INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 4 | Issue 3 [May, 2026]| Page 189 – 203

RIGHT TO BE FORGOTTEN UNDER INDIAN LAW: CONSTITUTIONAL ROOTS AND PRACTICAL BARRIERS

- Aryottansh Panigrahi[1]

-Achint Dubey[2]

-Shraddha Suman Paikray[3]

ABSTRACT

The current paper is a co-authored Art, which investigates the notion of the Right to be forgotten (RTBF) concerning Indian law, reveals the constitutional sources of the concept within the Indian privacy jurisprudence of Art 21, and provides an overview of the impediments in the practical implementation of the concept. Part I gives some conceptual background, the history of judicial law including K.S. Puttaswamy and the conflicting decisions of the HC which cannot be reconciled with the principles of free speech and open justice according to Art 19(1) (a). Part II considers structural obstacles including procedural loopholes, enforcement of global platforms, transnational jurisdiction, technological limitations (mirrors, archives, AI indexing, blockchain) and threats of abuse in censorship. The special focus is made on criminal justice implications on those who are not found guilty, children, and the transmission of digital stigma. The EU General Data Protection Regulation (GDPR) of proportionality balancing, the resistance of UK and 17th Amendment of US teaches us certain lessons. The new spin lies in the proposal of the integrated approach such as standardized balancing tests, graded processes, platform requirements, special purpose tribunals, and Supreme Court regulations, which can create a balance between dignity and transparency. Besides literature reviews, the contribution goes beyond it and enables real-world improvements DPDPA amendments,

[1] Assistant Professor of Law, School of Law, Centurion University of Technology & Management, Bhubaneswar (CUTM), Odisha

[2] Assistant Professor of Law, School of Law, Centurion University of Technology & Management, Bhubaneswar (CUTM), Odisha

[3] Assistant Professor of Law, School of Law, Centurion University of Technology & Management, Bhubaneswar (CUTM), Odisha

institutional structures and public interest exceptions allowing RTBF to be offered to other than elites, which is the constitutional rehabilitation of digital India coming to life.

Keywords: Right to be forgotten, International Self-Determination, Art 21, Open Justice and Freedom of Expression, Data Protection

CONSTITUTIONAL ROOTS AND JUDICIAL EVOLUTION

The RTBF enables people to demand that the online personal data is removed, which is outdated, inaccurate, or otherwise inappropriate and, thus, enables the individual to be in control of their own online life. In India, this right has a constitutional basis in Article 21 which incorporates the right to privacy, including to human dignity, informational self-determination, and to control over the identity and public image.[4] The RTBF, compared to the larger privacy protections against unreasonable intrusion into the personal space, addresses the specific problem of the digital persistence of personal information even after it has become irrelevant, inaccurate, or useless. The RTBF, as the seminal *Google Spain* case of the EU has stipulated and as GDPR Art 17 has formalized, is a qualified erasure right regulated by relevant exceptions based on the freedom of expression and the public interest.[5]

The idea is not limited to what can be seen on the internet. It is also what is held in primary systems and backup repositories, archived versions and search engines indexes. Its modern legal status is an indication of an expanding international agreement that people should have some kind of control over their online footprints, particularly in the context of the information whose further circulation does not serve any good purpose and can actually actively damage rehabilitation, reintegration or mental health.

Art 21 has been broadly interpreted within the Indian jurisprudence especially after the Justice K.S. Puttaswamy v. In UOI, where a 9-judge Constitutional Bench held that privacy was part of human dignity and individual autonomy.[6] The Court emphasized the inalienability of a person in his or her personal identity, life story and informational self-determination. The ruling was a warning against the continuing digitalization of what already took place in the past, acquittals, youthful misdeeds, outdated jobs that no longer correspond to the current individual and hinder recovery. Justice D. Y. Chandrachud explained that human dignity implies the right to control personal data and the image

[4] Constitution of India 1950, art 21

[5] *Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez* (Case C-131/12) [2014] ECLI:EU:C: 2014:317

[6] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

in society because the outdated, misleading, or disproportionate information should not hinder the ability to reinvent oneself, grow, and be reintegrated into society.[7]

The concept of informational self-determination as is described by Justice Sanjay Kishan Kaul offers the essential grounding to claims made on the RTBF.[8] This doctrine supports the capacity of an individual to request the deletion of information that is not necessary, relevant, and accurate and allows them to become actively involved in society without being under the continuous digital stigma. The proportionality doctrine that was developed in Puttaswamy applies to any alleged interference with basic rights, but that such interference must meet four conditions: *lawfulness* (authorized by a law), *legitimate purpose* (furtherance of a constitutionally valid objective), *necessity* (proportional to the purpose with minimal interference), and *strict proportionality* (ought to have substantially greater benefits than harms).[9] It follows that in RTBF claims, one must establish that the further presence of information results in a disproportionate encroachment on the dignity, rehabilitation or informational autonomy upon balancing with competing state interests including transparency, access of the courts to publicity, and freedom of the media.

RTBF has been slowly realized, through fact-specific directions in Indian courts, especially where acquittals or minor offences are concerned, as a manifestation of a growing judicial preference in favour of post-trial privacy. Nevertheless, the lack of a uniform doctrinal system has served to deliver highly divided results in the benches of the HCs with inconsistencies in outcomes and providing dubious solutions.

The prominent example is *Jorawer Singh Mundy v. UOI* where the Court directed Google and legal databases including Indian Kanoon to remove an acquittal judgment that had a negative implication on employment prospects of the petitioner in the United States.[10] The ruling thought off the RTBF as a process of privacy rights that has to be carefully balanced between the reputational interest of an individual to forget a criminal charge and the long-term right of people to know about judicial processes. The Court refused to recognize the RTBF, as it considered that the posting of acquittal judgments on the Internet, even when labeled as non-reportable according to the statutory provisions, did not amount to a constitutional violation, which should be actively addressed by the state and the listing of the platform.[11] The ruling accorded precedence to the principles of open justice and assumed

[7] ibid [149] (Chandrachud J)
[8] ibid [189] (Kaul J)
[9] ibid [180]-[183] (Chandrachud J)
[10] *Jorawer Singh Mundy v Union of India WP(C) 3918/2021 (Delhi HC, 8 June 2021)*
[11] *Dharamraj Bhanu Shankar Waghela v State of Gujarat* Special Civil Application No 7092/2017 (Gujarat HC, 19 May 2017)

that the general good of available databases of the judgment overrides arguments of reputational damage to individual plaintiffs or other negative impacts on their future employment.

The Karnataka HC required the anonymization of the judicial records of a rape victim whose daughter, in its turn, required the protection of the identity in the conditions of sexual crime, bodily dignity, and vulnerable identity.[12] Such a practice represents a wider international judicial trend of confidentiality and anonymity of cases that involve the rights of women, their modesty, child safety, and the security of the vulnerable persons. *Vysakh K G v. UOI* limited the use of the RTBF to very limited framed retrospective claims and denied it the power to weaken the spirit of open justice, where broad recognition would be a stimulus to strategic litigation to suppress unflattering but legitimate information.[13] On the same note, Madras HC in *Karthick Theodore* first denied relief under the provisions of the RTBF but a Division Bench reconsidered by permitting certain redaction under certain conditions.[14] The jurisprudence is in flux, with that decision and other related special leave appeals being suspended by the Supreme Court in 2024.

Taken together, these HC developments reveal the piecemeal and case by case application of the RTBF in India and highlights the lack of uniform and consistent judicial principles. This division promotes forum-shopping where petitioners shop in favourable venues and generates a substantive uncertainty as to whether remedies may be available in future similar patterns of facts.

STATUTORY FRAMEWORK AND COMPETING RIGHTS

The Information Technology Act of 2000 is only somewhat relevant to the RTBF (RTBF) with Section 79(3) and the Intermediary Guidelines of 2021 requiring the removal of privacy-invasive material at the time of receipt of a court order or other valid user complaints based on infractions of the law.[15] These provisions do not provide an active or autonomous erasure right, they are in fact reactive following the direction or complaint by the court. They do not legalize platforms to start erasure processes on their own and do not draw clear protocols on how people seek erasure.

The Digital Personal Data Protection Act of 2023 (DPDPA) is a positive legislative development. Section 12 lays down a qualified right to erasure which gives data principals a right to request the deletion of personal data after the consent is withdrawn or the initial purpose of the processing is

[12] *Name Redacted v Registrar General* Writ Petition No 62038/2016 (Karnataka HC)
[13] *Vysakh K G v Union of India* WP(C) No 18207/2022 (Kerala HC, 28 June 2022)
[14] *Karthick Theodore v Union of India* WP(MD) No 9414/2021 (Madras H
[15] Information Technology Act 2000, s 79(3)

achieved.[16] This right is however highly limited in terms of exceptions concerning legal duties like adherence to court orders or statutory retention demands, journalism vigor including lawful media and academic activities, archival services to historical archives and vaguely defined considerations of the public interest. Although withdrawal of consent has the effect of obligating data fiduciaries to immediately cease processing, the carve outs, especially to state activities and to the public, are far more expansive, which significantly narrows the practical meaning of erasure.

Section 27 also creates the DPB that has the power to examine breaches of the DPDPA, imposes penalty up to 250 crore rupees, makes binding compliance orders, and hears complaints involving erasure under Section 27.[17] The regulatory and inquisitorial functions of the Board partly fill the regulatory voids that once necessitated a visit to the constitutional courts, but this still does not cover court rulings and judicial decisions, so the Board has an essential shortcoming. Such omission requires that persons who seek to have judgment records removed seek constitutional redress as opposed to regulatory grievances and so provides dual and inefficient enforcement vehicle.

The freedom of speech and expression, as stated in Art 19(1)(a) of the Constitution of India, often goes against the RTBF.[18] The courts must strike a balance between informational privacy and the right to know, where the issues of transparency, especially concerning judicial records and issues of public interest, have usually won. It has become common practice to yield to proportionality since Puttaswamy, allowing delisting or erasure in case the ongoing provision of information does not have any subsisting public interest and where the prejudice to human dignity is substantially greater than the benefit of disclosure to the community. The open-court principle, which considers transparency and the ability to access as the cornerstones of the legitimacy and accountability of the justice system, adds to the sharpness of this controversy. The HCs, such as in Kerala, have also held that RTBF cannot be invoked in ordinary to stifle any proceedings taking place and that at best, it can have a retrospective and restrictive effect without providing the pre-emptive concealment of judgments that the administration of justice requires.[19]

Courts have generally favored public accountability, freedom of the media and institutional transparency over individual delinking requests in cases where criminal acquittals, cases of greater social interest (like corruption in government) or longer systemic issues of rights violation, or patterns of misconduct are concerned. However, an opposite judicial tendency has taken shape to advance

[16] Digital Personal Data Protection Act 2023, s 12
[17] ibid s 27
[18] Constitution of India 1950, art 19(1)(a)
[19] Vysakh K G v Union of India (n 10)

anonymization and redaction, especially when the victims, vulnerable individuals, children, or non-public personalities are involved. A subsequent authoritative decision of the Supreme Court may pull these two ways into a unified effort whereby human dignity and rehabilitation, and informational access and institutional responsibility are harmonized through a formulated set of guidelines.

At present, split decisions of the HC create confusion in the doctrines that create forum-shopping and procrastinating quality relief to deserving people. It is challenging to enforce it against transnational intermediaries, like Google, Meta, and Twitter, and often only voluntary compliance or contempt actions, which are expensive and time-consuming.

PRACTICAL BARRIERS, CRIMINAL JUSTICE IMPACTS, AND COMPARATIVE LESSONS

A clear and standard procedural mechanism that allows data principals to demand erasure or de-indexing on digital platforms does not exist in India at this time. Digital Personal Data Protection Act (DPDPA) does not provide in-depth subordinate regulations to clarify a set of procedural provisions, the level of the evidence, the time frame, or the possibility of an appellate procedure. Without special purpose regulatory tribunals with special expertise on matters of digital rights, individuals would be left to piece-meal litigation before the HCs and the lower civil courts, with their differences in civil judicial philosophy and competing legal values producing highly inconsistent standards and substantive results.

In contrast to the GDPR (GDPR), which explicitly sets direct and affirmative responsibilities on the controllers and processors to adhere to the erasure requests and provide a documented response, Indian legislation does not directly stipulate the search-engine-specific obligation in the de-indexing or de-referencing of legal content.[20] Isolated cases in which the HC issued directives were based on news portals or intermediaries, including the case of 2019 in which SC held that they are inter partes, meaning that they bind only the concerned parties, and have no precedent or model of systemic enforcement that can be enforced in general on the digital ecosystem at large.[21] Therefore, this case-by-case system does not produce scalable and repeatable mechanisms that the smaller platforms or individuals could look to.

Significant online platforms that store or catalogue material, including Google as well as Facebook, LinkedIn and hundreds of aggregators, are located abroad, mainly in the United States, thus

[20] Regulation (EU) 2016/679 (n 2) arts 12–17

[21] *Zulfiqar Ahman Khan v Quintillion Business Media Pvt Ltd* (2019) SCC Online Del 6871

implicating deep questions of extraterritoriality and conflict of laws. Mutual legal assistance requirements, the unequal recognition of foreign decisions, and essentially different free-speech principles all come in the way of erasing the data reflected on foreign servers or stored in third-party archives. A takedown request issued by an Indian court targeting Google.in domain can be partially successful, but so can a European.eu domain since it is governed by GDPR. However, the United States.com domain or archives remains intact, thus making erasure incomplete.

The technical and structural inertia of content via mirrors, web archives, content-scraping activity, data brokers and decentralized technologies, including some blockchain deployments, make full forgetting technically inaccessible even when it is enforced by the mandate of Indian authorities or courts. Information that has been dispersed by the indexing AI and large-language models that are trained to combine information in scattered traces can both rediscover so-called forgotten data, thus undermining the practical value of takedown or de-indexing requests. An unregulated or too general RTBF (RTBF) system would have been allowing influential parties to erase historical information in the name of privacy protection. Politicians, corporations, or government officials may erase evidence of past wrongdoings in the name of privacy protection, thus frustrating accountability and the memory of the democracy. Besides, this kind of regime is a significant threat of chilling effect on investigative journalism, academic commentary, research in archives, and the basic right of the people to know about those things of interest to the community.

The interests involved with RTBF are most intense in regard to persons involved with criminal cases, including the acquitted, the undertrials, the juveniles, and the victims, whose digital footprints frequently last longer than the length of the criminal case by many years or decades. Archivable records, press releases, aggregator websites, and social-media rhetoric create what is called a phenomenon of digital stigma, thus continuing to cause punitive and reputational damage regardless of conviction, acquittal or official exoneration. To acquitted persons trying to obtain a job, a place to live, loans, or even social acceptance, the fact that the high-ranking search results when their names are brought up are associated with criminal charges regardless of the results, is significant barriers.

In the case of *Jorawer Singh Mundy*, an American citizen of Indian descent who was acquitted in a narcotics case, the client wanted the records of judgments taken off Google, Indian Kanoon and other sites because the records were in his detriment more than an outright exoneration.[22] The Delhi HC offered some interim relief on the basis that irreparable prejudice can be caused to a social life of an

[22] Jorawer Singh Mundy v Union of India (n 7)

acquitted individual, his/her professional chances, and dignity. The juveniles enjoy a clean slate aspect evident in the JJ Act that hearts the belief of the constitution that young people deserve the chance to be rehabilitated without them bearing any legal stigma throughout life.[23] The Rajasthan HC determined that the RTBF by the destruction of juvenile delinquency records was an absolute right in which the advantages of Section 24 have been invoked, so it limited the State as such to request or access information on the previous juvenile delinquency.[24] The Court emphasized that the aim of section 24 and rule 14 of the Juvenile Justice Model Rules, 2016 is to cull the conviction as an effective disqualification of the future of the juvenile in question, which would be counter-intuitive in case digital records propagate the stigma that the statutory legislation strives to eliminate.

Even the right to life, liberty, and dignity is associated with rehabilitation of criminals and protection of children against stigmatization in adulthood, and this is already reflected in constitutional decisions that the conviction of juveniles should not be a permanent disqualification in education, employment, or social inclusion. Calibrated expansion of RTBF to convicted persons, rehabilitated offenders, and the vulnerable victims, in this commitment to the constitution, makes it easy to substantially reintegrate into the society as opposed to the digital punishment that may never be ended in line with rehabilitation.

Comparative jurisprudence exposes varying approaches to law in organizing the RTBF (RTBF) that does not entail a complete abandonment of the principles of free expression or the transparency of justice and can therefore be a very useful study in the development of the Indian legal system. In *Google Spain SL v. Agencia Espanola de Proteccion de Datos*, Court of Justice of the EU found that an operator of an internet search-engine bears liability in processing personal data that has come up on third-party webpages and could be ordered to de-index links when the information is incorrect, irrelevant and excessive to the purposes of processing and of the fundamental rights of the data subject.[25] Art 17 of the GDPR makes a right to erasure codified under certain exceptions, such as freedom of expression, legal considerations, the public interest in public health, and archival considerations to conduct research.[26]

The implementation of proportionality analysis on a case-by-case basis by UK courts applying the GDPR and the Data Protection Act 2018 has led to the occasional de-indexing of court records, where

[23] Juvenile Justice (Care and Protection of Children) Act 2015, s 24

[24] *Ravinder Singh @ Raj Pal v State of Rajasthan* Special Civil Writ Petition No 10931/2020 (Rajasthan HC, 26 February 2021)

[25] Google Spain SL and Google Inc v Agencia Española de Proteccion de Datos (AEPD) and Mario Costeja González (n 2)

[26] Regulation (EU) 2016/679 (n 2) art 17

the courts have shown reluctance to erase the records in favor of the principles of open-justice.[27] The United States, on the contrary, is shown to have been hesitant about the idea of a comprehensive RTBF, focusing instead on the First Amendment and allowing only restricted systems of expungement or sealing, highlighting the real dangers of erased history to democratic responsibility and historical continuity.[28] The comparative models suggest that India needs to consider a statutory, rights-based RTBF model with rigid grounds and exceptions and to take great care, where judicial and archival records are required, to draw a line between erasure and de-indexing. Moreover, these models also bear testament to the fact that independent data-protection authorities, with technical expertise and adjudicatory authority, should be vested with all RTBF determinations, as opposed to leaving all determinations of RTBF to constitutional courts on a writ-by-writ basis.

STRUCTURED FRAMEWORK, REFORMS, AND CONCLUSION

Due to the constitutionally assured privacy and the pragmatical obstacles mentioned above, India needs a more comprehensive outline that incorporates procedural protection, institutions of specialization, and platform requirements. A framework like this one should not be blind to the major power and access asymmetries: the RTBF (RTBF) should not end up as a privilege of the wealth, as common citizens continue to be constantly exposed on the internet.

A threshold process might draw the line between material that is obviously stale, inaccurate or lawless and which may be under-speedily removed by the courts or regulators and material that presents a significant public-interest or free-speech issue and in which case the latter would be subjected to a higher qualification and a trial to determine the matter between the original publisher and the representatives of the public interest. Courts are to express general constitutional principles and doctrinal limits, whereas specialized regulatory institutions or appellate courts under the Digital Personal Data Protection Act (DPDPA) should conduct more every day and fact-focused RTBF adjudication with technical support and technological advice.

An Indian balancing test may expressly consider such things as the character and seriousness of the underlying crime or incident, the length of time elapsed since the incident, the legal conclusion of any action (acquittal, conviction, dismissal), the position of the data subject as a public person or a private individual and the on-going newsworthiness of the information. The effect on the victims and

[27] Data Protection Act 2018
[28] US Constitution amend I

communities should also be included in this test, so RTBF claims do not unintentionally oppress the voice of the violence victims or have a deleting effect on documented patterns of systemic abuse. Platforms must have obligations to offer positive obligations to avail RTBF interfaces, make decisions on reasoned requests within a reasonable timeframe, record and document decisions, give transparent accountability to applicants and first content publishers. The design of the regulation has to consider programmatic non-compliance, which can be sanctioned periodically, and periodic compliance audits of systematic non-compliance, as opposed to purely notice-and-take-take-takedown models which leave all the burden on the individual to manoeuvre through the complex corporate procedures.

A number of legal and institutional changes are welcome to get out of ad hoc judicial experimentation and have a principled, workable RTBF regime. Parliament ought to make clear, by making changes to the DPDPA or other related laws, what RTBF does actually mean and how it connects with the open-court principle and the right of archives, as well as how it is actually applied in relation to intermediaries, search engines and public databases. Based on the Puttaswamy and other HC cases on acquitted individuals and juveniles, the Supreme Court may provide doctrinal teachings that the lower courts and regulators would systematically consider in RTBF decisions, to establish predictability and consistency.

Certain consistency in decisions, such as systematic review of platform refusals and regular compliance audits, could be guaranteed by having an independent Data Protection Board or specialized RTBF appellate body with techno-legal expertise. The public-interest exemptions about journalism, academic research, systemic violations of rights, and serious economic crimes should be properly specified, and a rebuttable presumption should be against erasure when the information is related to the current democratic debate or institutional responsibility. The debate on the Indian RTBF needs to take a decisive step beyond the abstract privacy speech dichotomy and address the reality of the institutional design, technological possibility and criminal-justice reform. With forward-looking the experienced life of the exonerated, the seeking-new-life juveniles and the victimized population, and by learning through comparative modes, an Indian RTBF structure can bring into play constitutional pledges of dignity and rehabilitation in a digital saturation industry.

RTBF can be taken as a civil right that enables people to demand the removal of their personal data on the Internet resources when these data become irrelevant, unproportional, superfluous, and harmful. This right is not limited to visible data only, but covers information held in primary systems, backup repositories, etc. The legal formulation of modern time can be traced to the historic case of the Spanish case of Mario Costeja Gonzalez where the Court of Justice of the EU ordered Google to

delete such links on its search engines to old auction notices.[29] The principle was later formalized in Art.17 of the GDPR of the EU, the qualified right to erasure, which is limited by restrictions based on freedom of expression and public interest.

The RTBF is theoretically different to the associated teachings. The privacy law is mainly used to protect people against unwarranted invasion into their personal lives. Erasure is the technical aspect of deleting information and the law of reputation is used to consider defamatory damage without requiring an obligation of proactive removal on the internet. Although the right to privacy is a broader argument that covers the control and sharing of personal data, the RTBF deals more specifically with the surge of digital data despite loss of relevancy.

The constitutional basis of the RTBF has enshrined under Art 21. Art 21 that protects the right to life and personal liberty has been widely applied to cover the right to privacy, especially in *K.S. Puttaswamy v. UOI*.[30] This historic decision by a nine-judge Constitution Bench confirmed that privacy cannot be separated out all of human dignity, individual autonomy and informational self-determination. The Court emphasized the right of a person over his or her own identity and personal life story and warned against the long-term digital marking of the events of the past that do not represent the current identity of a person.

The human dignity inevitably requires the ability to regulate the identity, personal information and public image, so that outdated or misleading facts cannot hinder the process of receiving assistance after acquittal or other dramatic changes in life. Informational self-determination is the idea that is advocated by Justice Sanjay Kishan Kaul that allows an individual to request the removal of the no longer needed, relevant, or accurate data, which allows one to develop and reinvent themselves.[31]

The doctrine of proportionality as the guiding principle in any state interference with the fundamental rights was also laid down in the Puttaswamy decision where such a course of action should pass the tests of legality, justified purpose, necessity and a proper balancing of the interests.[32] In turn, the claims made in the context of the RTBF should indicate that the ongoing provision of information is a disproportional intrusion upon its own scale, in comparison to other state interests, including the access of courts to their records.

The Indian judiciary has been progressively accepting the RTBF by the use of fact-specific commands, especially where acquittal or minor offences are involved, and is indicative of a new judicial tendency

[29] *Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja González* (n 2)
[30] *Justice KS Puttaswamy (Retd) v Union of India* (n 3)
[31] ibid [189] (Kaul J)
[32] ibid [180]– [183] (Chandrachud J)

to privacy after conviction. Nevertheless, there has been no coherent doctrinal framework and thus the divergent results among various benches.

An interesting example is *Jorawar Singh Mundy v. UOI*, in which the Court directed Google and legal databases like Indian Kanoon to delist an acquittal judgment which was negatively impacting the petitioner in his job search in the United States.[33] The ruling considered the RTBF as a dynamic aspect of the right to privacy where there was a need to find a balance between the reputation of a person and the right of the masses to information.

Dharamraj Bhanu Shankar Waghela v. State of Gujarat refused to acknowledge the RTBF, as the online posting of acquittal judgment which was declared as non-reportable did not constitute a constitutional violation.[34] It ruled in favor of the principle of open justice and public access to court documents rather than on the argument of reputational damages to individuals.

Compared to it, in *Name Redacted v. Registrar General (Karnataka HC)* the Court ruled that the name of the daughter of a rape victim must be removed off the judicial records, saying that protection of identity in sexual offence and dignity cases is essential.[35] This strategy is indicative of a wider international judicial trend to incline towards secrecy and anonymity in cases involving women issues, decency and frail identities.

Although a judicial trend is currently inclined to endorse anonymization in circumstances that require privacy, there is still high degree of doctrinal fallout. In a case known as *Vysakh K.G. v. UOI*, the Kerala HC limited the scope of the application of the RTBF to very specific retrospective claims and refused to allow it to erode the core value of open justice.[36] On the same note, relief based on RTBF was at first denied by the Madras HC in Karthick Theodore but a Division Bench would subsequently permit redaction to some extent.[37] The Supreme Court stayed that decision, as well as related SLP, in 2024. Together, the above-mentioned developments reveal fragmentary and case-specific enforcement of RTBF in India, which highlights the importance of the lack of clear and consistent judicial norms.

The IT Act, 2000 provides little RTBF relevance through Section 79(3) and Intermediary Guidelines 2021, requiring privacy-invasive content to be removed on the court order or complaint, but no proactive erasure rights.[38]

---

[33] *Jorawer Singh Mundy v Union of India* (n 7)
[34] *Dharamraj Bhanu Shankar Waghela v State of Gujarat* (n 8)
[35] *Name Redacted v Registrar General* (n 9)
[36] *Vysakh K G v Union of India* (n 10)
[37] *Karthick Theodore v Union of India* (n 11)
[38] Information Technology Act 2000, s 79(3); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

DPDPA (DPDP Act) makes the right to erase available in Section 12, which requests delegates of data may request to be deleted when they withdraw their consent or when the purpose has been fulfilled and it has become legal to do so, or when it is required by journalism or other reasons of interest.[39] The withdrawal of consent permits the halt of processing, but the carve-outs of archival or state purposes restrict processing.

Section 27, through the DPB, actively adjudges breaches, fines to 250 crore, orders remedies and addresses erasure complaints against data fiduciaries, encouraging compliance instead of direct judicial overruling.[40] The gap-filling powers of inquisitorial powers of DPB remain, although non-application to the court records has continued to be an obstacle.

RTBF collides with Art 19(1)(a) of the freedom of speech and expression where privacy versus freedom of the public to know is weighed on courts tend to give the second category a higher score on judicial proceedings.[41] Delinkings are only immediate in a situation where there is no current public interest.

Compared with the open court principle, which is based on transparency, Kerala HC rules RTBF inapplicable to current proceedings, is applicable however, not in masking judgments ex-ante.[42] Madras HC concurred with the fact that RTBF could not wipe away court records which are part of justice administration.

The trends in the acquittals of crimes or issues of common concern, which are dominated by public interest, transparency and media freedom, are observed in rejections where information assists in accountability, and the trends are anonymized in cases of victims or non-public individuals. Dignity vs access guidelines could harmonise the Supreme Court consolidation.

This uncertainty is a result of judicial inconsistency between HCs, where there is no binding precedent and forum-shopping and stalled relief. The global platforms such as Google are hard to enforce, and it depends on the voluntary compliance or contempt.

The limited scope of DPDP Act means that it does not govern government or judicial data, and the young nature of the DPB (as of 2026) is not proven to be effective. Barriers are enhanced by technical challenges in full delinking such as archives and caches.

This is too far to choke journalism or RTI which requires subtle tests. Legislative guidance through DPDP regulations or amendments is necessary to provide uniformity.

---

[39] Digital Personal Data Protection Act 2023, s 12

[40] ibid s 27

[41] Constitution of India 1950, art 19(1)(a)

[42] *Vysakh K G v Union of India* (n 10)

The IT ACT,2000, in its turn, indirectly supports the RTBF with the help of the Section 79(3) and is re-affirmed with the help of the Intermediary Guidelines, 2021, according to which the online platforms have an authority to respond to the court orders or substantive and legitimate complaints to remove the content that violates the law or infringes the privacy rights of an individual.[43] But the statutory framework does not grant an individual autonomous or proactive right to erasure, it limits erasure to reactive measures under the impact of extraneous requirements.

It is more clearly stated in the DPDPA. Section 12 brings a qualified right to erasure, in which personal data can be requested to be deleted by the data principal when the consent is withdrawn or when the data was originally gathered to meet the reason why it was gathered in the first place.[44] However, a set of exemptions limits this right such as legal considerations, journalism, the preservation of archives and the societal interests of people. Although the withdrawal of consent binds the data fiduciary to stop processing this is subject to broad carveouts especially those legislated by government and public bodies and thus limits the effective application of erasure.

Section 27 defines DPB that has powers to probe breaches, impose fines up to 250 crore, give compliance orders and adjudicate complaints in relation to erasure complaints filed against data fiduciaries.[45] Though the regulatory and inquisitorial roles of the Board somewhat seal the gaps in enforcement, by excluding the judicial records it deliberately does not cover the judicial records, which could be one of the most essential points of possible infringement.

The RTBF is often in conflict with the freedom of speech and expression in the Arts 19(1)(a).[46] The courts have no choice but to balance informational privacy and the right to know by the populace and in this balancing act, issues of transparency, in particular, judicial records, tend to carry the day. Developing out of the Puttaswamy ruling, proportionality has now been adopted as the general rule, allowing delisting or erasure only where the further provision of information in the public has no material public interest.

What adds to this tension is the open court principle which sees transparency as a pillar to judicial legitimacy. These HCs (such as the Kerala HC) have stated that the RTBF cannot be used to silence current proceedings and may at best act in a retrospective fashion, therefore barring pre-emptive concealment of judgment.[47] Similar findings have been made by the Madras HC, which decided that

[43] Information Technology Act 2000, s 79(3); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

[44] Digital Personal Data Protection Act 2023, s 12

[45] ibid s 27

[46] Constitution of India 1950, art 19(1)(a)

[47] *Vysakh K G v Union of India* (n 10)

the court records which are a part and parcel of the judicial administration are usually beyond any removal under RTBF claims.

Courts have frequently given more weight to societal accountability, media freedom and institutional openness than personal demands to delink in situations of criminal acquittal or of more general societal importance. However, another line of judicial trend, which leans towards anonymization, has taken shape where the victim, vulnerable individual or non-public person is concerned. The successful resolution of these conflicting approaches could be an authoritative ruling by the Supreme Court that could give order to this by setting down some orderly guidelines that would balance between the sanctity of human dignity and the right of the people to know.

Currently, the divided decisions of the HC create doubt in doctrinal matters, promote forum-shopping, and delay the administration of efficient relief. It is also difficult to enforce duties on transnational intermediaries like Google because the duties are often enforced by means of voluntary compliance or by contempt.

Besides, the restricted scope of the DPDP Act to governmental and judicial data, as well as the new and unexplored operation of the Data Protection Board, again restricts the potential practical scope of the RTBF. The enforcement is hampered by technical barriers such as perennial indexing, stashed content and third-party archival repositories.

Lastly, unqualified valuation of RTBF is also a threat to chilling journalism, scholarly research, and the right to information in general. This highlights the need of standards that are well-calibrated. The level of consistency, predictability and rational balance between privacy, transparency and free expression requires clear legislative guidance, either in the form of subordinate rules or statutory amendment.