Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2021 = 7.380, www.srjis.com
PEER REVIEWED & REFEREED JOURNAL, SEPT-OCT, 2021, VOL- 9/67

THE RIGHT TO BE FORGOTTEN IN INDIA: CONSTITUTIONAL FOUNDATIONS AND COMPARATIVE PERSPECTIVES

Lairenjam Dhanamanjuri Devi
B.R.M. Government Law College, Guwahati, Assam, 781037 E-mail: manjuazadi@gmail.com

Paper Received On: 21 OCT 2021
Peer Reviewed On: 31 OCT 2021
Published On: 1 NOV 2021

Abstract

The Right to Be Forgotten (RTBF) is an emergent aspect of digital privacy law that seeks to restore individual control over personal data in an era marked by the permanence of online information. In India, RTBF has been acknowledged by various High Courts as a derivative of the fundamental right to privacy recognized by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017. Although the decision laid a constitutional foundation for informational privacy, the absence of a dedicated statutory framework has led to inconsistent judicial interpretations and a lack of enforceable norms. This paper explores the judicial evolution of RTBF in India, critically assessing case law that balances individual privacy against competing interests such as freedom of expression and the public's right to know. The analysis is further enriched through comparative jurisprudence from the European Union, United Kingdom, and United States—jurisdictions that adopt varied approaches to the RTBF, shaped by their respective constitutional values and regulatory frameworks. The study highlights the significance of proportionality, necessity, and contextual sensitivity in adjudicating RTBF claims. It concludes by emphasizing the urgent need for a comprehensive data protection law in India that codifies RTBF within a rights-based and democratically accountable framework.

Keywords*: Right to Be Forgotten, privacy, Indian Constitution, Article 21, data protection, GDPR, proportionality, comparative law, judicial review, digital identity*

Introduction

The digital age has profoundly transformed the way information is stored, accessed, and disseminated, reshaping communication, commerce, governance, and social interaction on a global scale (Castells, 2010). The proliferation of internet-based platforms and digital technologies has brought immense benefits in terms of connectivity and knowledge-sharing. However, it has also significantly challenged conventional understandings of individual privacy and autonomy (Solove, 2004). Unlike physical records or ephemeral verbal interactions, digital information—whether accurate, outdated, or misleading—can persist indefinitely, often without the consent of the data subject (Cavoukian, 2012). This enduring

accessibility raises pressing concerns about personal dignity, reputational harm, and the ability to escape one's digital past, particularly in cases where the information no longer serves a legitimate purpose or was shared without proper authorization (Warren & Brandeis, 1890).

Amid these challenges, the Right to Be Forgotten (RTBF) has emerged as a globally debated legal and normative concept designed to recalibrate the balance of power between individuals and data controllers, such as search engines, social networks, and digital archives (Mantelero, 2013). The RTBF enables individuals to request the removal or de-indexing of personal information from online platforms when its continued availability causes undue harm or no longer aligns with public interest, thereby reasserting a measure of control over one's digital footprint (Kloza & Van der Sloot, 2015). This right is increasingly seen as central to protecting individual privacy in a digital environment where past information can significantly influence future opportunities.

The legal recognition and implementation of the RTBF vary across jurisdictions but are typically situated within constitutional or human rights traditions that prioritize data protection and personal autonomy (Fenwick et al., 2017). In India, a watershed moment in the legal understanding of privacy—and by extension the RTBF—was the Supreme Court's landmark ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017, which affirmed that privacy is a fundamental right under Article 21 of the Constitution. This judgment extended the scope of privacy to include informational autonomy—the right to control how personal data is collected, stored, and shared in the digital domain (Baxi, 2018). It laid a constitutional foundation for emerging data protection norms and opened the door to future legal recognition of rights like the RTBF (Garg & Mukherjee, 2019).

India's recognition of informational privacy parallels global shifts toward acknowledging data autonomy and digital dignity as integral to human rights (Kumar, 2020). These developments underscore the necessity for robust legal tools that empower individuals to manage their personal information online, minimize harm from enduring digital traces, and balance privacy rights with freedom of expression and the public's right to know (Narayanan & Shmatikov, 2008). Yet, India's statutory framework for data protection remains underdeveloped. The proposed Personal Data Protection Bill, introduced in 2019, has yet to be enacted and lacks explicit provisions for the RTBF (Das, 2020). This regulatory vacuum presents significant hurdles for courts, policymakers, and data subjects seeking effective redress in the face of pervasive data persistence.

In this context, the present article examines the conceptual origins and legal development of the RTBF, tracing its evolution as a response to the privacy risks posed by digital permanence. It explores the RTBF within India's legal framework, assesses international experiences, and engages with doctrinal and practical considerations. Ultimately, it advocates for a carefully balanced RTBF regime—one that protects individual dignity and privacy while preserving essential democratic values such as freedom of information and accountability.

Conceptual Foundations of the Right to Be Forgotten

The conceptual underpinnings of the Right to Be Forgotten (RTBF) are rooted in the broader principle of informational self-determination, a concept asserting that individuals must have control over the collection, processing, and erasure of their personal data (Westin, 1967). This principle evolved in response to the increasing complexity of personal autonomy in the digital age, wherein vast quantities of data are collected and circulated across digital networks often without sustained consent or awareness from the data subject (Kuner, 2017). Informational self-determination seeks to correct the structural power imbalance between data subjects and powerful digital intermediaries—such as search engines and social media platforms—that act as de facto gatekeepers of personal data (Schwartz & Solove, 2011).

The RTBF emerged as a legal response to the challenge of digital permanence, where outdated or irrelevant personal information remains indefinitely accessible online, potentially impairing an individual's privacy, dignity, and reputation (Giubilini, 2017). The enduring visibility of such data can entrap individuals in outdated narratives of their lives, hindering their ability to evolve and redefine their identities. The RTBF thus represents a critical mechanism to mitigate such harms by enabling individuals to request the removal or de-indexing of online content that no longer serves a legitimate public interest.

A pivotal moment in the modern legal articulation of the RTBF occurred in the Court of Justice of the European Union (CJEU) decision in *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, 2014. The court ruled that individuals have the right to request search engines to delist personal information from search results when it is "inadequate, irrelevant or no longer relevant" (CJEU, 2014, para. 94). Importantly, this judgment extended legal accountability from original content creators to digital intermediaries—particularly search engines—that amplify access to such information (Kemp, 2018). The court acknowledged that even factually

accurate data may warrant removal if its continued online presence unduly infringes on personal privacy without serving a compelling public interest (Giubilini, 2017).

The ruling was based on Directive 95/46/EC, the European Union's Data Protection Directive, which established the principle that personal data processing must respect fundamental rights, including the right to privacy and freedom of expression (European Commission, 1995). In balancing these rights, the CJEU emphasized that personal dignity and control over one's digital footprint are not absolute but must be weighed against legitimate public interest and freedom of information (CJEU, 2014).

Building on this jurisprudence, Article 17 of the General Data Protection Regulation (GDPR) 2016 codified the RTBF within EU law. It grants individuals the right to request the erasure of personal data under specific conditions—such as when the data is no longer necessary, the individual withdraws consent, or the data was processed unlawfully (European Parliament & Council, 2016). However, the GDPR also outlines exceptions that prevent misuse of this right, including where data retention is necessary for exercising freedom of expression, fulfilling legal obligations, or preserving public health and historical records.

This calibrated structure reflects the qualified nature of the RTBF: it is not an absolute entitlement but one that must be weighed against broader societal values (Cate, 2010). Critics have cautioned that without safeguards, the RTBF could lead to forms of censorship or erasure of public history, raising concerns about transparency and free access to information (Bygrave, 2014). These concerns are especially relevant in democratic societies where public figures, institutions, and records must be open to scrutiny.

From a broader normative standpoint, the RTBF signals a shift in data protection philosophy—from a model centered on restricting misuse of data to one that empowers individuals to actively manage their digital identities and reputations (Solove, 2007). It acknowledges that in an era defined by perpetual data circulation, autonomy over personal data is essential for preserving individual dignity and meaningful participation in public life (Kuner, 2017).

The operationalization of the RTBF entails legal, technical, and ethical challenges. Legally, it demands robust criteria for evaluating takedown requests and ensuring judicial oversight to prevent abuse (Kemp, 2018). Technologically, it requires consistent compliance across diverse platforms and jurisdictions, often involving intricate coordination mechanisms (Binns, 2018). Ethically, it raises difficult questions about the appropriate limits of personal privacy vis-à-vis public memory, accountability, and free expression (Giubilini, 2017).

Judicial Recognition of the Right to Be Forgotten in India

In India, the Right to Be Forgotten (RTBF) has largely evolved through judicial interpretation rather than formal legislative enactment. Unlike the European Union, where the RTBF has been codified under Article 17 of the General Data Protection Regulation (GDPR), Indian courts have played a key role in defining the contours of this right, particularly in the absence of a comprehensive data protection statute (Choudhary, 2018; Garg & Mukherjee, 2019).

Dharamraj Bhanushankar Dave v. State of Gujarat (2015)

One of the earliest Indian cases to confront issues related to RTBF was *Dharamraj Bhanushankar Dave v. State of Gujarat*, 2015. The petitioner, who had been acquitted of criminal charges, sought the removal of his name from online legal databases, citing concerns over reputational harm. The Gujarat High Court rejected the plea, emphasizing that judicial pronouncements are public records essential for maintaining transparency and legal accountability (Choudhary, 2018). This judgment underscored the inherent tension between the permanence of legal documentation in the public domain and an individual's interest in social reintegration.

Sri Vasunathan v. The Registrar General, High Court of Karnataka (2017)

In this significant decision, the Karnataka High Court acknowledged RTBF within the broader framework of the constitutional right to privacy. The petitioner had requested the redaction of his daughter's name from a court order publicly available online, expressing concern about possible harm to her personal relationships and reputation. Recognizing the risk of lasting digital stigma, the Court directed that her name be anonymized in online search results, thus reinforcing global privacy norms related to informational autonomy and individual dignity (Garg & Mukherjee, 2019).

S. v. State of Kerala (2017)

The Kerala High Court, in *S. v. State of Kerala*, 2017, recognized the RTBF as part of the constitutionally guaranteed right to privacy under Article 21. The petitioner requested the erasure of his name and personal information from digital platforms, fearing potential harm to his identity and personal life. The Court issued an interim order directing online platforms to delist the petitioner's name, illustrating a growing judicial sensitivity toward protecting personal data from unwarranted digital persistence (Kumar, 2020).

Subhranshu Rout v. State of Odisha, 2020

The *Subhranshu Rout* case represents a continuation of evolving judicial attitudes toward RTBF. The Orissa High Court addressed the non-consensual circulation of intimate images on social media, recognizing RTBF as a necessary remedy for protecting victims' dignity and privacy in the digital era. The Court noted the urgent need for statutory recognition of RTBF to address the growing challenges posed by online harms (Kumar, 2020).

Judicial Trends and Emerging Norms

These cases collectively reflect a nascent but growing judicial recognition of RTBF within Indian legal discourse. Courts are increasingly confronted with the consequences of digital permanence, particularly in matters where outdated or sensitive information remains indefinitely accessible online. While the decisions vary across jurisdictions and factual contexts, they increasingly rely on the proportionality test articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which mandates that any limitation on privacy rights must pursue a legitimate aim, be necessary, and constitute the least restrictive means (Supreme Court of India, 2017; Fenwick, 2017). However, in the absence of statutory codification or consistent standards, the enforcement of RTBF in India remains highly discretionary and context-dependent.

Legislative Framework and Gaps

Although Indian courts have begun to engage with the Right to Be Forgotten (RTBF), the absence of a clear statutory framework has led to inconsistent recognition and application. The right currently exists in a legal grey area—rooted in constitutional jurisprudence following the *Justice K.S. Puttaswamy (Retd.) v. Union of India* decision, 2017, yet lacking full legislative support. This legal lacuna has made the enforcement of RTBF fragmented and heavily reliant on judicial discretion (Kumar, 2020; Choudhary, 2018).

The Personal Data Protection Bill, 2019

The most prominent legislative attempt to codify RTBF in India came through the Personal Data Protection Bill, 2019 (PDP Bill), drafted by the Justice B.N. Srikrishna Committee and introduced in Parliament in response to the Supreme Court's privacy ruling in *Puttaswamy* (Bhandari et al., 2017). The PDP Bill sought to establish a comprehensive data protection regime, recognizing RTBF under Clause 20 as the "right to restrict or prevent continuing disclosure of personal data" (PRS Legislative Research, 2019).

This clause allowed data principals (individuals) to approach data fiduciaries (data processors) and request the restriction of their personal data under specific circumstances—

such as when the data had served its purpose, consent was withdrawn, or the data had become excessive or irrelevant (PRS Legislative Research, 2019). The proposed Data Protection Authority (DPA) was tasked with adjudicating these requests by weighing public interest, the sensitivity of the information, and the individual's role in public life (Mehta, 2020).

Despite its intent, the Bill received criticism. It conferred substantial discretionary power to the DPA, raising concerns about bureaucratic delays (Garg & Mukherjee, 2019). Moreover, it failed to clarify whether RTBF could apply to judicial records, media archives, or public databases. Additionally, the Bill did not obligate search engines to delist content, limiting its effectiveness in addressing digital erasure (Choudhary, 2018).

The Information Technology Act, 2000 and Its Limitations

The Information Technology Act, 2000 (IT Act), remains India's primary legislation governing digital content and intermediary liability. Section 79 of the Act offers "safe harbour" protections to intermediaries—such as social media platforms and search engines—provided they act with due diligence and comply with takedown requests issued by the government or courts (Government of India, 2000).

However, the IT Act does not explicitly recognize RTBF. Consequently, individuals seeking the erasure of digital content must rely on indirect legal routes, such as defamation, data misuse, or privacy infringement. These remedies are often inadequate for addressing the harms of digital permanence, particularly when personal data remains accessible long after its relevance has lapsed (LawBhoomi, 2019; Choudhary, 2018).

Fragmentation and Judicial Overdependence

In the absence of legislative clarity, Indian courts have shouldered the burden of shaping RTBF jurisprudence, resulting in inconsistent and fragmented outcomes across jurisdictions (Kumar, 2020). Individuals face uncertainty due to the lack of uniform criteria for adjudicating RTBF claims, and intermediaries have limited statutory accountability.

Though some courts have begun applying the proportionality framework from *Puttaswamy*—which requires a legitimate aim, necessity, and minimal intrusion into privacy—this remains underdeveloped and inconsistently applied (Bhandari et al., 2017; Fenwick, 2017). Procedural ambiguity persists, and judicial overdependence in regulating RTBF highlights the pressing need for comprehensive legislation that can provide procedural safeguards and standardized norms (Garg & Mukherjee, 2019).

Balancing Competing Interests

The Right to Be Forgotten (RTBF), rooted in the right to privacy and informational self-determination, often intersects with other constitutionally protected values such as freedom of speech and expression, the public's right to know, and the principle of open justice. These intersecting interests necessitate a calibrated and context-sensitive application of the RTBF, rather than its absolute enforcement. Legal scholars have emphasized that privacy rights must be balanced against democratic imperatives, especially where access to truthful information and judicial transparency are involved (Fenwick, 2017; Gellman, 2015). This balancing act is central to shaping the scope and legitimacy of digital privacy claims in evolving jurisprudence.

Privacy and the Right to Reputation

The recognition of privacy as a fundamental right under Article 21 of the Indian Constitution was solidified by the Supreme Court in its landmark decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017, which broadened the conception of privacy to include not only bodily and spatial integrity but also informational privacy—defined as an individual's right to control the dissemination and use of personal data. In a digital environment where personal data may persist indefinitely, the continued availability of outdated or no longer relevant information—such as data relating to legal acquittals or resolved allegations—can result in reputational harm. This harm may manifest in the form of restricted employment prospects, social exclusion, or psychological distress (Fenwick, 2017). In this context, the RTBF functions as a mechanism of restorative justice, empowering individuals to reclaim autonomy over their digital identity and personal narrative.

Freedom of Expression and Public Access to Information

While the right to privacy is firmly entrenched under Article 21 of the Indian Constitution, it must be harmonized with the equally fundamental right to freedom of speech and expression under Article 19(1)(a). An indiscriminate application of the RTBF may result in excessive censorship, the erasure of historical records, and a chilling effect on public discourse. The paradoxical "Streisand Effect" illustrates how attempts to suppress information may inadvertently amplify its public exposure (Solove, 2013).

A vibrant democracy depends on the public's access to information, particularly where the subject matter involves criminal justice, public officials, or corporate accountability. In such cases, the societal value of disclosure may outweigh individual privacy claims (Westin,

2003). As Westin argued, a balance must be struck between the individual's informational autonomy and society's interest in transparency and accountability.

European jurisprudence has recognized this delicate balance. In the landmark decision of *Google Spain SL v. Agencia Española de Protección de Datos*, 2014, the Court of Justice of the European Union (CJEU) emphasized that RTBF claims must be weighed against the public's right to know, considering the individual's role in public life and the continuing relevance of the data (CJEU, 2014). Furthermore, Article 17(3) of the General Data Protection Regulation (GDPR) enumerates exceptions to the RTBF, such as for journalistic purposes, legal compliance, public health, and research, ensuring that the right is not abused to obscure legitimate public interest matters (European Union, 2016).

Transparency and Judicial Records

Judicial transparency is a cornerstone of India's democratic and constitutional framework. Court judgments serve several critical functions: they uphold judicial accountability, foster public trust, and contribute to the development of legal doctrine (Baxi, 2018). Traditionally, access to such records was limited to physical archives or legal publications, but digitization and search engine indexing have made them instantly accessible, raising new challenges for privacy in the public domain.

This transformation necessitates a reconsideration of how court data is disseminated. The ease of online access, particularly without contextual framing, can result in reputational harm long after the resolution of a case. Indian High Courts have responded with limited measures such as redacting names or de-indexing content in sensitive cases, especially those involving acquittals or accusations in sexual offence matters. These actions reflect an attempt to balance the public's right to information with the individual's right to dignity and privacy.

However, courts have resisted establishing a general right to erase judicial records. Their approach remains rooted in the principle of proportionality as developed in *Modern Dental College v. State of Madhya Pradesh*, 2016 and reaffirmed in *Justice K.S. Puttaswamy (Retd.) v. Union of India,* 2017. This doctrine requires that any limitation on competing rights—such as expression or access to justice—must be necessary, proportional, and the least restrictive means of achieving the desired objective.

The RTBF is situated at the intersection of privacy and public interest. Its application must be tempered by constitutional principles that emphasize proportionality, necessity, and minimal intrusion. A one-size-fits-all approach to erasure would risk undermining democratic

values. Instead, courts and legislators must adopt a contextual approach—one that respects the dynamic interplay between individual dignity and collective transparency.

Comparative Jurisprudence on the Right to Be Forgotten

The Right to Be Forgotten (RTBF) has been interpreted and applied differently across jurisdictions, reflecting varying legal traditions and constitutional values. A comparative analysis of the European Union (EU), the United Kingdom (UK), and the United States (US) provides insights into these diverse approaches.

European Union: A Codified Privacy Right

The EU has established a robust framework for data protection, recognizing the RTBF as a fundamental right. In the landmark case of *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, the Court of Justice of the European Union (CJEU) held that individuals could request the removal of personal data from search engine results when the information is "inadequate, irrelevant or no longer relevant" (CJEU, 2014). This decision emphasized the need to balance the individual's right to privacy against the public's interest in accessing information.

Building on this, Article 17 of the General Data Protection Regulation (GDPR) codified the "right to erasure," allowing individuals to have their personal data deleted under specific circumstances, such as when the data is no longer necessary for its original purpose or when consent is withdrawn (European Union, 2016). However, Article 17(3) provides exceptions, ensuring that the RTBF does not override freedom of expression, legal obligations, or public interest considerations.

In *GC and Others v. CNIL*, the CJEU clarified that the RTBF does not have extraterritorial effect, limiting its enforcement to EU jurisdictions and highlighting the balance between privacy rights and the global flow of information (CJEU, 2019).

United Kingdom: Contextual Balancing Post-Brexit

Post-Brexit, the UK retained many GDPR provisions through the Data Protection Act 2018, including aspects of the RTBF. British courts have adopted a nuanced approach, emphasizing proportionality and context. In *NT1 & NT2 v. Google LLC*, the High Court considered delisting requests from two individuals with past criminal convictions. The court granted the request for NT2, recognizing his rehabilitation and the outdated nature of the information, while denying NT1's request due to ongoing public interest and lack of remorse (UK High Court, 2018). This case illustrates the UK's emphasis on balancing individual

privacy with freedom of expression and the public's right to know (Global Freedom of Expression).

United States: Emphasis on Freedom of Speech

In contrast, the US does not recognize the RTBF as a legal right, primarily due to the strong protections afforded to freedom of speech under the First Amendment. US courts have generally prioritized public access to information, making it challenging to mandate the deletion of truthful, lawfully obtained data (Solove, 2011).

While the California Consumer Privacy Act (CCPA) of 2018 introduced rights for consumers to request the deletion of personal information collected by businesses, these provisions are limited and do not establish a comprehensive RTBF. The CCPA focuses on consumer rights and business obligations rather than a broader right to personal data erasure (California Legislature, 2018).

This comparative analysis reveals distinct models: the EU's codified and enforceable RTBF, the UK's contextual and proportional application, and the US's emphasis on freedom of expression. India, in developing its approach to digital privacy, can draw valuable lessons from these jurisdictions to balance individual rights with democratic values (California DOJ Attorney General).

Conclusion

The Right to Be Forgotten (RTBF) in India represents a dynamic convergence of privacy, digital rights, and constitutional interpretation. It finds normative support in the Supreme Court’s recognition of informational privacy as intrinsic to the fundamental right to life and personal liberty under Article 21 of the Constitution in *Justice K.S. Puttaswamy v. Union of India*, 2017. This landmark judgment expanded the understanding of privacy to encompass the control individuals have over their personal information in digital spaces, laying the foundation for emergent rights like the RTBF (Supreme Court of India, 2017).

Despite these developments, the application of the RTBF in India remains fragmented and inconsistent. Courts have relied heavily on a case-by-case proportionality framework to resolve conflicts between privacy rights and countervailing principles such as freedom of expression and the public's right to know (Bhandari, Kak, Parsheera, & Rahman, 2017). This judicial discretion, while pragmatic, lacks the predictability and coherence of a codified statutory regime, resulting in uneven legal protection and uncertainty for petitioners.

The introduction of the Personal Data Protection Bill, 2019, was a significant legislative effort toward establishing a comprehensive data protection regime in India. The bill proposed

explicit RTBF provisions, such as the right to restrict or prevent continued disclosure of personal data where the purpose had been served or the data was no longer necessary (Mehta, 2020). However, its non-enactment stalled institutional progress and left individuals dependent on judicial remedies rather than enforceable statutory rights.

Comparative jurisprudence reveals differing models of RTBF enforcement. The European Union's General Data Protection Regulation (GDPR) provides a structured and enforceable right to erasure, with procedural safeguards, oversight mechanisms, and delineated exceptions to protect competing public interests (Voigt & Von dem Bussche, 2017). The United Kingdom, while following EU law pre-Brexit, has adopted a case-sensitive approach in line with its common law tradition, balancing reputational rights against the public interest (UK High Court, 2018). In contrast, the United States has largely rejected the RTBF, citing strong First Amendment protections and the societal value of unrestricted public discourse (Rosen, 2012).

India's legal and constitutional context necessitates a hybrid approach—one that honors informational privacy and digital dignity while safeguarding journalistic freedom and judicial transparency. A rights-based statutory framework with clearly defined criteria for RTBF enforcement and exceptions is essential for legal clarity and public accountability. In the absence of such legislation, Indian courts must continue to refine the doctrine in a manner that is technologically informed, constitutionally grounded, and responsive to the evolving nature of digital harm.

References

Baxi, U. (2018a). The future of human rights (3rd ed.). Oxford University Press.

Baxi, U. (2018b). Transparency and accountability of judicial function in India: A comprehensive analysis. Legal Service India. Retrieved from https://www.legalserviceindia.com/legal/article-17257-transparency-and-accountability-of-judicial-function-in-india-a-comprehensive-analysis.html

Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). An analysis of Puttaswamy: The Supreme Court's privacy verdict. IndraStra Global. https://www.ssoar.info/ssoar/bitstream/handle/document/54766

Binns, R. (2018). Data protection impact assessments: A meta-regulatory approach. International Data Privacy Law, 8(1), 52–66. https://doi.org/10.1093/idpl/ipx024

Bygrave, L. A. (2014). The right to be forgotten – Between expectations and practice. In S. Gutwirth, R. Leenes, P. De Hert, & Y. Poullet (Eds.), Reinventing data protection? (pp. 145–158). Springer. https://doi.org/10.1007/978-94-007-5170-5_6

California Legislature. (2018). California Consumer Privacy Act of 2018. California DOJ Attorney General. Retrieved from https://oag.ca.gov/privacy/ccpa

Castells, M. (2010). The rise of the network society (2nd ed.). Wiley-Blackwell.

Cate, F. H. (2010). The cost of blocking data: A look at the European right to be forgotten. Journal of Internet Law, 14(5), 3–7.

Cavoukian, A. (2012). Privacy by design: Origins, meaning, and prospects for assuring privacy and trust in the information era. In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), European data protection: Coming of age (pp. 119–142). Springer. https://doi.org/10.1007/978-94-007-5170-5_6

Choudhary, A. (2018). Right to be forgotten in India: A legal analysis. Journal of Indian Law and Society, 9(1), 45–60.

Court of Justice of the European Union. (2014). Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12. Retrieved from https://harvardlawreview.org/print/vol-128/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/

Das, S. (2020). The gaps in India's Personal Data Protection Bill: RTBF and data localisation. Economic & Political Weekly, 55(8), 17–19.

Dharamraj Bhanushankar Dave v. State of Gujarat, 2015 SCC OnLine Guj 2019.

European Commission. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281.

European Parliament & Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union L119.

Fenwick, H. (2017). Data protection and the right to be forgotten in the digital age. International Journal of Law and Information Technology, 25(3), 203–229.

Garg, A., & Mukherjee, S. (2019). The right to be forgotten: A constitutional perspective. Indian Journal of Constitutional Law, 13(2), 112–130.

Gellman, R. (2015). Three bad ideas in the US consumer privacy bill of rights. Open Journal of Political Science, 5(2), 61–68.

Giubilini, A. (2017). Digital forgetting and the ethics of deletion. Ethics and Information Technology, 19(2), 123–132. https://doi.org/10.1007/s10676-017-9429-z

Government of India. (2000). The Information Technology Act, 2000. Ministry of Law and Justice. https://www.indiacode.nic.in

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

Kemp, K. W. (2018). The balancing act: Reconciling the right to be forgotten with the right to freedom of expression in the European Union. Fordham Intellectual Property, Media & Entertainment Law Journal, 28(3), 1043–1082.

Kloza, D., & Van der Sloot, B. (2015). Privacy principles in the age of big data: An academic overview. In B. Van der Sloot, D. Broeders, & E. Schrijvers (Eds.), Exploring the boundaries of big data (pp. 199–226). Amsterdam University Press.

Kumar, R. (2020). Balancing privacy and public interest: The right to be forgotten in Indian jurisprudence. National Law Review, 15(3), 78–95.

Kuner, C. (2017). Transborder data flows and data privacy law. Oxford University Press.

LawBhoomi. (2019). A critical analysis of Section 79 of the IT Act, 2000. https://lawbhoomi.com/a-critical-analysis-of-sec-79-of-it-act-2000

Mantelero, A. (2013). The EU proposal for a General Data Protection Regulation and the roots of the "right to be forgotten". Computer Law & Security Review, 29(3), 229–235. https://doi.org/10.1016/j.clsr.2013.03.010

Mehta, A. (2020). Digital privacy in India: Legislative evolution and judicial interpretation. Indian Bar Review, 47(1), 98–117.

Modern Dental College and Research Centre & Ors. v. State of Madhya Pradesh & Ors., (2016) 7 SCC 353. Retrieved from https://indiankanoon.org/doc/93572510/

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. Proceedings of the 2008 IEEE Symposium on Security and Privacy, 111–125. https://doi.org/10.1109/SP.2008.33

NT1 & NT2 v. Google LLC, [2018] EWHC 799 (QB). Retrieved from https://www.judiciary.uk/judgments/nt1-and-nt2-v-google-llc/

PRS Legislative Research. (2019). The Personal Data Protection Bill, 2019. https://prsindia.org/billtrack/personal-data-protection-bill-2019

Phelps, A. S. (2021). Contract fixer upper: addressing the inadequacy of the force majeure doctrine in providing relief for nonperformance in the wake of the COVID-19 pandemic. Vill. L. Rev., 66, 647.

Rosen, J. (2012). The Right to Be Forgotten. Stanford Law Review Online, 64(88), 88–92. https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. New York University Law Review, 86, 1814–1894.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880–1903.

Sri Vasunathan v. The Registrar General, High Court of Karnataka, 2017 SCC OnLine Kar 424.

Subhranshu Rout @ Gugul v. State of Odisha, 2020 SCC OnLine Ori 878.

UNIDROIT. (2016). UNIDROIT Principles of International Commercial Contracts 2016. UNIDROIT.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. https://doi.org/10.2307/1321160

Westin, A. F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), 431–453.

Zimmermann, R. (1996). The Law of Obligations: Roman Foundations of the Civilian Tradition. Oxford University Press.