

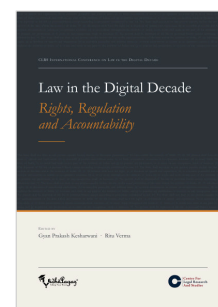
CHAPTER 20

Right to be Forgotten vs. Right to Information: Finding the Digital Balance

Gargi Bhatt

in *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma (VidhiAagaz 2026), pp. 239–252

DOI <https://doi.org/10.63108/VAB.LDD.1.20>



CITATIONS

BLUEBOOK (21ST ED.)

Gargi Bhatt, *Right to be Forgotten vs. Right to Information: Finding the Digital Balance*, in *LAW IN THE DIGITAL DECADE: RIGHTS, REGULATION AND ACCOUNTABILITY* 239 (Gyan Prakash Kesharwani & Ritu Verma eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Gargi Bhatt, 'Right to be Forgotten vs. Right to Information: Finding the Digital Balance' in Gyan Prakash Kesharwani and Ritu Verma (eds), *Law in the Digital Decade: Rights, Regulation and Accountability* (VidhiAagaz 2026) 239.

CHICAGO (17TH ED.)

Bhatt, Gargi. "Right to be Forgotten vs. Right to Information: Finding the Digital Balance." In *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma, 239–252. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.1.20>.

APA (7TH ED.)

Bhatt, G. (2026). Right to be forgotten vs. right to information: Finding the digital balance. In G. P. Kesharwani & R. Verma (Eds.), *Law in the digital decade: Rights, regulation and accountability* (pp. 239–252). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.1.20>

SOURCE

<https://doi.org/10.63108/VAB.LDD.1.20>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 20

Right to be Forgotten vs. Right to Information: Finding the Digital Balance

DR. GARGI BHATT*

The rapid expansion of digital platforms has fundamentally changed the way information is created, accessed, stored and circulated. Information once published online can remain searchable and accessible for years, often long after its relevance has diminished. In this context, the emerging Right to be Forgotten (RTBF) seeks to protect individuals from the continuing digital consequences of outdated, irrelevant or disproportionately harmful personal information. At the same time, the Right to Information (RTI) serves as an important instrument of transparency, accountability and informed democratic participation. The increasing overlap between these two rights raises a difficult question: how can individual privacy and dignity be protected without undermining society's legitimate interest in accessing information?

This paper examines the evolving relationship between the RTBF and the right to information, particularly within the Indian constitutional and legal framework. It explores the tension between privacy, reputation and informational autonomy on one hand, and freedom of expression, transparency and public interest on the other. The paper also considers the challenges posed by search engines, social media platforms and the permanence of digital records, where removing information from one platform may not necessarily erase its wider digital footprint.

The study argues that neither right should be treated as absolute. A balanced approach requires contextual assessment based on factors such as the nature and sensitivity of the information. The paper concludes by proposing the need for clearer legal standards and transparent mechanisms that can reconcile privacy with the democratic value of access to information in an increasingly digital society.

Keywords: Right to be Forgotten; Right to Information; Privacy; Digital Rights; Data Protection; Public Interest

1 INTRODUCTION

The digital environment has altered the relationship between information, time and identity. In the analogue world, information about an individual was dispersed across archives, newspapers, registries and personal recollection. Its practical accessibility was limited by geography, cost, institutional fragmentation and the ordinary processes of human forgetting. The internet has displaced these limitations. Information can now be copied indefinitely, indexed globally, retrieved instantaneously and recombined with other data to construct enduring profiles of individuals. The past is no longer merely remembered; it is continuously searchable.

This transformation has generated a conflict between two important but potentially competing interests. On one side lies the right to be forgotten, understood broadly as an individual's ability to seek the removal, erasure, de-indexing, anonymization or reduced accessibility of personal information. It is

* Assistant Professor & Head, Training & Placement Office at DME Law School, Delhi Metropolitan Education, Noida, Uttar Pradesh, India.

connected with privacy, dignity, autonomy, reputation and the possibility of personal development or social reintegration. On the other side lies the right to information, including freedom of expression, freedom of the press, the public's right to know and access to matters of legitimate public concern. Democratic societies require the circulation of information, including information that may be uncomfortable, embarrassing or critical of powerful individuals.

The conflict is not limited to obviously false or unlawful material. It frequently concerns information that was lawfully published, substantially accurate and once newsworthy, but which has become disproportionately harmful because search engines make it permanently prominent. A criminal conviction, bankruptcy, family dispute, professional disciplinary proceeding or youthful indiscretion may remain technically available for decades. The question is therefore not simply whether the information is true. It is whether continued, name-based prominence remains justified in light of changed circumstances.

European law has generally treated privacy and freedom of expression as rights of equal normative importance. Neither is automatically superior; the outcome depends upon the circumstances of the case.¹ The United States, by contrast, has been more resistant to a general right to be forgotten because of the First Amendment's strong protection of truthful publication and public access to information.² India occupies a developing middle position. The Supreme Court has constitutionally recognized privacy, including decisional autonomy and informational control, while the Digital Personal Data Protection Act 2023 creates a statutory framework whose relationship with freedom of expression and archival access remains unsettled.³

This chapter argues that the appropriate response is neither an absolute right to erase the past nor an unrestricted right of indefinite digital exposure. A principled, context-sensitive balance is required. That balance should distinguish between deletion and de-indexing, public and private information, public officials and ordinary individuals, current and historical relevance, truth and falsity, serious harm and ordinary embarrassment, and the interests of the data subject and those of the wider public. It should also recognize that the institutional location of decision-making matters. A system that leaves fundamental-rights adjudication primarily to search engines risks creating opaque private jurisprudence. The proper objective is therefore a framework in which individual protection is effective, public access is preserved where justified, and decisions are transparent, reviewable and proportionate.

2 CONCEPTUAL FOUNDATIONS

2.1 The Right to Be Forgotten

The expression “right to be forgotten” is rhetorically powerful but legally imprecise. It may describe several distinct remedies:

- a. Deletion of personal data from the original source;
- b. Erasure by a controller or processor;

¹ Kulk, S. & Zuiderveen Borgesius, Frederik. (2018). Privacy, freedom of expression, and the right to be forgotten in Europe. In E. Selinger, J. Polonetsky & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (pp. 301–320). Cambridge University Press. <https://doi.org/10.1017/9781316831960.018>

² Amy Gajda, (2018). *Privacy, Press, and the Right to Be Forgotten in the United States*, 93 Wash. L. Rev. 201. <https://digitalcommons.law.uw.edu/wlr/vol93/iss1/5>

³ Kaur, Gursimar, (2026). The Right to Be Forgotten in India: Balancing Privacy Rights and Freedom of Expression in the Digital Era. *Iconic Research and Engineering Journals*, 9(12), 2493–2497. <https://doi.org/10.64388/irev9i12-1719150>

- c. De-indexing of a webpage from searches based on an individual's name;
- d. Anonymization of the individual in an archival publication;
- e. Restriction of processing or reduced prominence; and
- f. Correction or contextualization of inaccurate or incomplete material.

These remedies have different effects. Deletion suppresses the source itself. De-indexing leaves the source available to those who know its location or search by other terms, but removes the ordinary name-based route to discovery. Anonymization preserves the historical record while reducing the connection between the event and the individual's present identity. Contextualization may correct the problem without suppressing access.

The modern debate emerged from older data-protection principles: purpose limitation, storage limitation, relevance, accuracy and the prohibition of processing that becomes excessive or unnecessary. The right to be forgotten is therefore not necessarily a wholly new right. It can be understood as an application of established privacy principles to a technological environment in which data persist and remain accessible long after the purpose of publication has changed.⁴

Its moral foundation is the idea that individuals require a degree of control over the presentation of their identity. Privacy is not limited to secrecy. A person may have a legitimate interest in controlling the circumstances in which information is collected, aggregated, interpreted and made salient. A public tweet, old newspaper report or court record may individually reveal little, yet become deeply intrusive when indexed, ranked and combined with other data. The central harm may arise not from the existence of information but from its perpetual accessibility and the inferences generated by its technical organization.

This is the “digital memory” problem. Digital networks eliminate the natural decay of information. An event may remain searchable without regard to time, context or the changed character of the person involved. The internet also collapses distinctions between different audiences. Information originally directed to a local readership may become globally available; an old report intended for contemporaneous consumption may become a permanent identity marker; and material that was once difficult to locate may be placed at the top of a search-results page.

The right to be forgotten should therefore be understood as a claim to temporal and contextual integrity rather than literal oblivion. It expresses the proposition that the legal significance of information may change over time. The continued processing of accurate data may become disproportionate when the information is no longer necessary for the original purpose or when its present effects are substantially different from those reasonably contemplated at the time of publication.⁵

At the same time, privacy cannot be treated as an automatic consequence of publication. Individuals may voluntarily disclose information, participate in public affairs or become subjects of legitimate public reporting. Nor does public availability eliminate all privacy interests. Scholarly analysis of public information has shown that privacy may concern control over the manner, aggregation and inference of information, rather than merely the secrecy of isolated facts.⁶ The fact that data are accessible does not conclusively answer whether their continued processing is fair.

⁴ Sartor, G. (2014). *The right to be forgotten in the draft data protection regulation*. International Data Privacy Law, 5(1), 64–72. <https://doi.org/10.1093/idpl/ipu030>

⁵ Iglezakis, I. (2014). *The right to be forgotten in the Google Spain case (Case C-131/12): A clear victory for data protection or an obstacle for the internet?* SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.2472323>

⁶ Rumbold, B., & Wilson, J. (2018). *Privacy rights and public information*. *Journal of Political Philosophy*, 27(1), 3–25. <https://doi.org/10.1111/jopp.12158>

2.2 The Right to Information and Freedom of Expression

The right to information encompasses several related interests. It protects the speaker's liberty to communicate, the media's ability to investigate and report, and the audience's interest in receiving information. In constitutional democracies, access to information also enables political accountability, informed voting, scrutiny of public institutions and the development of individual personality.

Freedom of expression protects more than agreeable or socially beneficial speech. It includes criticism, historical inquiry, investigative journalism and the communication of facts that may harm reputation. A right to information is therefore not exhausted by access to official documents or current news. Historical archives, judicial decisions, public registers and journalistic databases contribute to collective memory and democratic accountability.

The public interest is not identical to public curiosity. Information about a celebrity's private life may attract attention without contributing meaningfully to public debate. Conversely, material concerning corruption, public health, abuse of office, professional misconduct or threats to public safety may retain substantial public value even when it is old. The distinction is difficult because public interest is contextual, not reducible to the number of people interested in the information.

The relationship between privacy and information is also not necessarily zero-sum. Privacy may improve the quality of public discourse by enabling individuals to participate without fear of permanent surveillance. Conversely, excessive secrecy can undermine accountability. A constitutional order must therefore protect both the individual's capacity to develop a private life and society's ability to remember, investigate and criticize.

The underlying issue is one of institutional design. The internet does not merely host speech; it determines visibility. Search engines rank, organize and connect information. Their decisions affect the practical scope of expression even when no webpage is removed. The right to information must consequently include attention to the architecture through which information is found.

3 THE LANDMARK JURISPRUDENCE

3.1 Google Spain

The central European authority *Google Spain SL v Agencia Española de Protección de Datos*⁷, decided by the Court of Justice of the European Union in 2014, concerned a newspaper report about a property auction connected with social-security debts. The information had been lawfully published and was not alleged to be inaccurate. The claimant nevertheless argued that searching his name produced results linking him to an old financial difficulty, causing continuing harm.

The Court held that the activity of a search engine constituted processing of personal data and that the operator could be treated as a data controller in respect of that processing. It further held that, under the then-applicable Data Protection Directive, an individual could in appropriate circumstances request the removal of links from results displayed following a search of the person's name. The ruling did not require deletion of the source material from the newspaper's archive. It concerned the association generated by the search engine between the individual's name and the underlying information.

⁷ *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317 (13 May 2014)

The judgment's significance lies in its recognition that search engines alter the practical meaning of publication. The newspaper's archive and the search-results page were not treated as functionally equivalent. Search engines made it possible to obtain a comprehensive profile of an individual through a single name query. The Court consequently focused not only on the legality of the original publication but also on the continuing effects of automated indexing and name-based accessibility.

The Court adopted a balancing approach. The data subject's interests in privacy and protection of personal data had to be weighed against the interests of internet users and the public in accessing information. Relevant considerations included the nature of the information, its sensitivity, the role played by the individual in public life, the passage of time, the accuracy and continuing relevance of the material, and the contribution of the information to a matter of public interest.⁸

Importantly, the Court did not create an unconditional entitlement to removal. It contemplated circumstances in which the public interest in access would prevail. The identity and social role of the data subject mattered. A public official or influential businessperson could reasonably be subject to greater informational scrutiny than a private individual. The age of the information mattered because the public significance of an event may diminish, although time alone does not extinguish public interest. Accuracy mattered because inaccurate or misleading material presents a stronger case for correction or removal. The nature of the harm also mattered, particularly where the result created a seriously distorted or disproportionate picture of the person.

Google Spain nevertheless attracted substantial criticism. First, critics argued that it transformed data-protection law into a mechanism for controlling truthful speech. Secondly, the judgment imposed the initial balancing responsibility on search engines, private corporations whose principal expertise is technological and commercial rather than constitutional adjudication. Thirdly, publishers might not receive effective notice or participation when a link is de-indexed. Fourthly, the process could favour wealthy or powerful applicants able to submit sophisticated requests or threaten litigation. The result might be censorship without a conventional judicial order.

The concern is not merely theoretical. The removal of a link does not always suppress information completely, but it changes visibility. Search engines are important gateways to knowledge, and de-indexing can render information practically inaccessible to ordinary users. The decision therefore creates a form of indirect speech restriction while formally preserving the source publication.

3.2 Article 17 of the GDPR

Article 17 of the General Data Protection Regulation codifies a "right to erasure", also described as the right to be forgotten. It provides for erasure in several circumstances, including where data are no longer necessary for the purposes for which they were collected or processed, where consent is withdrawn and no other legal ground exists, where the individual objects to processing in specified circumstances, or where processing has been unlawful.

The right is not absolute. Article 17 contains express exceptions for freedom of expression and information, compliance with legal obligations, public interest in public health, archiving in the public interest, scientific or historical research, statistical purposes and the establishment, exercise or defence of

⁸ Jonason, P. (2018). The Right to Be Forgotten: *The Balance between the Right to Privacy and Freedom of Expression*. *Revue Européenne de Droit Public/European Review of Public Law*, 30, 213–226

legal claims. These exceptions reveal that the GDPR does not establish a hierarchy in which privacy automatically defeats information. Rather, it creates a structured proportionality inquiry.

Article 17 also raises questions about the distinction between controllers and publishers. Where an individual requests erasure, the controller may have obligations to take reasonable steps to inform other controllers processing the data. Yet the Regulation leaves difficult questions about hosting services, journalistic archives, search engines and cross-border accessibility. The provision addresses erasure but only partially resolves the underlying issue of online publication and the allocation of responsibility among different intermediaries.⁹

The GDPR's architecture confirms that different remedies should be considered before deletion. If the problem is inaccuracy, correction may be sufficient. If the problem is excessive prominence, de-indexing or anonymization may be preferable. If the information remains necessary for archival or journalistic purposes, continued access may be justified subject to safeguards. The remedy should correspond to the harm.

3.3 The Risk of Privatized Adjudication

A major structural objection is that search engines have become the first-instance decision-makers in disputes involving fundamental rights. They receive the application, gather information, assess the competing interests, decide whether the result should remain visible and communicate the outcome to the applicant. Their decisions may be reviewed by data-protection authorities or courts, but review is usually subsequent, selective and costly.

This has been described as “private jurisprudence”. Private actors effectively develop rules governing privacy, data protection and access to information without the procedural protections ordinarily associated with constitutional adjudication.¹⁰ The problem is heightened by secrecy. Search engines may not disclose detailed reasons because of concerns about privacy, fraud, manipulation or commercial confidentiality. A person whose link is removed may not know why; a publisher may not know that the link has disappeared; and the public cannot easily assess the consistency of decisions.

The model also produces asymmetry. Search engines face legal risk if they refuse removal, but may face less immediate risk if they remove a link too readily. This can create incentives toward over-removal. The public's interest in access is diffuse and difficult to represent, whereas the applicant's complaint is concrete and legally actionable. The resulting system may systematically undervalue collective interests.

The answer is not necessarily to exclude intermediaries. A centralized court-only model may be too slow and expensive for the volume of requests. The better approach is to require reasoned decisions, meaningful notice, standardized criteria, independent review, publication of anonymized statistics and escalation of difficult cases to public authorities. Private processing can be administrative; it should not become the final, unreviewable determination of constitutional rights.

⁹ Sartor, G. (2014). *The right to be forgotten in the draft data protection regulation*. International Data Privacy Law, 5(1), 64–72. <https://doi.org/10.1093/idpl/ipu030>

¹⁰ Leiser, M. (2020). ‘Private jurisprudence’ and the right to be forgotten balancing test. Computer Law & Security Review, 39, 105458. <https://doi.org/10.1016/j.clsr.2020.105458>

4 COMPARATIVE PERSPECTIVES

4.1 Europe: The GDPR and Strasbourg

The European approach combines data-protection law under the GDPR with privacy and expression principles developed under the European Convention on Human Rights. The Convention's Article 8 protects private and family life, while Article 10 protects freedom of expression. The European Court of Human Rights has generally approached conflicts through proportionality, asking whether the interference is prescribed by law, pursues a legitimate aim and is necessary in a democratic society.

Strasbourg case law emphasizes factors such as the contribution of the publication to a debate of general interest, the notoriety of the person concerned, the subject of the report, the prior conduct of the person, the content, form and consequences of publication, and the severity of the sanction imposed. These criteria are especially important in cases concerning archives and searchability because the original publication may have been lawful while later accessibility creates a new privacy impact.

In the case of *Hurbain v Belgium*¹¹, the Grand Chamber considered the publication of an old newspaper article identifying a driver involved in a fatal road accident. The Court accepted that continued identification could seriously affect the individual's private life and professional rehabilitation. At the same time, it treated the case as involving a historical journalistic archive rather than a demand for complete deletion. Anonymisation was significant because it could reduce the continuing harm while preserving the archival record. The case illustrates the value of graduated remedies: anonymity may be more proportionate than erasure.¹²

The Strasbourg approach also places emphasis on significant harm. Mere discomfort, embarrassment or the fact that information is unflattering should not automatically justify interference with expression. The applicant should demonstrate a substantial and continuing impact, assessed in light of the nature of the information, the passage of time and the person's circumstances. This is not a requirement that harm be catastrophic, but it discourages the transformation of ordinary reputational dissatisfaction into a right of suppression.

European law therefore contains two related but not identical tendencies. The Court of Justice of the European Union's (CJEU) search-engine jurisprudence focuses on data processing and name-based accessibility. The European Court of Human Rights' (ECtHR) approach concentrates on proportionality, journalistic freedom and the consequences of the restriction. The relationship between the two bodies of law remains complex, and inconsistent standards may produce uncertainty.¹³

4.2 The United States

The United States has no general statutory right to be forgotten comparable to Article 17 GDPR. The First Amendment creates strong constitutional protection for truthful information, particularly where the information concerns public proceedings, matters of public significance or lawfully obtained facts. The

¹¹ *Hurbain v Belgium*. GC no. 57292/16. Judgment of 4 July 2023. *European Court of Human Rights Grand Chamber*. Available at <https://hudoc.echr.coe.int/eng?i=001-225814>

¹² Oganessian, T. (2022). *The right to be forgotten: The European Court of Human Rights in search of the necessary balance*. *Meždunarodnoe Pravo*, 12(1), 32–56. <https://doi.org/10.21128/2226-2059-2022-1-32-56>

¹³ Oganessian, T. (2022). *The right to be forgotten: The European Court of Human Rights in search of the necessary balance*. *Meždunarodnoe Pravo*, 12(1), 32–56. <https://doi.org/10.21128/2226-2059-2022-1-32-56>

Supreme Court has repeatedly been reluctant to permit government restrictions on truthful publication merely because disclosure causes distress or reputational injury.

The American position reflects a different constitutional culture. The presumption is that the remedy for harmful or contested speech is often more speech, correction, context or counter-speech rather than suppression. Defamation law generally distinguishes false statements from truthful but embarrassing facts, and public figures face demanding standards when seeking damages. A general right requiring search engines or publishers to remove truthful information would risk prior restraint and content-based regulation.

This does not mean that American law ignores privacy. Intrusion upon seclusion, public disclosure of private facts, appropriation, breach of confidence, contractual obligations and sector-specific data-protection laws may provide protection. The law may also recognize claims involving false light or misuse of private data. But these doctrines do not amount to a general power to require de-indexing of truthful historical information.

The American resistance is especially strong where removal would conceal information about public officials, criminal justice, political conduct or matters of public safety. It also reflects concern that private intermediaries could make decisions with public consequences while avoiding the constitutional constraints applicable to the state. Comparative scholarship accordingly describes the United States as lacking a general common-law right to be forgotten and as facing significant difficulty reconciling such a right with the First Amendment.¹⁴

Nevertheless, the contrast should not be overstated. Even in the United States, the practical design of search engines raises questions about privacy and informational power. The First Amendment does not necessarily require that every piece of information receive equal prominence forever. Voluntary platform policies, technical measures, privacy-enhancing design and narrowly tailored statutory regulation may protect individuals without authorizing broad governmental censorship.

4.3 India

India's constitutional position has evolved substantially through *Justice K.S. Puttaswamy (Retd.) v Union of India*.¹⁵ The Supreme Court recognised privacy as a constitutionally protected right grounded in dignity, liberty, autonomy and the freedoms guaranteed by Part III of the Constitution. Privacy includes bodily, decisional and informational dimensions. Although the judgment did not settle the complete content of a right to be forgotten, its reasoning provides a constitutional foundation for protecting individuals against unjustified collection, processing and dissemination of personal data.

Indian constitutional law must also account for Article 19(1)(a), which protects freedom of speech and expression, and the recognized importance of press freedom and public access to information. Privacy under Article 21 cannot operate as an automatic injunction against publication. Restrictions on expression must satisfy constitutional standards of legality, legitimate purpose, necessity and proportionality.

Indian courts have occasionally addressed requests for removal or masking of personal information, including in relation to matrimonial disputes, criminal cases and online publication of sensitive personal

¹⁴ Federico, M. (2024). *Have We Forgotten Freedom of Information? A Comparative Critical Overview of the Right to be Forgotten in Europe and the United States*. ARCA (Università Ca' Foscari Venezia).

¹⁵ *Justice K.S. Puttaswamy (Retd.) v Union of India*; (2017) 10 SCC 1

material. The judicial treatment has been developing rather than uniform. Some decisions have accepted that continued online availability may cause disproportionate harm; others have stressed the importance of open justice, court records and the public character of proceedings. The central difficulty is to determine whether a request concerns legitimate privacy, reputational discomfort, suppression of adverse history or protection against a genuine and continuing injury.

The Digital Personal Data Protection Act 2023 marks an important legislative development. It establishes duties for data fiduciaries, rights for data principals and a framework for processing digital personal data. Its relevance to the right to be forgotten arises through rights relating to erasure or correction and through the regulation of processing. Yet the statute does not simply replicate Article 17 GDPR.¹⁶ Its institutional structure, exemptions, relationship with public authorities and interaction with journalistic and constitutional freedoms require careful interpretation. The Act must be read consistently with constitutional values, particularly privacy, dignity, equality, expression and access to justice.

India should avoid adopting either an unlimited European-style removal power or an absolutist American model. Its social conditions make protection against doxxing, non-consensual intimate imagery, cyber harassment, identity theft and caste- or gender-based targeting especially important. At the same time, historical records, court judgments, investigative journalism and public accountability cannot be casually erased. The Indian framework should therefore prioritise graduated remedies and judicially reviewable standards.

5 THE SEARCH FOR A BALANCE

5.1 The Applicable Balancing Criteria

A principled balance should begin with the recognition that neither privacy nor information is presumptively dominant. The following criteria should guide decision-making.

5.1.1 *Nature and Sensitivity of the Information*

Highly sensitive personal data—medical information, sexual life, intimate images, information concerning children, psychological distress or victim status—deserve strong protection. Information relating to public functions, corporate conduct, official decisions or criminal proceedings may attract a stronger public interest. The classification is not absolute, but it establishes the starting point.

5.1.2 *Public Interest Rather Than Public Curiosity*

The decisive question should be whether access contributes to democratic accountability, public safety, historical understanding, professional integrity or informed public debate. Mere popularity, sensationalism or commercial value should carry limited weight. A person's celebrity may increase public interest, but it should not convert every aspect of private life into legitimate public information.¹⁷

¹⁶ Saurabh, Shubham. (2024). *The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age*. International Journal of Law in Changing World. 77-94. 3. 10.54934/ijlcw.v3i2.84.

¹⁷ Von Hannover v Germany. no. 59320/00. Judgment of 24 June 2004. European Court of Human Rights. Available at <https://hudoc.echr.coe.int/eng?i=001-61853>

5.1.3 *Role of the Data Subject*

Public officeholders, senior professionals exercising public trust, corporate executives and persons who deliberately place themselves at the centre of public controversy may reasonably expect greater scrutiny. Private individuals generally have stronger claims to de-indexing, especially where the information relates to an isolated event rather than a continuing public role.

5.1.4 *Passage of Time and Changed Circumstances*

Time is central but not dispositive. Old information may lose relevance, particularly where the individual has reformed, completed a sentence, settled a dispute or rebuilt a private life. Conversely, historical information may retain importance where it concerns continuing accountability, patterns of conduct, unresolved wrongdoing or public office. The legal inquiry should ask whether the information's present value justifies its present accessibility.

5.1.5 *Accuracy, Completeness and Context*

False information should ordinarily be corrected or removed through existing legal remedies. But accuracy alone does not defeat a privacy claim. True information may become misleading when presented without subsequent developments or contextual explanation. Search engines should consider whether the result creates a distorted profile by highlighting a single historical incident.

5.1.6 *Seriousness and Causation of Harm*

The applicant should identify a substantial, foreseeable and continuing harm. Relevant factors include employment discrimination, harassment, threats, exclusion, psychological injury, family consequences and inability to reintegrate. Harm should be connected to the contested processing rather than merely to the underlying event. The emphasis on significant harm is particularly important in European human-rights analysis.¹⁸

5.1.7 *Availability of Less Restrictive Remedies*

Removal should not be the default. Alternatives include correction, annotation, updating, reduced ranking, geo-limited de-indexing, anonymization, suppression of autocomplete suggestions, removal of duplicated copies, or limitation to searches using additional terms. The remedy should be tailored to the source of the injury.

5.2 **Public Figures, Private Individuals and the Right to Information**

The distinction between public and private persons is not a complete rule, but it is a valuable organising principle. Information about a public official's corruption, a doctor's disciplinary history, a company's environmental violations or a politician's prior statements may remain relevant because the person's public role creates continuing accountability. A private person involved in an isolated incident should ordinarily have a stronger claim once the event has ceased to carry public significance.¹⁹

¹⁸ Oganessian, T. (2022). *The right to be forgotten: The European Court of Human Rights in search of the necessary balance*. *Meždunarodnoe Pravosudie*, 12(1), 32–56. <https://doi.org/10.21128/2226-2059-2022-1-32-56>

¹⁹ Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317 (13 May 2014), para 97.

However, public-figure status should not be permanent or total. A person may be publicly known in one domain but retain privacy in another. Nor should a person lose all protection merely because they once appeared in the news. The inquiry must remain tied to the particular information and the particular context.

The right to information also belongs to future users, not only present readers. Journalists, researchers, historians, lawyers and members of the public may have legitimate reasons to consult archives. De-indexing can impair access even where the original source remains technically available. A balance must therefore distinguish between preserving the record and maintaining unlimited discoverability through a person's name.

5.3 Courts, Regulators and Private Intermediaries

The most difficult institutional question is who should perform the balancing exercise. Courts offer independence, procedural safeguards, public reasons and authoritative interpretation. But judicial adjudication of every request is unrealistic. Data-protection authorities can develop expertise and issue guidance, yet may be slow or under-resourced. Search engines can process large volumes and respond rapidly, but they lack democratic legitimacy and may not adequately represent the public interest.²⁰

A layered system is preferable:

1. Initial administrative assessment by the intermediary: Using published criteria and a presumption against removal where there is a strong public-interest basis.
2. Notice and reasoned decision: Subject to privacy safeguards and protection against retaliation.
3. Independent review: By a data-protection authority or specialized tribunal for contested or significant cases.
4. Judicial review: Particularly where the matter concerns public officials, journalism, court records, political speech or a novel legal issue.
5. Periodic reconsideration: Because relevance and harm may change over time.

The process should include mechanisms for notifying publishers where appropriate, although notification must not expose applicants to further harm. It should also permit participation by public-interest representatives in cases involving journalism, archives or public records.

The goal is not to eliminate private decision-making but to prevent it from becoming private constitutional law. Search engines should administer a public framework, not invent one in secret.²¹ Their decisions should be auditable through anonymised transparency reports, consistent terminology, reason-giving and external oversight.

6 CHALLENGES AND OPEN QUESTIONS

6.1 Censorship and Historical Revision

The strongest objection to the right to be forgotten is that it can become a mechanism for censorship. Powerful individuals may seek to conceal misconduct, political actors may attempt to rewrite their

²⁰ Leiser, M. (2020). 'Private jurisprudence' and the right to be forgotten balancing test. *Computer Law & Security Review*, 39, 105458. <https://doi.org/10.1016/j.clsr.2020.105458>

²¹ Liambomba, Didier. (2023). *The Right of Access to Public Information: Human Rights Issues, Transparency and Good Governance*. Constitutionale. 4. 1-28. 10.25041/constitutionale.v4i1.2601.

histories, and corporations may use privacy claims to suppress investigative reporting.²² If removal decisions are secret, the public may never know what has disappeared.

This danger is especially acute where the information is accurate and concerns public conduct. A legal regime that treats reputational injury as sufficient would convert privacy into a veto over criticism. The law should therefore distinguish dignity-protective remedies from reputation management. The right to be forgotten should not be a general right to curate one's public image.

6.2 Global Enforcement and Territoriality

The internet is transnational, but privacy and speech laws remain territorially organised. A European order may require de-indexing within the European Union, while another jurisdiction may prohibit removal. Global application of a removal order risks exporting one jurisdiction's speech standards to the world. Territorial limitation, however, may be ineffective where users can access foreign versions of a search engine or use technical circumvention.²³

The CJEU has wrestled with the territorial scope of de-indexing, particularly in cases concerning whether removal should extend beyond European domains. The problem reveals a broader tension between effective privacy protection and respect for constitutional pluralism. A sensible approach should begin with territoriality, permit broader measures only where necessary and proportionate, and avoid requiring platforms to impose one state's balance globally.

6.3 The Right to Information as a Counterweight

The public's right to know is often diffuse and underrepresented in individual removal procedures. A person seeking removal is identifiable and motivated; the journalist, researcher or future citizen who may need the information is unknown. This structural asymmetry favours privacy claims.

Public-interest representation is therefore necessary. Data-protection authorities should issue guidance on categories of information presumptively linked to public interest, including corruption, serious professional misconduct, public-health threats, abuse of public office and threats to vulnerable groups. Courts should be cautious when removal would impair access to judicial records, historical archives or investigative journalism.²⁴

The existence of a public record should not automatically defeat privacy. Open justice has limits, and the continued online indexing of a judgment may impose a burden far greater than access to the physical file. But the solution should often be anonymization, redaction or controlled access rather than disappearance.

6.4 Technological Feasibility

Technical systems cannot reliably distinguish public interest from public curiosity. Automated tools may identify names, dates and categories, but proportionality requires contextual judgment. Machine-learning systems may reproduce bias, over-remove controversial content or under-protect marginalized persons. They may also fail to recognize cultural and linguistic differences.

²² Amponsah P., (2024) *Investigative Reporting: Its Practice, Boundaries and Implications*. Sub-Saharan Publishers (ISBN: 978-9988-9369-0-7)

²³ Gregorio G. (2024). *The Transnational Dimension of Data Protection*. <https://doi.org/10.1163/27725650-01020006>

²⁴ Singh S. *Studying the Intricacies of Privacy and Data Protection in India – A Critical Analysis of the Indian Laws*. pp.118. Notion Press

Search engines must additionally manage duplicate webpages, mirrors, cached content, social-media re-posts and alternative search terms. A single de-indexing order may be ineffective if information is replicated across platforms. Conversely, overly broad technical enforcement may suppress unrelated information sharing the same name.

Technological design should therefore support, rather than replace, legal judgment. Systems should provide graduated controls, record decision rationales, permit human escalation and preserve evidence for review. Privacy by design should include minimization, purpose limitation and mechanisms preventing unnecessary repetition of sensitive information.

6.5 Inconsistent Standards

The absence of uniform criteria creates uncertainty for applicants, publishers and platforms. European institutions themselves have developed overlapping but not identical approaches. The CJEU data-protection reasoning and the ECtHR's proportionality analysis may point in different directions. India is developing its constitutional and statutory position, while the United States remains resistant to a general removal right.

Some inconsistency is inevitable because privacy and expression are culturally and constitutionally situated. The aim should not be complete uniformity but principled compatibility. International standards could establish minimum procedural requirements: reasoned decisions, notice, independent review, protection for journalism, consideration of public interest, preference for less restrictive remedies and transparency concerning aggregate outcomes.

6.6 Identity, Equality and Social Reintegration

The right to be forgotten has an important equality dimension. Persistent digital records may disproportionately burden persons from disadvantaged groups, defendants who lacked resources to respond to allegations, victims of abuse, former offenders seeking reintegration and individuals targeted by online harassment. A purely formal commitment to equal access to information may reproduce unequal social consequences because some individuals bear far greater risks from permanent visibility than others.

At the same time, privacy remedies must not privilege elites. If only prominent or wealthy applicants can secure de-indexing, the system will become a tool of reputational control. Accessible procedures, legal aid, transparent criteria and regulatory oversight are essential.²⁵

7 CONCLUSION

The conflict between the right to be forgotten and the right to information is not a contest between a modern privacy right and an outdated conception of free expression. Both respond to genuine features of digital life. Individuals require protection from permanent, contextless and disproportionate exposure. Democratic societies require the preservation and circulation of information, including information that challenges reputations and unsettles the powerful.

The correct legal approach rejects hierarchy. Privacy should not automatically defeat expression, and expression should not automatically defeat privacy. The balance must be contextual and proportionate.

²⁵ Leiser, M. (2020). 'Private jurisprudence' and the right to be forgotten balancing test. *Computer Law & Security Review*, 39, 105458. <https://doi.org/10.1016/j.clsr.2020.105458>

It should consider the nature and sensitivity of the information, the public role of the individual, the contribution of the information to public debate, the passage of time, accuracy, context, the seriousness of harm and the availability of less restrictive remedies.

Five principles should guide the digital balance.

First, the law should distinguish source deletion from search de-indexing, anonymization, correction and contextualization. The least restrictive effective remedy should be preferred.

Secondly, public interest should be distinguished from public curiosity. Information concerning public accountability, safety, corruption, professional integrity and historical understanding should receive strong protection.

Thirdly, private individuals should generally receive greater protection than public officials or persons who voluntarily assume public-facing roles, though no category should be absolute.

Fourthly, decision-making should be transparent, reasoned and independently reviewable. Search engines may perform an initial administrative function, but they should not become the final arbiters of fundamental rights. The problem of private jurisprudence must be addressed through public standards, regulatory supervision and judicial review.²⁶

Fifthly, remedies should be temporally sensitive. A refusal to remove information today should not foreclose reconsideration when circumstances change. Conversely, a decision to de-index should not prevent legitimate archival or public-interest access through appropriate channels.

The European experience demonstrates both the necessity and the difficulty of recognizing informational self-determination. The American experience warns against allowing truthful information to be suppressed through broad governmental or private powers. The Indian constitutional framework offers an opportunity to develop a middle path grounded in dignity, autonomy, expression, open justice and proportionality. The Digital Personal Data Protection Act 2023 can contribute to that project if interpreted as part of a constitutional settlement rather than as a self-contained erasure mechanism.

The digital balance will never be achieved by a single rule. It requires institutions capable of distinguishing harm from discomfort, public interest from curiosity, historical preservation from perpetual exposure and privacy protection from censorship. The right to be forgotten should therefore be understood not as a right to erase history, but as a legal claim to prevent the unjustified transformation of a person's past into a permanent and disproportionate feature of their present. The right to information, correspondingly, should not mean that every fact must remain equally prominent forever. The enduring task is to preserve both human dignity and democratic memory.

* * *

²⁶ Leiser, M. (2020). 'Private jurisprudence' and the right to be forgotten balancing test. *Computer Law & Security Review*, 39, 105458. <https://doi.org/10.1016/j.clsr.2020.105458>