



Balancing Privacy And Public Interest: Why India Needs A Clear Constitutional Stand On The Right To Be Forgotten

Nikhil Raj & Dr. Kriti Agarwal
BALLB Student & Assistant Professor
IIMT College of Law, Greater Noida

Abstract

The right to be forgotten (RTBF) is slowly gaining ground in India's legal landscape, but it remains unclear where it fits within the Constitution. While the Supreme Court recognized privacy as a fundamental right under Article 21, RTBF has not yet been fully embraced or clearly defined. This paper explores how RTBF could be integrated into Indian constitutional law without clashing with other fundamental rights like freedom of expression. It looks at recent court decisions, the new data protection law, and international examples to argue that India needs judicial clarity on this issue—sooner rather than later. The rapid expansion of digital technologies has fundamentally altered the relationship between individual privacy and public access to information in India. Personal data, once obscure or time-bound, now remains permanently accessible through search engines and online archives, often causing lasting reputational, social, and economic harm. In this context, the *Right to Be Forgotten* (RTBF) has emerged as a crucial yet contested facet of the broader right to privacy. While the Supreme Court of India, in *Justice K.S. Puttaswamy v. Union of India* (2017), recognized privacy as a fundamental right under Article 21, it stopped short of explicitly articulating the contours of RTBF. Subsequent judicial decisions and legislative efforts, including provisions under the Digital Personal Data Protection Act, 2023, reveal an evolving but fragmented approach marked by inconsistencies and uncertainty. This paper argues that India urgently requires a clear constitutional stand on the Right to Be Forgotten to effectively balance individual dignity and autonomy against legitimate public interest, freedom of expression, and the right to information. It examines the doctrinal foundations of RTBF, comparative constitutional practices, and the challenges posed by vague statutory safeguards and ad hoc judicial balancing. The study contends that without constitutional clarity, RTBF risks either being overused to suppress public accountability or under-enforced, leaving individuals vulnerable to perpetual digital punishment.

Keywords : Right to privacy, Constitutional privacy, Informational privacy, Digital privacy, Data protection, Freedom of speech and expression, Digital footprint

Introduction

In an age where digital footprints last forever, the right to be forgotten has become an urgent issue. It refers to the ability of individuals to request the removal of personal information from the internet, especially when it's outdated or no longer relevant. The idea may sound simple, but it opens up a legal and constitutional Pandora's box—especially in a country like India, where fundamental rights often come into conflict. While the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017) recognized

privacy as a fundamental right under Article 21, it didn't directly tackle RTBF. So, the question arises: Can the RTBF find a home in the Indian Constitution? And if so, what should its limits be?

The digital revolution has transformed the way information is created, stored, and disseminated, fundamentally reshaping notions of privacy, identity, and reputation. In an era where search engines, social media platforms, and online databases ensure the perpetual availability of personal information, individuals increasingly find themselves defined by past actions, allegations, or records that may no longer reflect their present realities. This phenomenon has given rise to the demand for the *Right to Be Forgotten* (RTBF), a legal claim that enables individuals to seek the removal, delinking, or restriction of personal data that is outdated, irrelevant, or disproportionately harmful. In India, the debate surrounding RTBF occupies a complex constitutional space, situated at the intersection of the right to privacy, freedom of speech and expression, and the public's right to information. The Supreme Court's landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017) recognized privacy as a fundamental right intrinsic to life and personal liberty under Article 21 of the Constitution. However, the Court did not explicitly define or constitutionalize the Right to Be Forgotten, leaving its scope to be shaped by subsequent judicial interpretation and legislative action. As a result, Indian courts have adopted inconsistent approaches—sometimes granting relief through anonymization or delinking, and at other times prioritizing transparency and open justice—thereby generating legal uncertainty.

The absence of a clear constitutional framework becomes particularly problematic in a democratic society committed to accountability, free expression, and an open judicial system. While RTBF seeks to protect individual dignity and informational self-determination, an unregulated or overly broad application risks censorship, historical erasure, and the suppression of legitimate public interest, especially in matters involving public figures, criminal proceedings, or issues of governance. Conversely, the lack of effective safeguards exposes individuals to perpetual digital stigma, undermining rehabilitation, equality, and the constitutional promise of dignity. Against this backdrop, this paper examines the necessity of articulating a clear constitutional stand on the Right to Be Forgotten in India. It explores the evolving jurisprudence on privacy, analyzes the tensions between individual rights and collective interests, and evaluates emerging statutory frameworks such as the Digital Personal Data Protection Act, 2023. The central argument advanced is that constitutional clarity—grounded in proportionality, reasonableness, and public interest—is essential to ensure that the Right to Be Forgotten functions as a protective mechanism for dignity rather than a tool for erasing accountability in India's digital constitutional order.

The Constitutional Groundwork: Article 21 and the Right to Privacy

Article 21 of the Indian Constitution guarantees the right to life and personal liberty. Over the years, the courts have expanded this to include dignity, autonomy, and privacy. The Puttaswamy judgment in 2017 was a turning point—it confirmed that privacy is not just a common law right but a constitutional one. However, informational privacy (the ability to control how personal data is shared or stored) is still a developing concept in India. If we accept that people have a right to control their data, then RTBF naturally becomes part of that conversation. But without direct judicial affirmation, it remains on shaky ground.

Article 21 of the Indian Constitution, which guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law, has been the primary constitutional foundation for the evolution of privacy jurisprudence in India. Initially interpreted narrowly, Article 21 has, through judicial creativity and constitutional morality, expanded into a repository of substantive rights essential for the realization of human dignity. The right to privacy has emerged from this expansive interpretation as an intrinsic component of life and personal liberty. In its early phase, the Supreme Court adopted a cautious approach towards privacy. In *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1963), the Court declined to recognize privacy as a fundamental right, reflecting a formalistic understanding of constitutional text. However, even within *Kharak Singh*, minority opinions and subsequent judgments hinted at the importance of privacy as a condition of personal liberty. Over time, as social realities evolved and state surveillance expanded, the Court increasingly acknowledged privacy-related interests under Article 21.

The doctrinal shift became evident in cases such as *Gobind v. State of Madhya Pradesh* (1975), where the Court recognized privacy as a “penumbral” right, subject to compelling state interest. This was followed by decisions like *R. Rajagopal v. State of Tamil Nadu* (1994), which linked privacy to the protection of reputation and autonomy, and *PUCI v. Union of India* (1997), which recognized informational privacy in the context of telephone tapping. These judgments collectively laid the constitutional groundwork for treating privacy as a fundamental right, even in the absence of an explicit textual guarantee. The culmination of this jurisprudential evolution occurred in the landmark nine-judge bench decision of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which unequivocally affirmed the right to privacy as a fundamental right under Article 21, and as part of the freedoms guaranteed by Part III of the Constitution. The Court emphasized that privacy is essential to dignity, autonomy, and the free development of personality, and recognized its multiple dimensions—spatial, decisional, and informational. Informational privacy, in particular, assumes central importance in the digital age, where personal data is continuously collected, processed, and disseminated by both state and non-state actors.

While *Puttaswamy* did not expressly articulate the Right to Be Forgotten as a standalone constitutional right, it acknowledged the individual’s interest in controlling the dissemination of personal information and in being protected against perpetual exposure of past data. Several concurring opinions hinted at the necessity of future legal frameworks to address issues such as data erasure, consent, and proportionality in information retention. Thus, Article 21, as interpreted in *Puttaswamy*, provides a strong constitutional basis for claims related to the Right to Be Forgotten, even though its precise contours remain undefined. In this sense, the constitutional groundwork laid by Article 21 establishes both the possibility and the limits of the Right to Be Forgotten. Privacy under Article 21 is not absolute and must be balanced against competing constitutional values such as freedom of speech and expression under Article 19(1)(a), the right to information, and the principle of open justice. The challenge, therefore, lies not in locating RTBF within the Constitution, but in developing a coherent constitutional framework that harmonizes individual privacy with public interest—an endeavor that remains incomplete in India’s constitutional jurisprudence.

RTBF in Indian Courts: A Mixed Picture

Indian courts have begun engaging with RTBF, but the responses have been inconsistent. For example, in *X v. Registrar General, Madras High Court* (2021), the court showed support for RTBF in principle but said the matter needed legislation. On the other hand, in *Jorawar Singh Mundy v. Union of India* (2021), the Delhi High Court allowed the removal of an old acquittal order from search engines to protect the petitioner’s dignity. These decisions show growing awareness of RTBF but also highlight the lack of a clear standard. Without a constitutional or statutory framework, courts are deciding on a case-by-case basis, which creates uncertainty.

The judicial engagement with the Right to Be Forgotten (RTBF) in India has been cautious, fragmented, and largely case-specific, reflecting the absence of a clear constitutional or statutory framework. Indian courts have acknowledged privacy-based claims seeking removal or restriction of online information, yet they have stopped short of recognizing RTBF as an independent, enforceable fundamental right. As a result, judicial outcomes reveal a mixed picture—oscillating between the protection of individual dignity and the preservation of transparency, free expression, and open justice. Early references to RTBF emerged in the context of reputational harm and media reporting. In *R. Rajagopal v. State of Tamil Nadu* (1994), though not directly addressing RTBF, the Supreme Court recognized an individual’s right to safeguard personal matters from unwanted public exposure, thereby laying the conceptual groundwork for future claims. However, the digital dimension of privacy and data permanence came to the forefront only in recent years, compelling courts to confront RTBF more directly. High Courts have been the primary arenas for RTBF litigation. In *Sri Vasunathan v. Registrar General* (2017), the Karnataka High Court permitted the anonymization of a party’s name in an online judgment involving sensitive matrimonial disputes, emphasizing the right to privacy and dignity, particularly where continued disclosure served no public purpose. This decision marked one of the earliest judicial acknowledgments of RTBF in India. Similarly, the Delhi High Court in *Jorawar Singh Mundy v. Union*

of India (2021) ordered the delinking of a judgment from search engine results where the petitioner had been acquitted, recognizing the disproportionate harm caused by continued online accessibility of criminal records.

Conversely, courts have also declined RTBF claims where public interest outweighed individual privacy. In *Subhranshu Rout v. State of Odisha* (2020), while the Orissa High Court acknowledged the relevance of RTBF, it emphasized the need for legislative clarity and cautioned against judicial overreach. The Delhi High Court, in several cases, has expressed concern that indiscriminate removal or anonymization of judicial records could undermine the principle of open justice and the public's right to know, especially in matters involving public officials, serious crimes, or issues of systemic importance. This inconsistency underscores a key structural problem: courts are forced to balance competing constitutional values without guiding standards. Decisions often hinge on factors such as the nature of the information, the passage of time, the status of the individual (private person versus public figure), and the societal relevance of the data. While such ad hoc balancing allows flexibility, it also generates unpredictability and uneven protection, leaving both individuals and digital intermediaries uncertain about their rights and obligations.

The Tension with Freedom of Speech

RTBF doesn't exist in a vacuum—it must be balanced with other rights, especially the right to free speech under Article 19(1)(a). For example, should someone be allowed to remove a public court judgment from the internet just because it hurts their reputation? What about news stories that are factually correct but damaging? These are not easy questions, and that's why a simple yes-or-no approach won't work. What's needed is a proportionality test, something the courts already use in other contexts (like in *Modern Dental College v. State of M.P.*, 2016). The idea is to weigh competing rights and find a fair balance.

The recognition of the Right to Be Forgotten (RTBF) inevitably generates a constitutional tension with freedom of speech and expression guaranteed under Article 19(1)(a) of the Indian Constitution. In a democratic society, free speech, a free press, and public access to information are foundational to accountability, transparency, and informed civic participation. Any attempt to restrict the circulation of information—particularly through erasure, delinking, or anonymization—must therefore be carefully scrutinized to ensure that it does not become a tool for censorship or historical revisionism. At the core of this tension lies the conflict between individual dignity and collective democratic interests. RTBF seeks to protect individuals from disproportionate harm caused by the perpetual availability of outdated, irrelevant, or misleading information. However, freedom of speech protects not only the right to express opinions but also the right to receive information, including access to judicial records, media reports, and historical data. When individuals seek to remove information from the public domain, especially information that was lawfully published, courts must determine whether such removal unjustifiably curtails the public's right to know.

Indian constitutional jurisprudence has consistently treated freedom of speech as a preferred right, subject only to the reasonable restrictions enumerated under Article 19(2). These restrictions—such as public order, decency, morality, defamation, and contempt of court—are narrowly construed to prevent excessive state interference. RTBF does not neatly fall within these established grounds, raising concerns about its constitutional legitimacy if applied without clear safeguards. Granting RTBF claims too readily may lead to a “chilling effect,” discouraging journalists, researchers, and digital platforms from reporting or archiving information of public relevance. The principle of open justice further complicates this balance. Judicial transparency requires that court proceedings and judgments remain accessible to the public, reinforcing trust in the legal system and enabling scrutiny of judicial decision-making. Blanket anonymization or delinking of court records, particularly in criminal or constitutional matters, risks undermining this principle. Indian courts have therefore been cautious in granting RTBF relief in cases involving public figures, serious offences, or matters with ongoing societal implications.

At the same time, an absolutist commitment to free speech ignores the asymmetry of power and harm in the digital age. The permanence and searchability of online content can amplify stigma, impede rehabilitation, and disproportionately affect private individuals who lack the means to counter negative narratives. In such cases, continued public access to certain information may contribute little to public

discourse while inflicting significant personal harm. The challenge, therefore, is not to subordinate free speech to privacy, but to calibrate both rights through a proportionality-based framework. A constitutionally sound approach to RTBF must recognize freedom of speech as a central democratic value while allowing narrowly tailored privacy protections in exceptional circumstances. Factors such as the nature of the information, its accuracy, the passage of time, the individual's role in public life, and the continuing public interest must inform judicial balancing. Without such principled limits, RTBF risks becoming either constitutionally suspect due to its encroachment on free speech or practically ineffective due to judicial reluctance. Thus, resolving the tension between RTBF and freedom of speech is essential to evolving a coherent and democratic digital constitutional order in India.

The Digital Age and the Role of New Laws

India is one of the most digitized countries in the world. With the rise of platforms like Google, Facebook, and LinkedIn, personal data can spread in seconds and stay online forever. The new Digital Personal Data Protection Act, 2023, tries to tackle some of these issues. It even mentions RTBF, giving users the right to request removal of personal data from digital platforms. But here's the catch: the law gives too much discretion to a new authority—the Data Protection Board—without clear constitutional checks. It also doesn't apply retroactively, which means older content may still stay online indefinitely. So even though the law is a step in the right direction, it's not enough.

The advent of the digital age has fundamentally transformed the nature, scale, and impact of information dissemination. Unlike traditional media, digital platforms enable instantaneous, borderless, and permanent circulation of data, making personal information easily searchable and perpetually accessible. This technological reality has intensified privacy harms and rendered conventional legal remedies—such as defamation or injunctive relief—largely inadequate. In this context, the demand for the Right to Be Forgotten (RTBF) has gained renewed urgency, compelling lawmakers to rethink privacy protection within a data-driven ecosystem. In India, the legislative response to these challenges has been gradual and evolving. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant step towards regulating the collection, processing, and retention of personal data. The Act recognizes the rights of data principals, including the right to correction, completion, updating, and erasure of personal data, thereby indirectly engaging with the logic of RTBF. By imposing obligations on data fiduciaries to process data lawfully and proportionately, the statute acknowledges the need for informational self-determination in the digital age.

However, the DPDP Act adopts a cautious and limited approach to RTBF. It does not explicitly recognize the right as a constitutional or standalone legal entitlement, nor does it provide clear standards for balancing data erasure against freedom of expression, public interest, or journalistic exemptions. Broad exemptions granted to the State and to certain categories of data processing further dilute the effectiveness of privacy protections. Consequently, individuals seeking relief often remain dependent on judicial discretion, reinforcing inconsistency rather than legal certainty. The digital environment also raises complex questions about intermediaries such as search engines, social media platforms, and online news portals. These entities play a decisive role in shaping visibility, memory, and reputational harm, yet Indian law remains ambiguous regarding their obligations in RTBF claims. Unlike the European Union's General Data Protection Regulation (GDPR), which provides a relatively structured framework for data erasure and delinking, India's approach remains fragmented and reactive. This regulatory gap places courts in the difficult position of resolving technologically sophisticated disputes without clear legislative guidance.

Moreover, the transnational nature of digital data complicates enforcement. Information hosted on foreign servers or governed by international platforms often falls beyond the effective reach of domestic law, raising concerns about jurisdiction, compliance, and regulatory sovereignty. Without harmonized standards and constitutional clarity, RTBF risks becoming unevenly enforceable, benefiting only those with the resources to litigate. Thus, while new laws like the DPDP Act reflect a growing recognition of digital privacy concerns, they fall short of resolving the deeper constitutional questions surrounding RTBF. In the absence of a clear constitutional framework, statutory protections remain vulnerable to dilution and inconsistent interpretation. A

principled constitutional stand is therefore essential to guide legislative design, regulate digital intermediaries, and ensure that privacy protections in the digital age remain balanced, enforceable, and aligned with democratic values.

Looking Abroad: What Can India Learn?

The European Union offers a useful model. In the famous *Google Spain v. AEPD* (2014) case, the Court of Justice of the EU ruled that individuals have a right to ask Google to delist outdated or irrelevant search results, even if the original content remains online. This shows that RTBF doesn't necessarily mean erasing history—it can be about limiting access. India can adapt this idea, but with local safeguards that respect both transparency and personal dignity.

Comparative constitutional experience offers valuable insights for India as it grapples with the challenge of balancing the Right to Be Forgotten (RTBF) with freedom of expression and public interest in the digital age. Different jurisdictions have responded to the problem of digital permanence in diverse ways, shaped by their constitutional cultures, regulatory capacities, and conceptions of privacy. Examining these approaches helps illuminate both the possibilities and the pitfalls of recognizing RTBF within a democratic framework. The European Union provides the most developed model of RTBF. In *Google Spain SL v. AEPD* (2014), the Court of Justice of the European Union recognized an individual's right to request the delinking of personal information from search engine results when such data is inadequate, irrelevant, or excessive in relation to the purposes for which it was processed. This judicial recognition was subsequently codified in Article 17 of the General Data Protection Regulation (GDPR), which establishes the "right to erasure," subject to clearly defined exceptions for freedom of expression, public interest, legal obligations, and historical or scientific research. The EU approach demonstrates that RTBF can coexist with free speech when governed by proportionality, procedural safeguards, and independent regulatory oversight.

In contrast, the United States has largely resisted the concept of RTBF, prioritizing the First Amendment's strong protection of free speech and press freedom. American courts have been wary of content removal mandates, viewing them as incompatible with constitutional commitments to open discourse and historical record-keeping. Instead of erasure, U.S. law relies on counter-speech, reputational remedies, and market-based solutions. This approach underscores the risks of over-regulating speech but also highlights the limited protection available to individuals facing enduring digital harm. Other jurisdictions adopt intermediate positions. The United Kingdom, while influenced by EU data protection norms, has emphasized a careful balancing of privacy with journalistic freedom and open justice. Argentina and South Korea have experimented with data erasure and delinking mechanisms, though not without controversy regarding censorship and administrative overreach. These experiences suggest that RTBF is most effective when embedded within transparent procedures, clear eligibility criteria, and appellate safeguards.

For India, comparative practice offers two key lessons. First, RTBF should not be conceived as an absolute or automatic right; rather, it must operate within a structured balancing framework that accounts for public interest, the nature of information, and the status of the individual concerned. Second, constitutional clarity is crucial. Jurisdictions with well-defined constitutional or statutory standards provide greater predictability for courts, intermediaries, and citizens, reducing arbitrary decision-making. India's constitutional tradition, grounded in proportionality, reasonableness, and the harmonization of fundamental rights, is well suited to developing a distinct RTBF framework rather than importing foreign models wholesale. While the EU's regulatory sophistication offers useful guidance, India must adapt these principles to its own democratic priorities, including transparency, access to justice, and social accountability. Learning from comparative experience thus reinforces the central argument of this paper: that a clear, principled constitutional stand is essential for ensuring that the Right to Be Forgotten in India protects individual dignity without compromising the public interest.

The Way Forward: Why the Supreme Court Must Step In

India can't afford to wait for Parliament to act. The Supreme Court should step in and issue clear guidelines. Here's what those could include- Harm threshold: RTBF should apply only if real harm is shown- Proportionality: Courts should balance privacy with public interest.^[SEP] Scope: RTBF should focus on delisting from search engines, not erasing public records.^[SEP] Appeal mechanism: There must be a way to challenge misuse or overreach. This kind of framework would give both citizens and institutions a roadmap for handling RTBF requests responsibly.

The fragmented evolution of the Right to Be Forgotten (RTBF) in India reveals a pressing need for authoritative constitutional guidance. While High Courts have addressed RTBF claims on a case-by-case basis and Parliament has introduced limited statutory protections through the Digital Personal Data Protection Act, 2023, neither route has produced a coherent, uniform, or principled framework. In this institutional vacuum, the Supreme Court of India is uniquely positioned—and constitutionally obligated—to clarify the scope, limits, and enforceability of RTBF within India's fundamental rights architecture. As the final interpreter of the Constitution, the Supreme Court has historically played a transformative role in expanding Article 21 to meet changing social and technological realities. Just as *Maneka Gandhi*, *Gobind*, and *Puttaswamy* redefined liberty and privacy in response to evolving threats to dignity, the digital age demands a similar jurisprudential intervention. The persistence of personal data online raises constitutional concerns that cannot be adequately resolved through ad hoc balancing by lower courts or through incomplete legislative measures. Without Supreme Court guidance, RTBF risks remaining unevenly applied, dependent on judicial discretion rather than constitutional principle.

Judicial intervention is also necessary to harmonize RTBF with competing fundamental rights. The Supreme Court can articulate a structured proportionality test that weighs privacy, dignity, and rehabilitation against freedom of speech, the right to information, and the principle of open justice. Clear constitutional criteria—such as the relevance of the information, the passage of time, the individual's public status, the accuracy of the data, and the continuing public interest—would enable consistent and predictable adjudication. Such guidance would not only protect individuals but also provide much-needed clarity to digital intermediaries, media organizations, and public authorities. Moreover, Supreme Court intervention can prevent the misuse of RTBF as a tool for suppressing dissent or evading accountability. By explicitly recognizing that RTBF is limited, conditional, and subject to public interest exceptions, the Court can ensure that privacy protection does not devolve into censorship. This is particularly crucial in a constitutional democracy like India, where transparency and free expression serve as safeguards against abuse of power.

Conclusion

The right to be forgotten is not about hiding the truth—it's about giving people a second chance in a world that never forgets. India's Constitution, especially Article 21, already has the tools needed to support this right. What's missing is judicial clarity. By stepping in now, the Supreme Court can prevent confusion, protect individual dignity, and make sure RTBF evolves in a way that fits with our democratic values. The debate surrounding the Right to Be Forgotten (RTBF) in India reflects a deeper constitutional struggle to reconcile individual dignity with the collective values of transparency, accountability, and free expression in the digital age. As personal information becomes permanently embedded in online spaces, the harm caused by outdated, irrelevant, or disproportionate data exposure can no longer be dismissed as incidental. Yet, the solution cannot lie in unrestrained erasure, which risks undermining democratic discourse, open justice, and the public's right to know. This paper has argued that while Article 21 of the Constitution, as interpreted in *Justice K.S. Puttaswamy v. Union of India*, provides a strong normative foundation for RTBF, India lacks a clear and authoritative constitutional framework governing its application. Judicial responses have remained fragmented, legislative interventions cautious, and regulatory guidance incomplete. The resulting uncertainty has led to inconsistent outcomes, leaving individuals vulnerable to digital stigma while simultaneously raising fears of censorship and historical manipulation. A clear constitutional stand by the Supreme Court is therefore essential. Such an intervention can articulate principled limits, embed proportionality and public interest safeguards, and

ensure harmonization between privacy, freedom of speech, and the right to information. RTBF must be recognized not as an absolute right to erase the past, but as a conditional and carefully regulated claim aimed at preventing disproportionate harm without compromising democratic accountability. Ultimately, the challenge before India is not whether society should remember or forget, but how constitutional values should govern that choice. By grounding the Right to Be Forgotten within a transparent, balanced, and constitutionally coherent framework, India can protect individual dignity while preserving the integrity of its democratic and informational ecosystem. In doing so, the Constitution can remain responsive to technological change without sacrificing the foundational principles upon which it rests.

References

- * Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- * X v. Registrar General, High Court of Madras, 2021 SCC OnLine Mad 276.
- * Jorawar Singh Mundy v. Union of India, 2021 SCC OnLine Del 2305.
- * Modern Dental College v. State of Madhya Pradesh, (2016) 7 SCC 353.
- * Google Spain SL v. Agencia Española de Protección de Datos, C-131/12 (2014).
- * Digital Personal Data Protection Act, 2023 (India).
- * European Union (2016). General Data Protection Regulation (GDPR).

