International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

From Erasure to Forgetting: A Comparative Analysis of Emerging Data Privacy Rights

Muskan Bansal[1], Dr Navjot Kaur[2]

[1]Research scholar, University Institute of Legal Studies, Chandigarh University, Mohali.
[2]Assistant Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.

Abstract
A key debate in law has resurfaced considering the digital age, where individuals' personal data lives on the internet indefinitely. This paper explores how two concepts have developed and become distinct from one another: the 'right to be forgotten' and 'erasure'. Whilst both are frequently confused with each other, the former is a data protection right which requires controllers to erase personal data. Using a doctrinal and comparative approach, this paper discusses the evolution of the right to be forgotten and how it was reflected in the Google Spain decision and Article 17 of the General Data Protection Regulation within the Court of Justice of the European Union. In addition, it examines how different countries have adopted differing approaches to this issue. These include the free-speech focused approach of the United States, the case law based and somewhat uncertain approach of India, and developments in Brazil, Argentina, Japan, South Korea, China, Russia and Canada. This paper will argue that the modern approach is moving towards a 'right to erasure', however there is a large variation in how countries approach the 'right to be forgotten'. These differences arise due to differing constitutional values being placed on dignity, freedom, and transparency. However, with technologies such as generative artificial intelligence, blockchain and profiling algorithms now becoming prominent, we are witnessing the limitations of the concept of 'deletion'. Overall, this paper will propose a 'tiered' approach to the right to be forgotten, based on time and context. This can be implemented into modern data protection systems.

Keywords: right to erasure; right to be forgotten; data privacy; delisting; General Data Protection Regulation; Digital Personal Data Protection Act 2023; comparative data protection law; machine unlearning

I. Introduction

Unlike human memory, digital memory is a permanent record. Over the majority of history, forgetting was the norm and remembering the exception. However, the advent of cheap storage, interconnectedness and worldwide searches has resulted in the "reversal of the balance of remembering and forgetting", with forgetting becoming a 'costly' task and remembering the norm.[3] A young indiscretion, cleared debts, exonerations and images uploaded with poor judgment can now all be located within seconds by any

[1]Muskan, Research scholar, University Institute of Legal Studies, Chandigarh University, Mohali.
[2]Dr Navjot Kaur, Assistant Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.
[3]Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (Princeton University Press, Princeton, 2009).

stranger. The right to be left alone, coined by Warren and Brandeis in 1890 to protect themselves from prying journalists, now faces a new scenario.[4]

There has been inconsistent and inconsistent terminology surrounding the response to this issue. In May 2014, in Google Spain, the Court of Justice of the European Union (CJEU) decided that in some situations, operators may be required to remove links to legal web pages of third parties from search results relating to a particular individual. This decision became widely known as the 'right to be forgotten'.[5] Two years later, the GDPR included the 'right to erasure ('right to be forgotten')'[6] causing much confusion. Many have adopted, rejected, or modified this. For example, whilst India's Digital Personal Data Protection Act 2023 includes provisions for rectification and erasure of personal data, there is no explicit 'right to be forgotten' for delisting.[7] The US have largely rejected this right due to First Amendment issues, however do have rights to delete information in specific sectors and at State level. Finally, Brazil, Japan and China all have different conclusions.

This paper seeks to argue that erasure and forgetting are not the same. Erasure is a data focused concept asking whether there is a lawful basis for the controller to retain or process such personal data. If not, then the personal data must be erased. Whereas forgetting is a personal and temporal concept asking whether it is justifiable to have true information relating to an individual available to the public. The first is common in data protection law whereas the latter is an issue surrounding reputation, memory and expression which has been borrowed from data protection law.[8] A lot of the conflict between different jurisdictions stems from the fact these two concepts are often conflated.

This paper will first explain the concepts and background behind this argument (Part II). It will then look at how the EU approach this issue with the Google Spain and Article 17 examples (Part III). It will then analyze the issues with this approach (Part IV). Next, the paper will look at how the US handles this (Part V), India (Part VI) and other emerging jurisdictions (Part VII). Finally, this paper will look at how compare (Part VIII) and consider the challenges presented by artificial intelligence and distributed ledgers. Finally, recommendations will be made (Part IX).

II. Conceptual and Historical Foundations

A. Forgetting as a social and legal practice

The law has always acknowledged the effect time can have on facts. Criminal justice systems allow for deletion or sealing of records; the Bankruptcy Act releases debtors from their obligations; limitation periods extinguish old claims and credit reporting laws provide maximum periods for reporting. All of these are examples of legislation creating a forgetful element to proceedings. However, it is not the fact that time is taken into consideration that is relevant in relation to this debate. Instead, it is a fact that we no longer have a physical element to time, such as in the past.

James Whitman famously argues that legal cultures will have a stronger attitude to preventing unwelcome publicity if they view privacy as a right stemming from dignity (as is the case in much of continental

[4]Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" 4 Harvard Law Review 193 (1890).

[5]Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ECLI:EU:C:2014:317.

[6]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 17, [2016] OJ L119/1.

[7]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 8(7), 12.

[8]Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice" 8(3) SCRIPTed 229 (2011).

Europe), as opposed to privacy being viewed as a liberty right against the state (as is the case in the United States). The difference between the two cultures will be discussed below.[9]

The common law and civil law systems had cases relating to this issue at an early stage. In Melvin v Reid the court found that a woman who had moved away from her past life of prostitution and had been acquitted of murder had a right to pursue happiness which was being infringed by the film showing her past.[10] In contrast, only a decade later in Sidis v F-R Publishing Corp the Second Circuit refused to provide relief to a former child prodigy because they felt there was an interest in seeing how the famous individual was doing now.[11] This created a debate between the right to rehabilitate and the interest of the public. In continental Europe the droit à l'oubli and diritto all'oblio was developed within the French and Italian doctrines in relation to personality rights. This protected individuals who had either been convicted or had been involved in some newsworthy event from having their past circulated indefinitely after they have completed their rehabilitation.[12]

B. From the 1995 Directive to the digital age

The precursor to the modern right to be forgotten can be seen in Directive 95/46/EC which provided that personal data must be erased once they are no longer necessary to keep in an identifiable format. It also gave Data Subjects the right to have incorrect processing of their data rectified, erased or blocked and provided them with the right to object.[13] Whilst these provisions clearly provide Data Subjects with control and assurance over the accuracy of their data, there was no reference to 'forgetting'. In 2012 the term 'right to be forgotten' was introduced into the EU policy discussion by the Commission in its reform proposal. It took inspiration from the French concept of 'oblivion' and the data protection principle of limitation of retention.[14] This concept brought together different traditions and can still be seen in the formulation of Article 17.

C. Differentiating between Erasure, Delisting and Forgetting

It is useful to separate out the concepts of erasure, delisting and forgetting to aid analysis. Erasure involves the deletion of personal data within the systems of the controller (often the creator/holder of the data). Delisting (de-referencing) refers to the removal of links to the information from search results when searching using a name. However, it does not remove the page itself. Finally, forgetting refers to the result of using these tools. They may lead to a restoration of a practical level of 'forgetting', whereby the information will no longer identify the individual.[15] Meg Leta Jones has highlighted that the right to be forgotten should be seen as a range of diverse practices which differ across different legal cultures. The concept should be viewed as a balance of interests 'in the flux of time'. Giovanni Sartor[16]

[9]James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" 113 Yale Law Journal 1151 (2004).

[10]Melvin v. Reid, 112 Cal. App. 285, 297 P. 91 (1931).

[11]Sidis v. F-R Publishing Corp., 113 F.2d 806 (2d Cir. 1940).

[12]Franz Werro (ed.), The Right to Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia (Springer, Cham, 2020).

[13]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on the free movement of such data, arts. 6(1)(e), 12(b), 14, [1995] OJ L281/31.

[14]Alessandro Mantelero, "The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'" 29 Computer Law & Security Review 229 (2013).

[15]Jef Ausloos, The Right to Erasure in EU Data Protection Law (Oxford University Press, Oxford, 2020).

[16]Giovanni Sartor, "The Right to Be Forgotten: Balancing Interests in the Flux of Time" 24 International Journal of Law and Information Technology 72 (2016).

This can have practical implications. Whilst deletion could be carried out, there may still be a complete record of the individuals past due to copies, archives and other controllers holding the data. Alternatively, whilst the individual may have had their data delisted it could still be a practical 'forgetting'. Daniel Solove has described the 'digital person' as a dossier of information that is made up of pieces of data held within many databases. Therefore, whilst deletion may have occurred within one database it is rarely a practical 'forgetting'.[17] Therefore, prior to the GDPR Paul Bernal argued that a 'right to delete' should be created based on autonomy, rather than a general right to change the past.[18] This terminology will be used throughout the remainder of this paper.

III. The European Union: From Google Spain to Article 17

A. The decision in Google Spain

In the Google Spain case, Mario Costeja González, a Spanish citizen brought a complaint to the Spanish Data Protection Authority (AEPD) in 2010 regarding the fact that when searching for his name on Google, it returned links to a newspaper article published in 1998 relating to an auction of his property in relation to attachment orders for social security debts. This issue had long since been resolved. However, the AEPD dismissed this complaint against the newspaper. They found that the newspaper was justified in publishing, but agreed with the complaint against Google Spain and Google Inc. The Grand Chamber of the CJEU decided on referral from the Audiencia Nacional that the search engine operators of the data were 'controllers' under the Data Protection Directive. Secondly, that the Data Protection Directive did apply because the advertising activities of Google's Spanish subsidiary were closely connected to the search engine service. Finally, that the rights of erasure and objection under the Data Protection Directive applied to the search engine operator directly.

This caused the modern debate surrounding this issue. The Court reasoned that searching for a person's name allows any individual on the internet to have a structured overview of their lives. This means that the interference with their rights under Articles 7 and 8 of the Charter of Fundamental Rights could be much more severe than the original publication. Initially, the data had been processed lawfully, but after a period this could be inconsistent with the Data Protection Directive. If the data were no longer relevant, irrelevant, or excessive in relation to the purpose and time elapsed, then they would no longer be adequate. Usually, the rights of the data subject will prevail over the economic interests of the operator and the public interest in accessing the information, unless there are special reasons to justify a dominant public interest in accessing the data. Such as if the data subject has a prominent role in public life.

B. Response and criticism

The decision was met with praise and concern. Orla Lynskey commented that the CJEU had taken a broad approach when determining that a search engine operator is a controller, the extraterritorial reach of the directive and that data protection is a fundamental right and, in most circumstances, will prevail.[19] However, critics such as Stefan Kulk and Frederik Zuiderveen Borgesius believed that the Court did not

[17]Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age (New York University Press, New York, 2004).

[18]Paul Bernal, "A Right to Delete?" 2(2) European Journal of Law and Technology (2011).

[19]Orla Lynskey, "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez" 78 Modern Law Review 522 (2015).

pay much attention to the freedom of expression under Article 11 of the Charter.[20] By leaving the balance to a private company, the Court had created a form of privatized justice. The Article 29 Working Party issued guidelines on how to determine delisting requests.[21] There are thirteen factors to consider. Including if the data subject has a role in public life, if the information is accurate, if it were a minor, and if the information is current and relevant. Google's own Advisory Council came to similar conclusions. However, they stated that delisting should not be used for information relating to political life, professional conduct, or criminal activity.[22]

C. Article 17 GDPR

The GDPR, which came into force on the 25th May 2018, brought together and extended the previous case law. It provides individuals with the right to have their data erased without undue delay if it is no longer necessary for the purpose for which it was collected, consent has been withdrawn and there is no other grounds to process the data, the data subject has objected under Article 21 and there are no overriding legitimate grounds, data has been unlawfully processed, it is required by a legal obligation, or if the data was collected from a child in relation to information society services. If the controller has made the data public, then they must also take reasonable steps to inform other controllers who process the data of the request for erasure. They must do this having regard to the technology available and the cost (Article 17(2)). This provision was intended to enhance the right to be forgotten in an online environment.

However, there are exceptions to this. Under Article 17(3) the right does not apply if it is necessary to exercise the right to freedom of expression and information, to comply with a legal obligation or if it is in the public interest, to protect public health, for archiving purposes, scientific or historical research and statistical purposes and if the erasure would seriously affect these purposes. Or if it is necessary for the establishment, exercise, or defence of legal claims. The controller must respond within a month. This can be extended if the matter is complex by a further 2 months. If they violate the rights of a data subject, they will receive the higher tier of administrative fines up to 20 million Euros or 4% of their worldwide annual turnover. Paul De Hert and Vagelis Papakonstantinou have commented that this article is not a new right, but rather the application of existing data protection principles.[23] This can be seen in the fact that it is included in the chapter relating to the rights of the data subject. Alongside the right to rectification and objection.

The article encompasses confusion from part II. The title of the article refers to the right to erasure. However, the note refers to the right to be forgotten. The body of the article uses data protection terminology such as purpose, necessity, consent, and lawfulness. The right to be forgotten is only mentioned once in the article. Within Article 17(3)(a). And in Article 85, which requires member states to balance data protection and freedom of expression and information. Therefore, the balance between privacy and memory was left to the exceptions.

[20]Stefan Kulk and Frederik Zuiderveen Borgesius, "Google Spain v. González: Did the Court Forget About Freedom of Expression?" 5 European Journal of Risk Regulation 389 (2014).

[21]Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. AEPD and Mario Costeja González" C-131/12, WP 225 (26 November 2014).

[22]The Advisory Council to Google on the Right to be Forgotten, Final Report (6 February 2015).

[23]Paul De Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" 32 Computer Law & Security Review 179 (2016).

IV. Limits and Doctrinal Tensions within the European Model

A. Territorial reach

The first and most controversial restriction is geographically based. Within Google LLC v CNIL, the Grand Chamber held that EU law does not require a search engine provider to apply delisting across all iterations of the search engine. However, all Member State iterations must delist and must put appropriate measures, for example, for geolocation blocking, to ensure that the delisting cannot be accessed by users in the EU.[24] However, it was also held that national authorities can impose delisting across the globe, using national standards in accordance with a balance of rights. This shows how the practicality of the 'right to be forgotten' has been acknowledged; the right to be forgotten cannot be argued internationally without conflicting with the interests of other countries. This shows how forgetting is very much restricted to particular areas.

B. Sensitive Data, Inaccuracies and Images

This was then further clarified within three subsequent judgments. GC and Others v CNIL held that special categories of data (Article 9) and data relating to convictions (Article 10) cannot be processed by search engines and must be considered. A balance must be made between the rights of the data subject and public interest and delist if the linking is not strictly necessary to protect the freedom of information of internet users.[25] TU and RE v Google LLC held that the manifest inaccuracy of the data must be shown by the data subject wishing to delist the information. However, the data subject does not need to prove the court has ruled against the publisher before requesting delisting. Furthermore, search engines must view thumbnail images separately to the context of the article.[26] This along with the Guidelines 5/2019 from the European Data Protection Board clarifies that the European right to be forgotten does not give people the right to censor information. It gives people the right to make information obscure when searching for it by name.[27]

C. Source Issues - Registers

The European viewpoint is far more cautious when the source of information is being targeted. Within Manni, it was held that a person cannot ask to erase their personal data from the companies to register following the dissolution of the company. This is due to the interest in legal certainty and transparency of such registers. However, Member States can exceptionally allow a restriction on access.[28] The European Court of Human Rights has also held similar views regarding archives. Within Węgrzynowski and Smolczewski v Poland it was held that the courts had not breached article 8 by refusing to remove an article from an online archive. The courts do not have the role to rewrite history.[29] Furthermore, in M.L. and W.W. v Germany it was held there was no breach of Article 8 as the German courts refused to make media anonymise reports about two men who were convicted of murder. This was even after their release.[30] The Grand Chamber upheld this by holding that an order for a newspaper to anonymise an article about a fatal road traffic accident in an online archive to protect the driver's reputation many years later

[24]Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), Case C-507/17, ECLI:EU:C:2019:772 (CJEU, 24 September 2019).
[25]GC and Others v. CNIL, Case C-136/17, ECLI:EU:C:2019:773 (CJEU, 24 September 2019).
[26]TU, RE v. Google LLC, Case C-460/20, ECLI:EU:C:2022:962 (CJEU, 8 December 2022).
[27]European Data Protection Board, 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 (7 July 2020).
[28]Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, Case C-398/15, ECLI:EU:C:2017:197 (CJEU, 9 March 2017).
[29]Węgrzynowski and Smolczewski v. Poland, App. No. 33846/07 (ECtHR, 16 July 2013).
[30]M.L. and W.W. v. Germany, App. Nos. 60798/10 and 65599/10 (ECtHR, 28 June 2018).

did not breach Article 10. However, this must be exceptionally rare and must meet a detailed list of requirements and be proportionate to its purpose.

Overall, the European model shows two different approaches. Firstly, the Court of Justice has taken a fairly strong view of forgetting within search engines due to the unique harm caused by searching for the name. However, European courts have taken an archival approach to forgetting when the source is being targeted. This means that forgetting will not be applied as press freedom, and legal certainty will override it unless exceptional circumstances arise. The European courts have tried to strike a balance between allowing some memory within archives whilst making sure things are obscured.

V. The United States: Remembering as a Constitutional Default

A. The First Amendment barrier

This is not the case in the United States. It is difficult to reconcile the general right to force the removal of accurate information with the Supreme Court's decision in Cox Broadcasting Corp v Cohn, where it was decided that a state could not hold a broadcaster liable for the broadcast of a victim of rape's name obtained from judicial records that were open to public scrutiny.[31] This was followed in Smith v Daily Mail Publishing Co where it was decided that it was not permissible for a state to hold a publisher liable for the lawful publication of the name of a juvenile offender.[32] This was also decided in Florida Star v B.J.F., where the same outcome was reached for information obtained from a police report.[33] The Supreme Court affirmed that the creation and sharing of information constitutes speech in Sorrell v IMS Health.[34] Eugene Volokh and Donald Falk have argued that search engine results are protected editorial discretion, meaning that name based search ranking and removal would be protected. Furthermore, lower courts have been skeptical about the argument that the passage of time or subsequent expungement of accurate information creates a tort. In Martin v Hearst Corp, the Second Circuit decided that a publication of accurate information about an arrest by a newspaper was not defamatory despite a statute in Connecticut erasing the arrest from occurring.[35]

Jeffrey Rosen's popular statement that the European right presents the greatest threat to free speech on the internet in the next decade reflects the common American view.[36] However, Edward Lee has argued that if the United States recognizes any such right it would need to be very specific to survive First Amendment challenges. This can be explained by the way in which American privacy laws center on privacy rights as opposed to dignity rights, with privacy being about resisting government intrusion rather than public exposure. This means that public records and accurate information are almost sacred in the United States

B. Statutory Erasure

However, the United States does recognize a right to erase. The United States has created the right through data protection and consumer protection laws. The California Consumer Privacy Act (as amended by the California Privacy Rights Act) gives consumers the right to request the erasure of personal information

[31]Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).
[32]Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).
[33]Florida Star v. B.J.F., 491 U.S. 524 (1989).
[34]Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).
[35]Martin v. Hearst Corp., 777 F.3d 546 (2d Cir. 2015).
[36]Jeffrey Rosen, "The Right to Be Forgotten" 64 Stanford Law Review Online 88 (2012).

they have provided, with exceptions for free speech and legal compliance.[37] The California Delete Act of 2023 requires the state privacy regulator to create one method of consumers requesting all registered data brokers to erase their personal information. Brokers must respond to these requests periodically.[38] The state also has an 'eraser' law, allowing minors to request the removal of content they have posted on websites and apps aimed at them. At a federal level there is the Fair Credit Reporting Act, which requires negative information to be reported for a set period, usually seven years for most negative information and ten years for bankruptcies.

This shows how the United States has separated the two concepts. There is increasing acceptance that data held by commercial entities should be erased. However, there is a constitutional distaste for the concept of forgetting to prevent the publication or indexing of accurate information. Michael Rustad and Sanna Kulevska suggest that this can be overcome by redefining the right to data minimization by commercial entities, allowing data to flow across the Atlantic.

VI. India: Judicial Experimentation and Legislative Ambivalence

A. Constitutional foundations

In the Indian jurisprudence, the right to be forgotten was first recognised by the Supreme Court in the case of R. Rajagopal v State of Tamil Nadu. The Supreme Court recognised that a right to privacy exists under Article 21, but this does not extend to information that is public information, such as judicial proceedings. Public officials have a reduced right to privacy.[39] Later, in the landmark case of Justice K.S. Puttaswamy (Retd.) v Union of India, a fundamental right to privacy was recognised. This includes the right to informational self-determination. Kaul J specifically refers to the right to be forgotten in Europe. However, he notes that this cannot be absolute. He states that this right will not apply if the information is necessary for the exercise of freedom of expression, a legal duty, public interest relating to health or legal claims.[40]

B. High Court Jurisprudence

The High Courts have adopted a practical and inconsistent approach to this issue as there is no statute. In Sri Vasunathan v Registrar General the Karnataka High Court ordered that the name of a female should be obscured in the search results. This relates to the trend in Western countries to recognise a right to be forgotten in sensitive cases relating to women.[41] In contrast, the Gujarat High Court in Dharamraj Bhanushankar Dave v State of Gujarat did not order the removal of an acquittal from an online legal database. The Court noted that publishing on an online website does not amount to reporting. There was also no breach of Article 21.[42] However, in Zulfiqar Ahman Khan v Quintillion Business Media Pvt Ltd, the Delhi High Court ordered an interim remedy to remove articles related to sexual misconduct allegations. The Court recognised a right to privacy, which includes a right to be forgotten and a right to be left alone.[43] The Orissa High Court in Subhranshu Rout v State of Odisha recognised a right to be forgotten in relation to non-consensual intimate images, however they noted that there is no statutory

[37]California Consumer Privacy Act of 2018, Cal. Civ. Code s. 1798.105, as amended by the California Privacy Rights Act of 2020.
[38]California Delete Act, S.B. 362 (2023), Cal. Civ. Code s. 1798.99.80 et seq.
[39]R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[40]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Kaul J.).
[41]Sri Vasunathan v. Registrar General, 2017 SCC OnLine Kar 424.
[42]Dharamraj Bhanushankar Dave v. State of Gujarat, 2017 SCC OnLine Guj 2493.
[43]Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd., 2019 SCC OnLine Del 8494.

recognition so victims do not have any real remedies.[44] Lastly, in Jorawer Singh Mundy v Union of India the Delhi High Court ordered an interim remedy to block an acquittal from appearing in search results.[45] Overall, this can be described as a positive rights-based approach. However, the Courts have often confused deleting judicial records, removing search engines, and anonymizing. Therefore, there is no clear test for the Courts to follow, such as the Google Spain criteria, and whether something should be removed will depend on the sensitivity of the information and who the applicant is.

C. Legislative Development

In 2018, the Justice B.N. Srikrishna Committee released a report suggesting a statutory right to be forgotten. This is a right to limit or prevent the ongoing disclosure of personal data. An Adjudicating Officer will decide based on factors such as the sensitivity of the data, extent of disclosure, prominence of the data principal in public life and nature of disclosure.[46] This right was included in the Personal Data Protection Bill (2019) under clause 20.[47] However, the Bill was withdrawn in 2022 after the report by the Joint Parliamentary Committee. The Digital Personal Data Protection Act (2023) has a very narrow approach to this right. It gives data principals the right to rectify, complete, update or delete personal data. Data fiduciaries must delete personal data if consent is withdrawn or the purpose is no longer fulfilled. This right does not exist for delisting.

There are several factors that make this Act ineffective in providing a right to be forgotten in the European way. Firstly, this Act does not apply to personal data that has been published by the data principal or another party under a legal duty to publish. This means many pieces of data will not be covered by this Act. Many pieces of archival data and judicial data will be excluded. Arguably, many pieces of data published by news media will not apply. Secondly, the exemptions are very broad. This includes processing necessary for the enforcement of legal rights, prevention and detection of offences and research. The Central Government also have the power to exempt State Instrumentalities. Thirdly, this Act amends section 8(1)(j) of the Right to Information Act (2005) to reduce the exemption of personal information. This creates a new balance between transparency and privacy. Lastly, in relation to intermediaries, the Supreme Court has interpreted section 79 of the Information Technology Act (2000) in Shreya Singhal v Union of India. This means that intermediaries can only be required to remove content with a court order or government notification. This means there are limited private remedies to enable a right to be forgotten.[48] The Digital Personal Data Protection Rules (2025) have been notified in November 2025. This provides mechanisms for consent, time limits for deletion and the Data Protection Board. However, there is no standalone right to be forgotten.[49] Overall, in India there is a distinct difference between deleting data and the right to be forgotten. Deleting data is now a statutory right based on the principle of limiting purposes and consent. However, the right to be forgotten is a personal right which only applies to lawful, published, and accurate information. This is a judicially determined exception and

[44]Subhranshu Rout v. State of Odisha, 2020 SCC OnLine Ori 878.

[45]Jorawer Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306.

[46]Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, New Delhi, 2018).

[47]The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019), cl. 20.

[48]Shreya Singhal v. Union of India, (2015) 5 SCC 1; Information Technology Act, 2000, s. 79.

[49]Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025 (notified November 2025).

will depend on how the Constitution, DPDP Act and Data Protection Board deal with this issue in the future.

VII. Other Emerging Jurisdictions

A. Latin America

Brazil's General Data Protection Law (LGPD) provides data subjects with the right to erase personal data processed with their consent and to anonymise, block or destroy redundant or excessive data. However, the Federal Supreme Court ruled in the Aída Curi case in 2021 that there is no 'right to be forgotten' in Brazilian law. The case concerned a claim by the family of a woman murdered in 1958 seeking compensation from a television programme depicting the crime. The Court ruled that a right to be forgotten, preventing the disclosure of true facts obtained lawfully, is unconstitutional. Instead, any excesses will be dealt with on a case-by-case basis using the rights to honour, image and privacy. Argentina provides a further example. The Supreme Court ruled in Rodríguez v Google that search engines cannot be strictly liable for third party content. The individual must have actual knowledge of the content for liability to arise, unless it is obvious that the content is illegal.

B. Asia

The Supreme Court of Japan ruled in 2017 that in cases where an individual has requested the removal of search results relating to an arrest for child prostitution, deletion will only apply if there is a clear balance in favour of the interest in keeping the information private. The Court ruled that this was not the case.[50] South Korea provides individuals with the right to correct, delete and suspend processing under the Personal Information Protection Act. In 2016, the Korea Communications Commission issued guidelines to allow individuals to restrict access to their posts on websites.[51] This however, is a very limited form of forgetting as it only applies to content created by the individual. In China, in Ren Jiayu v Baidu the Beijing No 1 Intermediate People's Court ruled that there was no right to be forgotten. They ruled that the right to be forgotten was not a statutory right to personality and there was no legitimate and necessary interest. However, erasure has been implemented in data governance terms. The Civil Code provides individuals with the right to ask for deletion if processing is unlawful or breaches an agreement. The Personal Information Protection Law (2021) provides that personal information must be deleted by processors if it has fulfilled its purpose or the retention period has expired. Alternatively, individuals can request deletion in certain circumstances.[52]

C. Russia and Canada

Russia were amongst the first States to introduce legislation. Under Federal Law No 264-FZ (2015), search operators must stop providing links to information that is being unlawfully disseminated, incorrect or outdated, if requested. However, exceptions apply to information relating to crimes where the time limit has not expired and convictions. There have been criticisms of this legislation due to the lack of procedural protections for expression. In Canada, the Federal Court ruled in 2021 that the federal private sector privacy statute (PIPEDA) applies to Google's search engine. A proposed federal Bill C-27 which would have provided individuals with a right to dispose of personal information, has failed to pass in January

[50] Supreme Court of Japan, Decision of 31 January 2017, 71 Minshū 63.

[51] Personal Information Protection Act (South Korea), arts. 36-37; Korea Communications Commission, Guidelines on the Right to Request Access Restriction of Personal Internet Postings (2016).

[52] Civil Code of the People's Republic of China (2020), art. 1037; Personal Information Protection Law of the People's Republic of China (2021), art. 47.

2025. This however, has been improved upon in Quebec. The amended private sector privacy statute provides individuals with the right to ask for the discontinuation of dissemination or de-indexing of personal information if it causes serious damage to their reputation or privacy. This right is subject to the public interest and freedom of expression.

VIII. Comparative Synthesis: What Is Converging and What Is Not

A. Three models

This comparative overview shows three different models: (1) the dignity based model (European Union) whereby the right to forget is primarily protected through a balancing act at the point of name based aggregation; (2) the speech protection model (United States) where the right to forget is accepted as part of consumer control over commercial data but resisted as a constraint on legal publication; and (3) the hybrid model (India, Brazil, Japan, China), where the right to be forgotten is enshrined in statute but there is judiciary scepticism or uncertainty. A summary of the comparative overview is given below.

Jurisdiction	Principal sources	Erasure of data held by controllers	Delisting or forgetting of public information	Principal constraint
European Union	GDPR Art 17; Google Spain	Statutory right with enumerated grounds	Recognised for name-based search; exceptional for archives	Art 17(3); Art 85; press and register interests
United States	CCPA/CPRA; Delete Act; FCRA	Consumer and sectoral rights	Constitutionally disfavoured	First Amendment
India	DPDP Act 2023; High Court decisions	Statutory (ss 8(7), 12)	Judicially recognised, not codified	Public-data carve-out; exemptions; transparency law
Brazil	LGPD; STF Tema 786	Statutory	Rejected in the abstract; case-by-case remedies	Constitutional press freedom
Japan	APPI; Supreme Court 2017	Statutory, limited	Only where privacy clearly outweighs public interest	Public interest in information
China	PIPL; Civil Code; Ren Jiayu	Statutory	Not recognized as a right	Platform and State governance

B. Explaining the divergence

The first aspect to consider is the nature of constitutional culture. In jurisdictions where privacy is based on a value of dignity (such as the European Union), access to outdated personal data can easily be seen to be an insult to someone's personality. Conversely, where privacy is based on a value of freedom from the State and freedom of information (such as the United States), access to outdated personal data can be seen as a necessary consequence of a free and open society. India is somewhere in between. It has a constitution that protects both dignity and expression, and it has a judiciary that has so far managed to balance this tension without a general test.

The second aspect to consider is the structure of the system. The European approach has a private sector body responsible for initial adjudication, although this body is regulated by data protection authorities and the courts. The Indian approach currently relies upon constitutional courts which can be slow, restrictive and inconsistent. Finally, the American approach relies on a market and legislative approach which can be effective for commercial data but are unable to deal with lawful disclosure. Therefore, the effectiveness of the right to be forgotten depends on whether it can be cheaply, quickly and consistently applied, and whether there is a principled test.

Finally, consideration of time. Only the European jurisprudence explicitly considers time, requiring that data is no longer relevant or excessive given the amount of time that has passed. The American Fair Credit Reporting Act and criminal expungement statutes also consider time but only for very specific categories. The Indian DPDP Act only implicitly considers time, through the expiry of the purpose. A real law of forgetting, rather than law of deletion, must consider time. A fact's importance to the public interest will depend on time, the role of the individual, the nature of the fact and how it is used.

C. The technological frontier

There is a growing divide between the concepts of deletion and forgetting due to technology. Firstly, large machine learning models trained on personal data are not trained in a way that allows for easy deletion of records. This has led to a new field of study looking at whether it is possible to remove the impact of certain training data on a trained model without having to train the model again.[53] Whilst early research has shown that forgetting can be made efficient by re-structuring learning algorithms to be in a summative format, there are technical challenges with achieving precise unlearning in large neural networks. Regulatory bodies are beginning to address this, with the Italian data protection authority intervening in 2023 in relation to a generative AI service. Issues included in the inability to correct or delete incorrect personal data in the model's output. The European Data Protection Board also addressed this in Opinion 28/2024 by considering whether AI models trained on personal data can be considered anonymous.[54] Secondly, distributed ledger technology stores data in a way that is intended to be immutable. Where possible, the CNIL advises that personal data should not be stored on chain. If this cannot be avoided, then personal data can be stored off-chain with hashes on-chain, or keys can be cryptographically deleted. Finally, there has been a shift in regulation of platforms meaning that the focus has moved away from data subject rights. The EU Digital Services Act now provides an additional method of removing unlawful content using a notice and action approach.[55]

This confirms the main point of this paper. If forgetting is deletion, then it will fail to work where it is not possible or effective. However, if forgetting is re-introducing obscurity in context, then there are numerous methods to achieve this. This can include delisting, limiting access, anonymization, de-ranking, key destruction, and filtering outputs.

IX. Conclusion and Recommendations

This paper argues that the development of data privacy rights has resulted in a bifurcation between rights to 'erasure' and 'forgetting'. While rights to erasure based on principles of storage limitation, consent and lawfulness, have become almost universal in modern data protection statutes (GDPR, DPDP Act, LGPD,

[53]Lucas Bourtoule et al., "Machine Unlearning" in 2021 IEEE Symposium on Security and Privacy (SP) 141 (IEEE, 2021).

[54]European Data Protection Board, Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models (17 December 2024).

[55]Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act), art. 16, [2022] OJ L277/1.

PIPL, California statutes). Rights to 'forgetting' based on principles of temporality, dignity and personal information integrity, however, are jurisdictionally specific, unclear and depend on the balance between privacy and freedom of expression, public memory and transparency in each legal order. This has been exacerbated by the misnomer 'right to be forgotten'.

Recommendations

Differentiate between remedies: Differentiate between erasure, delisting and anonymization /contextualization in data protection statutes. Each remedy should have specific criteria and exemptions.

Temporal considerations: Any right to be forgotten should include consideration of the age of the information, type of data, the individual's public role and ongoing public interest in the information. These factors should be included in the statute, such as in the Google Spain case and factors set out by the Article 29 Working Party.

Proportionality of remedies in relation to archives: As stated by Hurbain and the case law of the European Court of Human Rights, courts should consider whether information can be updated, annotated, anonymised or de-indexed in name searches before ordering deletion of journalistic or judicial information.

Accountability of adjudication: While private bodies may be responsible for the initial request, an independent body such as the Data Protection Board of India should be responsible for appeals. Publication of transparency reports is also important.

Public data: Consider whether section 3(c)(ii) of the DPDP Act should be amended. Alternatively, a limited right to limit ongoing disclosure of personal data made publicly available should be included. This should be in relation to specific sensitive information (acquittals, sexual offences, juveniles, non-consensual intimate images). Guidance should also be provided for judicial information.

Consideration of technological limitations: Regulators should provide guidance on what constitutes effective erasure in machine learning and distributed ledger technologies. Privacy by design should be encouraged, such as minimizing data and designing systems to allow for unlearning.

The aim is not to create a society where we forget. Archives, journalism, research, and accountability rely on our ability to remember. We want to create a society where we thoughtfully and proportionally remember. We do not want individuals to be defined by the most easily accessible piece of their past forever. The tool is erasure, but we should be seeking to uphold the value of forgetting. This can only be achieved if the distinction is clearly made in the law.

References

Books

1. Ausloos, Jef, The Right to Erasure in EU Data Protection Law (Oxford University Press, Oxford, 2020).
2. Jones, Meg Leta, Ctrl+Z: The Right to Be Forgotten (New York University Press, New York, 2016).
3. Mayer-Schönberger, Viktor, Delete: The Virtue of Forgetting in the Digital Age (Princeton University Press, Princeton, 2009).
4. Solove, Daniel J., The Digital Person: Technology and Privacy in the Information Age (New York University Press, New York, 2004).
5. Werro, Franz (ed.), The Right to Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia (Springer, Cham, 2020).

Articles and chapters

1. Bernal, Paul, "A Right to Delete?" 2(2) European Journal of Law and Technology (2011).
2. Bourtoule, Lucas et al., "Machine Unlearning" in 2021 IEEE Symposium on Security and Privacy (SP) 141 (IEEE, 2021).
3. Cao, Yinzhi and Yang, Junfeng, "Towards Making Systems Forget with Machine Unlearning" in 2015 IEEE Symposium on Security and Privacy 463 (IEEE, 2015).
4. De Hert, Paul and Papakonstantinou, Vagelis, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" 32 Computer Law & Security Review 179 (2016).
5. Koops, Bert-Jaap, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice" 8(3) SCRIPTed 229 (2011).
6. Kulk, Stefan and Borgesius, Frederik Zuiderveen, "Google Spain v. González: Did the Court Forget About Freedom of Expression?" 5 European Journal of Risk Regulation 389 (2014).
7. Lee, Edward, "The Right to Be Forgotten v. Free Speech" 12 I/S: A Journal of Law and Policy for the Information Society 85 (2015).
8. Lynskey, Orla, "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez" 78 Modern Law Review 522 (2015).
9. Mantelero, Alessandro, "The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'" 29 Computer Law & Security Review 229 (2013).
10. Rosen, Jeffrey, "The Right to Be Forgotten" 64 Stanford Law Review Online 88 (2012).
11. Rustad, Michael L. and Kulevska, Sanna, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow" 28 Harvard Journal of Law & Technology 349 (2015).
12. Sartor, Giovanni, "The Right to Be Forgotten: Balancing Interests in the Flux of Time" 24 International Journal of Law and Information Technology 72 (2016).
13. Volokh, Eugene and Falk, Donald M., "Google: First Amendment Protection for Search Engine Search Results" 8 Journal of Law, Economics & Policy 883 (2012).
14. Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy" 4 Harvard Law Review 193 (1890).
15. Whitman, James Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty" 113 Yale Law Journal 1151 (2004).

Cases

1. Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, Case C-398/15, ECLI:EU:C:2017:197 (CJEU).
2. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).
3. Dharamraj Bhanushankar Dave v. State of Gujarat, 2017 SCC OnLine Guj 2493.
4. Florida Star v. B.J.F., 491 U.S. 524 (1989).
5. GC and Others v. CNIL, Case C-136/17, ECLI:EU:C:2019:773 (CJEU).
6. Google LLC v. CNIL, Case C-507/17, ECLI:EU:C:2019:772 (CJEU).
7. Google Spain SL v. AEPD, Case C-131/12, ECLI:EU:C:2014:317 (CJEU).
8. Hurbain v. Belgium [GC], App. No. 57292/16 (ECtHR, 2023).
9. Jorawer Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306.
10. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
11. M.L. and W.W. v. Germany, App. Nos. 60798/10 and 65599/10 (ECtHR, 2018).
12. Martin v. Hearst Corp., 777 F.3d 546 (2d Cir. 2015).
13. Melvin v. Reid, 112 Cal. App. 285 (1931).

14. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
15. Ren Jiayu v. Beijing Baidu Netcom Science Technology Co. Ltd. (Beijing No. 1 Intermediate People's Court, 2015).
16. Rodríguez, María Belén c. Google Inc., Fallos 337:1174 (Argentina, 2014).
17. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
18. Sidis v. F-R Publishing Corp., 113 F.2d 806 (2d Cir. 1940).
19. Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).
20. Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).
21. Sri Vasunathan v. Registrar General, 2017 SCC OnLine Kar 424.
22. Subhranshu Rout v. State of Odisha, 2020 SCC OnLine Ori 878.
23. TU, RE v. Google LLC, Case C-460/20, ECLI:EU:C:2022:962 (CJEU).
24. Węgrzynowski and Smolczewski v. Poland, App. No. 33846/07 (ECtHR, 2013).
25. Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd., 2019 SCC OnLine Del 8494.

Statutes and legislative instruments

1. California Consumer Privacy Act of 2018; California Privacy Rights Act of 2020; California Delete Act (S.B. 362, 2023); Cal. Bus. & Prof. Code s. 22581.
2. Charter of Fundamental Rights of the European Union, [2012] OJ C326/391.
3. Civil Code of the People's Republic of China (2020); Personal Information Protection Law of the People's Republic of China (2021).
4. Digital Personal Data Protection Act, 2023 (India); Digital Personal Data Protection Rules, 2025 (India); Information Technology Act, 2000; Right to Information Act, 2005; Personal Data Protection Bill, 2019 (Bill No. 373 of 2019).
5. Directive 95/46/EC, [1995] OJ L281/31.
6. Fair Credit Reporting Act, 15 U.S.C. s. 1681 et seq.
7. Federal Law No. 264-FZ of 13 July 2015 (Russian Federation).
8. Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 (Brazil).
9. Personal Information Protection Act (South Korea).
10. Quebec, Act respecting the protection of personal information in the private sector, CQLR c P-39.1.
11. Regulation (EU) 2016/679 (GDPR), [2016] OJ L119/1; Regulation (EU) 2022/2065 (Digital Services Act), [2022] OJ L277/1.

Reports, guidelines and regulatory materials

1. Article 29 Data Protection Working Party, Guidelines on the Implementation of the CJEU Judgment in Google Spain, WP 225 (2014).
2. Commission nationale de l'informatique et des libertés, Blockchain and the GDPR (2018).
3. Committee of Experts under Justice B.N. Srikrishna, A Free and Fair Digital Economy (2018).
4. European Data Protection Board, Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR (Part 1), v. 2.0 (2020).
5. European Data Protection Board, Opinion 28/2024 on AI Models (2024).
6. Garante per la protezione dei dati personali (Italy), Order of 30 March 2023 (OpenAI).
7. Korea Communications Commission, Guidelines on the Right to Request Access Restriction of Personal Internet Postings (2016).
8. The Advisory Council to Google on the Right to be Forgotten, Final Report (2015).