

1. Right To Be Forgotten- Polity

The Supreme Court issued notice on a plea challenging a December 2025 Delhi High Court ruling that ordered the removal of past news reports about a banker discharged in a money laundering case, raising questions on the scope of the “right to be forgotten” (RTBF)

Background and Origin of the Right to be Forgotten (RTBF)

European Jurisprudential Foundation

The Right to be Forgotten (RTBF) gained global prominence through the 2014 judgment of the European Court of Justice in the *Google Spain SL v. AEPD and Mario Costeja González* (2014) case. In this case, a Spanish citizen sought removal of links to a newspaper notice about his past debt recovery proceedings, arguing that the information was outdated and prejudicial. The Court held that search engines qualify as “data controllers” under EU law and can be directed to remove links to personal data that is–

1. Inadequate
2. Irrelevant
3. No longer relevant
4. Excessive in relation to the purposes for which it was processed

This judgment established the principle that individuals can demand delinking of personal data from search engine results, even if the original publication remains lawful.

Codification in EU Law

The principle was formally incorporated into the General Data Protection Regulation (GDPR) under Article 17 (Right to Erasure).

Article 17 provides grounds for erasure such as–

1. Withdrawal of consent
2. Data no longer necessary for original purpose
3. Unlawful processing
4. Legal obligation to erase

However, it also establishes limitations where erasure may be refused, including–

1. Freedom of expression and information
2. Compliance with legal obligations
3. Public interest in public health
4. Scientific or historical research
5. Legal claims

This structured balancing model became the global benchmark for RTBF discussions.

What is the Right to be Forgotten?

The Right to be Forgotten is a privacy-based entitlement allowing individuals to–

1. Request deletion or removal of personal information from online platforms.
2. Seek “delinking” of content from search engine results.
3. Prevent continued public accessibility of outdated, irrelevant, or prejudicial data.

It typically applies to–

1. News reports
2. Court records
3. Photographs and videos

4. Social media posts
5. Archived digital content

Importantly, RTBF does not automatically erase history. Rather, it regulates digital accessibility and discoverability, particularly via search engines.

Normative Importance of RTBF

Protection of Privacy– Prevents perpetual digital exposure of outdated or irrelevant personal data. Reinforces informational self-determination in the digital age.

Preservation of Digital Dignity– Protects individuals from permanent reputational harm due to past allegations, minor offences, or acquitted cases. Recognises that digital permanence can undermine social mobility.

Alignment with Global Standards– Moves India closer to data protection regimes such as the GDPR. Strengthens India's position in cross-border data governance.

Balancing Competing Constitutional Values

Attempts to harmonise–

1. Right to Privacy (Article 21)
2. Freedom of Speech (Article 19(1)(a))
3. Public interest in transparency

Rehabilitation and Reintegration

Particularly relevant for–

1. Acquitted individuals
2. Persons who have completed sentences
3. Juveniles in conflict with law

RTBF supports restorative justice principles.

Key Challenges in Implementing RTBF

Conflict with Press Freedom

1. Risk of censorship or rewriting history.
2. Journalistic archives serve democratic accountability.

Determining Public Interest

Courts must conduct a proportionality analysis–

1. Is the individual a public figure?
2. Is the information relevant to public discourse?
3. Is the data accurate and lawful?

Limited Statutory Clarity in India– The Digital Personal Data Protection Act, 2023 (DPDP Act) provides data erasure rights but does not explicitly codify RTBF in the European sense. No detailed procedural mechanism exclusively for RTBF claims.

Technological Complexity

Data replication across–

1. Multiple platforms
2. Cloud storage
3. Global servers

Erasure across jurisdictions is difficult.

Judicial Burden– Potential surge in petitions may overburden courts.

Risk of Misuse– Powerful individuals may attempt to suppress legitimate reporting. Could reduce transparency in cases involving corruption or public office.

Legal Position in India

Information Technology Act, 2000– Section 43A of the Information Technology Act, 2000 imposes liability on companies for failing to protect sensitive personal data. Focus is on data security breaches rather than erasure rights.

IT Rules, 2021– Provide grievance redressal mechanisms. Enable users to request removal of certain unlawful or harmful content. However, they do not formally recognise RTBF.

Digital Personal Data Protection Act, 2023– Provides a right to correction and erasure of personal data. Establishes the Data Protection Board of India for enforcement.

Based on principles of–

1. Consent
2. Purpose limitation
3. Data minimisation
4. Accountability

However, unlike GDPR Article 17, it does not articulate a comprehensive RTBF balancing doctrine.

Judicial Recognition in India

Constitutional Foundation

In *K.S. Puttaswamy v. Union of India*, the Supreme Court recognised privacy as a fundamental right under Article 21. The Court acknowledged informational privacy and referred to global practices including EU regulation. It noted that RTBF may be part of privacy rights but is not absolute.

Delhi High Court Precedent

In *Jorawar Singh Mundy v. Union of India*, the Delhi High Court directed removal of online records of a narcotics case where the petitioner had been acquitted. The Court held that continued digital availability was adversely affecting employment prospects. It emphasised proportionality and fairness. Indian courts have thus applied RTBF on a case-by-case basis without comprehensive legislation.

Comparative Perspective

Aspect	European Union	India
Explicit RTBF Law	Yes (Article 17 GDPR)	No explicit RTBF provision
Constitutional Basis	Data protection as fundamental right	Privacy under Article 21
Balancing Framework	Statutorily defined	Judicially evolved
Enforcement Body	Data Protection Authorities	Data Protection Board of India

Way Forward– Policy and Institutional Roadmap

Codified RTBF Framework

Explicit statutory articulation of–

1. Scope
2. Grounds
3. Exceptions
4. Procedural safeguards

Proportionality–Based Adjudication

Courts and regulators should apply a structured test–

1. Legality

2. Legitimate aim
3. Necessity
4. Proportionality

Independent Oversight Mechanism- Empower Data Protection Board to adjudicate RTBF claims rather than burdening constitutional courts.

Technological Cooperation- Mandatory compliance frameworks with search engines and digital intermediaries. Interoperability standards for cross-platform delinking.

Safeguards Against Abuse- Strict scrutiny for requests from public officials or politically exposed persons. Protection of investigative journalism archives.

Public Awareness and Digital Literacy- Citizens must understand both their privacy rights and limits.

Concluding Assessment

The Right to be Forgotten in India is evolving at the intersection of-

1. Constitutional privacy jurisprudence
2. Data protection legislation
3. Technological realities
4. Democratic accountability

Its future trajectory will depend on crafting a calibrated legal architecture that-

1. Protects dignity and informational autonomy,
2. Preserves freedom of expression, and
3. Maintains transparency in a constitutional democracy.

Source- <https://indianexpress.com/article/legal-news/right-to-be-forgotten-supreme-court-to-examine-if-it-applies-to-online-news-10518268/#~~~text=The%20Supreme%20Court%20Friday%20issued,past%20news%20reports%20after%20an>