ibid
[48] ibid
[49] ibid
[50] ibid

Freedom of information could be compromised by unrestricted RTBF enforcement, especially when it comes to historical events, public figures, or court documents. For instance, the US Supreme Court ruled that, as long as the information was obtained lawfully, states cannot prevent the media from sharing embarrassing but true information. Public accountability may be compromised if public figures try to delete contentious past remarks or court documents. Notably, the Madras High Court decided that the "right to be forgotten" cannot be applied to the administration of justice because it violates the universal right to information, particularly with regard to court orders.

Risk of overreach by the government (such as censorship under IT Rules): In India, there is a lot of worry about the conflict between preserving user privacy and government requests for data access in criminal and national security cases. Critics claim that the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, require platforms to track the origin of specific messages, jeopardizing user privacy and encryption. The Pegasus spyware controversy highlights issues about mass surveillance and the erosion of constitutional protections like the right to privacy because of a lack of transparency and judicial oversight. It also serves as an example of how surveillance technologies can be abused to monitor journalists, activists, and political figures. Without, clear legislative or judicial oversight, granting broad data removal powers could allow the government to overreach or even be abused to stifle legitimate information and dissent. An excessively broad RTBF is feared to have a "serious chilling effect" on free speech by turning tech giants into "censor-in-chief" or causing deletion in unclear situations because of the possibility of crippling financial penalties.

3. A cautious but vital balancing act between privacy (Article 21) and free speech (Article 19(1)(a)) is reflected in India's developing jurisprudence on the right to be forgotten (RTBF). India's approach, which has emerged through cases like Subhranshu Rout[51] (2020) and Jorawar Singh Mundy[52] (2023), suggests a contextual, limited RTBF in contrast to the U.S.'s free speech absolutism or the EU's GDPR, which enshrines RTBF as a statutory right. As demonstrated in Dharamraj Bhanushankar Dave [53](2017), where courts denied RTBF for serious acquitted crimes but permitted it for expunged records

[51] ibid
[52] ibid
[53] ibid

that aid in reintegration, this model may limit the right to non-public figures and non-criminal records with exceptions for rehabilitation. Despite lacking specific RTBF provisions, the Digital Personal Data Protection Act (DPDPA), 2023, allows for judicial and regulatory discretion, guaranteeing that privacy claims are balanced against historical accountability, public interest, and democratic discourse.

To keep RTBF from turning into a censorship tool, a strong public interest test that is administered by courts or a Data Protection Authority[54] (DPA) is essential. Similar to the GDPR's exceptions, but with more robust protections for transparency, the Supreme Court upheld in K.S. Puttaswamy[55] (2019) that RTBF must give way to free speech, legal requirements, and journalistic purposes. To prevent arbitrary removals, for example, platforms might be required to reveal anonymized takedown requests, as suggested in U.S. legislative drafts. This balance could be further institutionalized by the DPDPA's proposed DPA, which would guarantee that RTBF requests are decided independently, especially in delicate cases involving victims of sexual assault, State of Punjab v. Gurmeet Singh[56] or deepfake harms, where privacy is more important than public scrutiny.

In the current digital environment, where permanent online records and AI-exacerbated reputational harm collide, proportionality must be given top priority in India's middle path. A customized RTBF framework can preserve dignity without limiting transparency; it is neither as rigid as the EU's nor as contemptuous as America's. The success of the DPDPA depends on precise rules that define "public interest" exceptions, protect historical and journalistic content, and provide appeal procedures for platform overreach. This strategy could establish a standard for democracies in the Global South facing comparable conflicts by taking inspiration from international models while putting India's constitutional values front at the heart of it.

Conclusion

A classic constitutional conundrum of the digital age is the interaction between India's right to be forgotten (RTBF) and freedom of speech and expression (Article 19(1)(a)). Although RTBF, as an extension of the right to privacy (Article 21), aims to shield people from ongoing stigmatization online, its unchecked use could jeopardize democratic discourse, historical

[54] ibid
[55] ibid
[56] ibid

transparency, and public accountability. India's emergent, context-sensitive approach is exemplified by judicial precedents such as Jorawar Singh Mundy (2023) and Subhranshu Rout (2020), which rejects the absolutism of RTBF while cautiously acknowledging it for non-public figures and rehabilitative cases. But because the DPDP Act of 2023 lacks a statutory RTBF framework, there are significant gaps that force courts and intermediaries to negotiate this area on their own, frequently at the expense of legal certainty.

India's path must strike a balance between two conflicting imperatives in the age of algorithmic permanence and AI-driven reputational harm: protecting privacy without permitting censorship and preserving free speech without devaluing human dignity. These conflicts might be resolved by a proportionality-based approach that is based on strict public interest testing and judicial supervision. To do this, the scope of RTBF must be made clear (for example, by excluding topics of public record or journalistic value), takedowns must be transparent, and the Data Protection Authority (DPA) must be given the authority to resolve disputes. There is no one-size-fits-all solution, as international discussions—from the EU's GDPR to the US First Amendment—highlight. India's challenge is to find a middle ground that respects rights, complies with its constitutional values, and takes into account the particularities of its digital ecosystem. The stakes are high: if we strike this balance incorrectly, we run the risk of either unchecked reputational damage or privatized censorship; if we strike it correctly, India may set a precedent for other Global South democracies facing comparable conflicts. Clarity in legislation and the judiciary is urgently needed.