



Balancing Digital Privacy and Freedom of Information: The Right to Be Forgotten Across Three Jurisdictions

Ms. Meenakshi Singh^{1,*}, Dr. Vivek Malik²

¹ Research Scholar, Department of Law, Kalinga University, Raipur, Chhattisgarh, India

² Assistant Professor, Department of Law, Kalinga University, Raipur, Chhattisgarh, India

* Corresponding author: meenakshi495684@gmail.com

ARTICLE INFO

Article history:

Received: 22-07-2026

Received in revised form:
31-07-2026

Accepted: 04-08-2026

Available online :05-08-2026

Keywords:

Freedom of expression

Informational privacy

Open justice

Right to be forgotten

ABSTRACT

Digital search makes accurate but outdated personal information persistently accessible, creating tension between informational privacy and interests protected by freedom of expression, access to information, and open justice. This article compares the law governing the right to be forgotten in the European Union, the United States, and India through a qualitative doctrinal analysis of legislation, regulatory materials, and leading judgments available through 19 July 2026. The comparison identifies three models. European Union law recognises qualified erasure and de-referencing subject to safeguards for expression, journalism, archives, research, legal claims, and continuing public interest. United States law generally protects truthful, lawfully obtained public-record information, while sectoral and state consumer laws provide narrower deletion rights. India recognises informational privacy constitutionally, but its statutory erasure right was not yet in force at the study's cut-off and the Supreme Court had not finally settled the treatment of online judicial records. The Delhi High Court's 2026 distinction among preservation, masking, and name-based de-indexing offers a less restrictive remedial framework, although its authority remains subject to appellate clarification. The article proposes a remedy ladder and a structured proportionality test for Indian courts, designed to preserve authoritative judicial records while reducing disproportionate name-based exposure.

1. INTRODUCTION

Digital networks have transformed the practical meaning of memory. Information that once became difficult to locate over time can now be retrieved within seconds through a name-based search. Even when the underlying material is accurate and was lawfully published, persistent prominence can affect employment, housing, immigration, personal relationships, and social rehabilitation. The right to be forgotten should therefore not be understood simply as a power to erase facts. It raises a narrower question about the continuing accessibility, context, and ranking of personal information [1–5].

Platform-mediated memory and automated information retrieval intensify the need to govern algorithmic agents that mediate access to personal data and public records [6, 7].

The label “right to be forgotten” covers several legally distinct remedies. Erasure requires a controller to delete personal data within its control when a legal ground applies, subject to retention duties and other statutory exceptions. De-indexing, also called de-referencing or delisting, removes a specified link from results returned for a name-based query but leaves the source page unchanged and accessible through other queries or its direct address. Masking or anonymisation suppresses identifying details in a public-facing copy while an unredacted authoritative version may be retained. Takedown removes the underlying

publication, whereas sealing or access restriction limits who may consult the record. These remedies impose different burdens on privacy, expression, historical accuracy, and institutional transparency; treating them as interchangeable obscures the proportionality analysis [2, 8–10].

The competing interests are substantial. Privacy protects dignity, autonomy, reputation, and a person's capacity to develop without being permanently reduced to a past event. Freedom of expression protects journalists, publishers, researchers, and members of the public who impart or receive truthful information. Open justice also has an institutional dimension: public judgments promote accountability, consistent precedent, legal research, and confidence in courts. An overbroad removal order may protect one claimant while weakening public discourse or transferring difficult constitutional choices to private intermediaries [11–16].

Legal systems answer this conflict differently. European Union law places data protection within a fundamental-rights framework and recognises qualified erasure and de-referencing subject to express exceptions. United States doctrine gives unusually strong protection to truthful information lawfully obtained from public records and has not created a general right to suppress such information merely because time has passed. India combines a constitutional right to privacy, an enacted but only partly commenced personal-data statute, and a strong tradition of open justice; its courts have nevertheless taken differing approaches to online judgments. The uncertainty is especially significant for acquittals, quashed criminal proceedings, intimate family disputes, and judgments indexed by search engines and legal databases [10, 17–21].

This article asks how the European Union, the United States, and India balance informational privacy against freedom of information and open justice, and which remedial design best fits India. It identifies the controlling legal principles in each jurisdiction, examines the treatment of elapsed time, public records, and search-engine amplification, and develops a model that preserves authoritative judicial records while reducing disproportionate name-based exposure. To make the proposed Indian approach clear from the outset, Section 3.4.4 sets out a six-stage test: verify status and accuracy; classify the source; assess the claimant's public role; identify continuing public interest; evaluate actual harm and context; and select the least restrictive effective remedy with appropriate limits and review.

2. MATERIALS AND METHODS

This study uses qualitative, comparative, and doctrinal legal research. It does not measure public attitudes or platform-compliance rates. Instead, it examines how authoritative legal texts define the relevant rights and exceptions, allocate decision-making authority, and determine the available remedies. The comparison is functional: each jurisdiction is assessed against the recurring claim that the continued online accessibility of personal information that was once lawfully published or publicly available should be limited.

2.1 Source Selection and Temporal Scope

Primary sources were selected for their authority and direct relevance. The European materials comprise the Charter of Fundamental Rights, the General Data Protection Regulation (GDPR), European Data Protection Board guidance, and leading decisions of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) [8–9, 11, 19, 22–24]. The United States analysis draws on Supreme Court public-record cases, California decisions, federal appellate authority, and the California consumer-deletion statute effective at the cut-off [17, 25–29]. The Indian analysis relies on constitutional decisions, the Digital Personal Data Protection Act, the 2025 commencement notification and Rules, and decisions concerning online judgments and name-based searchability [10, 13, 16, 20–21, 30–36].

The legal cut-off is 19 July 2026. This date matters because the Delhi High Court delivered a detailed right-to-be-forgotten judgment on 29 May 2026, while the Supreme Court proceedings concerning the Madras High Court's redaction directions had not produced a final merits decision in the primary materials located by the cut-off. The article therefore distinguishes enacted provisions from provisions actually in force, final judgments from interim orders, and binding holdings from persuasive High Court reasoning [10, 31–33].

2.2 Analytical Framework

Each jurisdiction was analysed across seven dimensions: the legal source of the asserted right; the nature and accuracy of the information; the identity and public role of the claimant; the persistence of public interest; the effect of time and procedural finality; the remedy granted; and the territorial or institutional

scope of the order. Particular attention was paid to whether the decision separated preservation of the source from its algorithmic discoverability.

The method has two limitations. First, the expression “right to be forgotten” describes several causes of action and remedies rather than a single, globally uniform rule. Second, Indian High Court decisions may be appealed, distinguished, or superseded. The comparative categories are therefore used as explanatory tools, not as a claim that any of the three systems is internally homogeneous.

3. RESULTS AND DISCUSSION

3.1 European Union: A Rights-Based Model of Erasure and De-Referencing

The European model begins from the premise that privacy and personal-data protection are fundamental rights, while freedom of expression and information are equally protected interests that must be reconciled rather than treated as secondary [11–12, 19]. This framework explains why European law may require de-referencing of accurate information without requiring deletion of the original publication.

3.1.1 *Google Spain and the Separation of Source from Search*

A Google search for Mario Costeja González’s name returned links to an old newspaper notice concerning attachment proceedings and a property auction. The CJEU held that a search-engine operator processes personal data and acts as a controller in relation to its search results. The operator could therefore be required to remove links returned by a person’s name where the information had become inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of processing [9].

The decision’s most enduring contribution is remedial. The CJEU did not require the newspaper to erase its original notice. It addressed instead the search engine’s aggregation and presentation of dispersed information. A source may remain lawful and available in an archive while its appearance in an ordinary name search is limited. This separation recognises the distinct privacy harm created when search engines collect, rank, and associate personal information at scale, and it reflects the idea of practical obscurity [3, 9, 12, 15].

Google Spain did not establish automatic removal. The public’s interest may prevail where the person plays a role in public life or the information remains relevant to public debate. The judgment nevertheless shifted the inquiry from the original source’s lawfulness to the proportionality of continued name-based indexing. That shift places search intermediaries in a difficult position because they make initial rights-balancing decisions subject to regulatory and judicial review [8–9, 12].

3.1.2 *Article 17 GDPR and Express Safeguards for Expression*

Article 17 GDPR codifies a qualified right to erasure. Relevant grounds include that data is no longer necessary for the original purpose, consent has been withdrawn and no other legal ground exists, the data subject successfully objects, the processing is unlawful, or erasure is required by law. Article 17(3) preserves processing needed for freedom of expression and information, compliance with a legal obligation or exercise of official authority, public-health purposes, archiving and research in the public interest, and the establishment, exercise, or defence of legal claims. Article 85 separately requires Member States to reconcile data protection with journalistic, academic, artistic, and literary expression [8, 19].

The resulting structure is more qualified than the phrase “right to be forgotten” sometimes suggests. The GDPR creates an enforceable right but places competing interests within the same legal instrument. Accuracy, purpose, elapsed time, the claimant’s role, and the character of the source remain relevant. A historical commercial notice, a judicial decision, a press archive, and current evidence of official misconduct cannot be assessed in the same way [2, 8, 18–19, 37].

3.1.3 *Territorial Scope: Google v. CNIL*

Google v. CNIL asked whether an accepted de-referencing request had to be implemented on every version of a search engine worldwide. The CJEU held that EU law did not, as a general rule, require global de-referencing. The operator had to de-reference results on Member State versions and adopt measures that effectively prevented, or at least seriously discouraged, users in the European Union from accessing the links through non-EU versions [22].

The territorial limit reflects both enforceability and respect for divergent constitutional traditions. A worldwide order would protect the claimant more completely but could export one jurisdiction’s balance between privacy and speech to users elsewhere. Geo-limited relief can be circumvented, yet global relief

creates conflicts of law and comity. Territorial scope is therefore part of the proportionality analysis, not merely a technical implementation question [22].

3.1.4 Media Archives: *Hurbain and M.L. and W.W.*

The ECtHR has addressed the more intrusive remedy of altering a publisher's own archive. In *Hurbain v. Belgium*, the Grand Chamber held that a Belgian order requiring the publisher of *Le Soir* to anonymise the online archive of an article about a fatal road accident did not violate Article 10. The Court relied on the time elapsed, the individual's rehabilitation, the absence of a continuing public interest in his name, and the limited nature of anonymisation compared with deletion [23, 37].

M.L. and W.W. v. Germany reached the opposite result on different facts. Two men convicted of a widely reported murder sought anonymisation of online press reports after their release. The ECtHR emphasised the seriousness and continuing public interest of the case, the applicants' own renewed contact with the media, and the potential burden on press archives. It held that the domestic courts' refusal to require anonymisation did not violate Article 8 [24, 37].

Together, these decisions do not impose an expiry date on truthful news. They require a contextual assessment of the individual's role, the subject matter, elapsed time, continuing contribution to public debate, and the intrusiveness of the proposed remedy. European law protects privacy without treating historical accuracy or archive integrity as irrelevant [5, 23–24, 37].

3.2 United States: Strong Protection for Truthful Public Information

The United States has no single federal analogue to Article 17 GDPR. The First Amendment, especially where information was lawfully obtained and drawn from official records, is a major barrier to a general right to suppress truthful information. Privacy remedies exist, but they operate within a speech-protective constitutional framework [14–15, 17, 26].

3.2.1 From Rehabilitative Privacy to the Public-Records Doctrine

Melvin v. Reid is an early example of rehabilitative privacy. A California appellate court permitted a claim arising from a film's use of the real name of a woman who had been prosecuted and acquitted years earlier and had since rebuilt her life. The decision linked privacy to the ability to live without unnecessary attacks on reputation after reform [29]. Its historical importance lies partly in the contrast with later constitutional doctrine, which gives far greater protection to truthful information derived from public records.

In *Cox Broadcasting Corp. v. Cohn*, the United States Supreme Court held that a State could not impose civil liability on a broadcaster for accurately reporting a rape victim's name obtained from a publicly available court record. The Court stressed the special protection afforded to truthful reports of official proceedings and the democratic importance of public records [17].

Florida Star v. B.J.F. extended this protection to a newspaper that published a victim's name obtained from a government-released police report. The Court did not hold that privacy can never justify liability, but required a state interest of the highest order and a narrowly tailored rule before truthful, lawfully obtained information could be punished [26].

In *Gates v. Discovery Communications, Inc.*, the California Supreme Court applied these principles to an old criminal record and rejected the argument that elapsed time alone transformed truthful reporting into an actionable invasion of privacy. Because the report concerned an official record, First Amendment interests defeated a broad rehabilitative-privacy claim [28]. Time therefore has less independent legal force in this setting than it often has in European doctrine.

3.2.2 Search Engines, Injunctions, and Narrow Consumer Deletion Rights

Federal appellate authority also illustrates judicial caution toward injunctions removing online content. *Garcia v. Google* was a copyright case, not a right-to-be-forgotten decision. The En banc Ninth Circuit vacated an injunction requiring removal of a video and emphasised the exceptional nature of prior restraints and the need to account for the speech interests of others [27]. The case does not answer whether a narrowly designed privacy remedy could ever be valid, but it demonstrates the demanding standard applied to orders that restrict online expression.

California consumer law provides a narrower right to delete personal information collected by a covered business. California Civil Code section 1798.105 requires deletion in specified circumstances but recognises exceptions, including compliance with legal obligations, security, and the exercise of free-speech rights. The statutory definition of personal information excludes publicly available information and lawfully obtained, truthful information that is a matter of public concern [25]. These provisions regulate

commercial data practices; they do not create a general authority to de-index truthful judicial decisions or historical reporting.

The United States position should therefore be stated with care. Individuals may obtain relief through sealing or expungement statutes, privacy torts, defamation law, contractual rights, consumer-deletion rights, or voluntary platform policies. What is generally absent is a broad legal entitlement to suppress truthful information found in public records merely because it is old or damaging to reputation. The distinction between unlawful disclosure of genuinely private material and accurate reporting of an official record remains central [14–15, 17, 26].

3.3 India: Constitutional Privacy, Open Justice, and an Unsettled Remedy

India occupies a more fluid legal position. Privacy is constitutionally protected, and Parliament has enacted a personal-data framework. At the same time, Article 19(1)(a), open courts, publicly accessible judgments, legal research, and institutional accountability protect access to judicial information [13, 16, 21]. The principal unresolved question is not whether privacy matters, but when it justifies reducing the digital visibility of a lawfully public record.

3.3.1 *Puttaswamy and Early High Court Approaches*

Justice K.S. Puttaswamy (Retd.) v. Union of India unanimously recognised privacy as a fundamental right under Part III of the Constitution. The opinions identified informational privacy, dignity, autonomy, and control over personal data as constitutional interests. They also made clear that privacy is not absolute and that restrictions must satisfy requirements of legality, legitimate aim, and proportionality [21]. The judgment supplies the constitutional foundation for later right-to-be-forgotten claims, but it did not establish a general procedure for removing or de-indexing judgments.

Before Puttaswamy, the Gujarat High Court in *Dharamraj Bhanushankar Dave v. State of Gujarat* refused a request to prevent online publication of an acquittal judgment. It stressed the High Court's status as a court of record and found no legal right requiring removal of the judgment from the internet [30]. The decision reflects the traditional presumption that lawfully delivered judgments are public records.

Post-Puttaswamy decisions did not follow a single path. In *Jorawer Singh Mundy v. Union of India*, the Delhi High Court granted interim protection to an acquitted person who alleged employment harm. Pending final adjudication, it directed the named search engines to remove the judgment from search results and directed Indian Kanoon to block access through external search engines [34]. In *Vysakh K.G. v. Union of India*, the Kerala High Court rejected a blanket right to prevent publication of lawfully delivered judgments, while accepting that courts may grant contextual de-indexing or erasure relief in appropriate cases and that statutory confidentiality rules govern family, matrimonial, custody, and adoption matters [36].

3.3.2 *The Digital Personal Data Protection Framework*

Section 12 of the Digital Personal Data Protection Act, 2023 creates, upon commencement, rights to correction, completion, updating, and erasure of personal data. On a valid erasure request, a Data Fiduciary must erase the data unless retention is necessary for the specified purpose or compliance with law. Section 17 contains relevant exemptions for processing needed to enforce legal rights or claims and for judicial, quasi-judicial, regulatory, or supervisory functions [20]. These provisions concern controller-held personal data; they do not by themselves prescribe whether a constitutional court should alter a judgment or order a search engine to de-index it.

The commencement position is essential. The Central Government's G.S.R. 843(E), dated 13 November 2025, brought selected definitional and institutional provisions of the Act into force immediately but scheduled sections 3–17, including section 12, to commence eighteen months after publication [31]. The Digital Personal Data Protection Rules, 2025, notified the same day as G.S.R. 846(E), also use staggered commencement: Rules 1, 2, and 17–21 commenced on publication; Rule 4 was deferred for one year; and Rules 3, 5–16, 22, and 23 were deferred for eighteen months [32]. Rule 8 was therefore not in force at the 19 July 2026 cut-off. In any event, Rule 8 provides at least 48 hours' prior notice before specified inactivity-based erasure, not 30 days [32].

Accordingly, the Act had enacted a statutory erasure right, but that right was not yet operational at the study's cut-off. It would be inaccurate to treat the entire DPDP framework as already in force or to present Rule 8 as the governing procedure for online judgments. Judicial records, legal claims, statutory retention, and the constitutional role of courts require a distinct proportionality analysis even after the data-protection provisions commence [10, 20, 31–32, 36].

3.3.3 *Karthick Theodore and Supreme Court Intervention*

In *Karthick Theodore v. Registrar General, Madras High Court*, a Division Bench directed the Registry to redact the appellant's name and identifying details from an acquittal judgment and to replace the publicly accessible online version with the redacted copy. The Court emphasised the continuing harm caused by digital association with serious allegations and located the claimed right within Article 21 privacy [35].

On 24 July 2024, the Supreme Court issued notice in *Ikanoon Software Development Pvt. Ltd. v. Karthick Theodore*, tagged the matter with *Alka Malhotra v. Union of India*, and stayed the directions in the Madras High Court judgment [33]. The order was interim, not a final determination of the constitutional issue. No final Supreme Court merits ruling was located in the primary materials available by 19 July 2026; the Madras directions therefore cannot be treated as settled national law.

3.3.4 *Laksh Vir Singh Yadav: Preservation, De-Indexing, and Masking*

The most comprehensive Indian treatment available at the cut-off is *Laksh Vir Singh Yadav v. Union of India*, decided by the Delhi High Court on 29 May 2026. Addressing a group of petitions, the Court treated the right to be forgotten as an aspect of informational privacy under Article 21 but rejected the idea that it requires wholesale destruction of judicial records. It distinguished the court's preservation of an authoritative judgment from that judgment's discoverability through a person's name on a search engine or legal database [10].

The judgment separated two principal remedies. De-indexing prevents a specified link from appearing in a name-based search while leaving the record available through neutral identifiers such as case number, citation, court, or date. Masking replaces names and personal identifiers in the publicly accessible copy while the court retains an unredacted internal record. The Court considered the originating court ordinarily best placed to decide masking because it controls its registry and can protect the integrity of the authoritative record [10].

Relief was not automatic. The Court considered the outcome and finality of proceedings, the claimant's public role, the seriousness and public character of the conduct, the continuing relevance of the information, actual harm, and the availability of a narrower remedy. Acquittal, discharge, mistaken identity, or a concluded intimate dispute could weigh in favour of relief. A public figure's attempt to suppress public conduct, serious convictions, ongoing proceedings, or a continuing public-safety or accountability interest could weigh against it [10].

Where relief was granted, the Court made URL-specific directions to the named search engines and database and directed the Ministry of Electronics and Information Technology to communicate the judgment to intermediaries operating within India [10]. This approach reduces evasion of a single-platform order but should not be described as a settled rule requiring worldwide de-indexing. Compared with *Google v. CNIL*, it leaves significant questions about territorial reach, comity, and compliance by foreign providers [10, 22]. The judgment is therefore an important framework, not a final Supreme Court resolution of Indian law.

3.4 Comparative Synthesis

The comparison shows that the central dispute is not simply whether privacy or speech is more important. The jurisdictions differ in their treatment of public-record status, elapsed time, search intermediaries, and alteration of authoritative records. Table 1 summarises the principal features of the three models.

Table 1. Comparative features of the right to be forgotten in the European Union, the United States, and India.

Dimension	European Union	United States	India
Primary basis	Charter rights and GDPR	First Amendment doctrine; sectoral and state privacy law	Article 21 privacy; Article 19(1)(a); enacted DPDP Act; case law
General orientation	Qualified right to erasure and de-referencing	No general right to suppress truthful public-record information	Constitutional privacy recognised; statutory erasure provisions not yet commenced at the cut-off; remedies remain contested
Typical remedy	Erasure, de-referencing, or anonymisation	Business-held data deletion, sealing, tort, or platform relief	Targeted de-indexing or masking; authoritative court record preserved
Judicial records	Privacy balanced with expression, archives, and public interest	Strong protection for accurate reports derived	Open justice is presumptive; privacy may

Dimension	European Union	United States	India
		from public records	justify targeted relief
Role of time	Can reduce continuing relevance	Usually insufficient by itself to defeat public-record protection	Relevant but not determinative
Territorial approach	Generally EU-wide, with effective geo-measures	Domestic constitutional limits resist broad speech restrictions	2026 Delhi High Court directions reached specified intermediaries operating within India; final scope remains unsettled
Current legal status	Mature statutory and judicial framework	Stable rejection of a broad right; limited consumer deletion	Developing; DPDP erasure provisions await commencement and a Supreme Court merit ruling

3.4.1 Remedy Design: A Ladder Rather Than a Binary Choice

European and recent Indian decisions show why a binary choice between full publication and complete deletion is inadequate. The source may retain legal value even when unrestricted retrieval by name is disproportionate. Remedies can be arranged by increasing interference: contextual correction or linking to the final outcome; reduced ranking; name-based de-indexing; masking of identifiers in the public copy; access restriction or sealing; and, as a last resort, takedown or erasure of information that is unlawfully published or held [9–10, 23].

This remedy ladder answers the concern that a right to be forgotten rewrites the past. De-indexing and masking can preserve legal reasoning, citations, chronology, and institutional accountability while reducing the routine association of a private person with outdated allegations. The approach reflects Google Spain’s separation of source from search, the narrow anonymisation upheld in Hurbain, and the preservation principle developed in Laksh Vir Singh Yadav [5, 9–10, 23].

3.4.2 Time, Finality, and Continuing Public Interest

Time matters, but it is not decisive. An old minor charge ending in acquittal or closure may have little present value, whereas a judgment concerning corruption, serious violence, public office, professional misconduct, or systemic wrongdoing may remain important. Procedural finality also matters: courts should be cautious while investigation, trial, appeal, or review continues. Once proceedings are final, online presentation should reflect the legal outcome accurately; search results that foreground an accusation while obscuring an acquittal may create a misleading context even when each source is factually accurate [10, 23–24, 28].

The jurisdictions give elapsed time different weight. Gates treats the official-record status of information as strongly resistant to decay, while Hurbain allows time and rehabilitation to shift the proportionality balance. Indian law has not selected a single rule. A principled Indian test should consider time within a broader inquiry into present relevance, public purpose, gravity, and the final judicial outcome [10, 23, 28].

3.4.3 Institutional Competence and Procedural Safeguards

Search engines can process requests quickly but should not be left to make unreviewable judgments about public interest. Courts understand procedural history and can distinguish acquittal, discharge, quashing, compromise, closure, and conviction. Court registries control official copies, while publishers and databases hold independent expression and research interests. A legitimate process should therefore provide notice, an opportunity to respond, reasoned decisions, and review [10, 16, 36].

When relief concerns a judicial record, the originating court should ordinarily decide whether masking or access restriction is justified. A consequential de-indexing order may then be implemented by a search engine or database. Direct deletion from a commercial service may be appropriate for unlawfully held personal data, but deletion of a court source should be exceptional. This allocation reduces inconsistent orders and protects the completeness of the authoritative record [8, 10, 16].

3.4.4 A Structured Test for India

A future Indian framework should proceed in six stages. First, verify the claimant’s identity, the accuracy of the material, and the final legal status of the matter. Second, classify the source as a private database entry, news report, search result, or judicial record. Third, identify the claimant’s role: private person, public official, professional fiduciary, or public figure. Fourth, assess continuing public interest by

considering seriousness, recency, public safety, institutional accountability, historical value, and the claimant's later conduct. Fifth, evaluate the demonstrated harm of name-based accessibility and whether the legal outcome is presented in context. Sixth, choose the least restrictive effective remedy and define its duration, search terms, territorial scope, and review mechanism.

Categorical bars should be narrow and tied to genuine public interest rather than moral disapproval alone. Acquittal should carry substantial weight but should not produce automatic relief, because acquittals arise in different factual and procedural settings. The court should explain why continued name-based visibility either contributes to public understanding or imposes a disproportionate burden unrelated to a present public interest [10].

This model draws on Puttaswamy's proportionality requirement, the GDPR's express safeguards, the public-record concerns in *Cox and Vysakh*, and the remedial distinctions in *Laksh Vir Singh Yadav* [10, 17, 19, 21, 36]. It presumes neither permanent exposure nor automatic erasure.

4. CONCLUSION

The right to be forgotten is best understood as a family of remedies directed to the proportionality of continued retention, publication, and discoverability of personal information. The European Union recognises qualified erasure and de-referencing within a fundamental-rights framework that protects expression, journalism, archives, research, legal claims, and continuing public interest. The United States protects truthful public-record information more strongly and offers narrower consumer-deletion and privacy remedies. India has constitutional and statutory foundations for informational privacy, but the treatment of searchable judicial records remains unsettled.

For India, deleting legal history is neither necessary nor generally desirable. A more proportionate approach separates preservation from discoverability. Contextual correction, name-based de-indexing, and masking can protect private persons after acquittal, discharge, quashing, or the resolution of an intimate dispute without destroying the authoritative record used by courts, lawyers, researchers, and the public. Relief should follow a structured proportionality test, be ordered by the institution best placed to protect the record, and remain subject to notice, reasons, defined scope, and review.

The principal limitation of this study is that Indian appellate law and implementation of the Digital Personal Data Protection framework are still developing. Future research should examine implementation data, platform compliance, variation among High Court orders, and whether artificial-intelligence search and summarisation tools recreate name-based exposure after conventional links have been de-indexed.

REFERENCES

- [1] Ambrose, M. L. (2013). It's about time: Privacy, information lifecycles, and the right to be forgotten. *Stanford Technology Law Review*, 16, 369–422.
- [2] de Terwangne, C. (2012). Internet privacy and the right to be forgotten/right to oblivion. *Revista de Internet, Derecho y Política*, 13, 109–121. <https://doi.org/10.7238/idp.v0i13.1400>
- [3] Hartzog, W., & Stutzman, F. (2013). The case for online obscurity. *California Law Review*, 101(1), 1–49. https://scholarship.law.bu.edu/faculty_scholarship/3024/
- [4] Jones, M. L. (2016). *Ctrl+Z: The right to be forgotten*. New York University Press.
- [5] Pressly, L. (2024). The right to be forgotten and the value of an open future. *Ethics*, 135(1), 65–87. <https://doi.org/10.1086/731431>
- [6] Pandey, J. K., & Kumar, R. (2025). Governing the algorithmic agent: Confronting overt and covert challenges to justice and the future of work. *International Journal of Law Management & Humanities*, 8(4), 1974–1984. <https://doi.org/10.1000/IJLMH.1110648>
- [7] Veeraiah, V., Naga Ganesh, C., Bhavagna, L., Pradeep, S., Pandey, J. K., & Gupta, A. (2026). Digital transformation and leadership: Managing transition to a tech-driven business with big data. In *Proceedings of the NIELIT International Conference on Communication*.
- [8] European Data Protection Board. (2020). Guidelines 5/2019 on the criteria of the right to be forgotten in the search engines cases under the GDPR (Part 1) (Version 2.0). https://www.edpb.europa.eu/documents/guideline/guidelines-52019-on-the-criteria-of-the-right-to-be-forgotten-in-the-search_en
- [9] *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317 (Court of Justice of the European Union, May 13, 2014).

- [10] Laksh Vir Singh Yadav v. Union of India, W.P. (C) No. 1021 of 2016 and connected matters (Delhi High Court, May 29, 2026).
- [11] European Union. (2012). Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.
- [12] Post, R. C. (2018). Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, 67(5), 981–1072. <https://scholarship.law.duke.edu/dlj/vol67/iss5/2/>
- [13] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (Supreme Court of India, October 7, 1994).
- [14] Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online*, 64, 88–92. <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>
- [15] Solove, D. J. (2002). Access and aggregation: Public records, privacy, and the Constitution. *Minnesota Law Review*, 86(6), 1137–1218. <https://doi.org/10.24926/265535.1994>
- [16] Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 639 (Supreme Court of India, September 26, 2018).
- [17] Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).
- [18] Erdos, D., & Garstka, K. (2020). The ‘right to be forgotten’ online within G20 statutory data protection frameworks. *International Data Privacy Law*, 10(4), 294–313. <https://doi.org/10.1093/idpl/ipaa012>
- [19] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- [20] Government of India. (2023). Digital Personal Data Protection Act, 2023, No. 22 of 2023.
- [21] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India, August 24, 2017).
- [22] Google LLC v. Commission nationale de l’informatique et des libertés (CNIL), Case C-507/17, ECLI:EU:C:2019:772 (Court of Justice of the European Union, September 24, 2019).
- [23] Hurbain v. Belgium [GC], App. No. 57292/16 (European Court of Human Rights, July 4, 2023).
- [24] M.L. and W.W. v. Germany, App. Nos. 60798/10 and 65599/10 (European Court of Human Rights, June 28, 2018).
- [25] California Privacy Protection Agency. (2026). California Consumer Privacy Act of 2018, as amended, Cal. Civ. Code §§ 1798.100–1798.199.100 (effective January 1, 2026). https://coppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf
- [26] Florida Star v. B.J.F., 491 U.S. 524 (1989).
- [27] Garcia v. Google, Inc., 786 F.3d 733 (9th Cir. 2015) (en banc).
- [28] Gates v. Discovery Communications, Inc., 34 Cal. 4th 679, 101 P.3d 552 (2004).
- [29] Melvin v. Reid, 112 Cal. App. 285, 297 P. 91 (1931).
- [30] Dharamraj Bhanushankar Dave v. State of Gujarat, Special Civil Application No. 1854 of 2015 (Gujarat High Court, January 19, 2017).
- [31] Government of India. (2025a). Notification bringing provisions of the Digital Personal Data Protection Act, 2023 into force, G.S.R. 843(E), Gazette of India, Extraordinary, Part II, Section 3(i) (November 13, 2025). <https://www.meity.gov.in/static/uploads/2025/11/c56caee6c383460ca69577428d36828b.pdf>
- [32] Government of India. (2025b). Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, Section 3(i) (November 13, 2025). <https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf>
- [33] Ikanoon Software Development Pvt. Ltd. v. Karthick Theodore, S.L.P. (C) No. 15311 of 2024 (Supreme Court of India, order dated July 24, 2024).
- [34] Jorawar Singh Mundy @ Jorawar Singh Mundy v. Union of India, W.P. (C) No. 3918 of 2021, 2021 SCC OnLine Del 2306 (Delhi High Court, interim order dated April 12, 2021).
- [35] Karthick Theodore v. Registrar General, Madras High Court, W.A. (MD) No. 1901 of 2021, 2024 SCC OnLine Mad 6529 (Madras High Court, February 27, 2024).
- [36] Vysakh K.G. v. Union of India, 2022 SCC OnLine Ker 7337 (Kerala High Court, December 22, 2022).
- [37] Anderez Belategi, M. (2024). The right to be forgotten concerning the criminal past: Developments in the case law of the European Court of Human Rights with particular reference to the anonymisation of digital press archives. *Oñati Socio-Legal Series*, 14(6), 1639–1669. <https://doi.org/10.35295/osls.iisl.1938>