

The Right to be Forgotten in the Digital Age: A Comparative Analysis Between Spain and Peru

El derecho al olvido en la era digital: un análisis comparativo entre España y Perú

 Natalia Ivett Arbildo Pérez*, Universidad Nacional de Trujillo, Perú,
jniarbildo@unitru.edu.pe

 Anthony Rolando Medina Rivas Plata, Universidad Nacional Toribio Rodríguez de
Mendoza, Perú, docente409@untrm.edu.pe

* Corresponding author

Abstract

The right to be forgotten has become one of the most relevant legal responses to the indefinite retention of personal information online. This article analyzes its content, limits, and conditions for its exercise from a comparative perspective between Spain and Peru. Methodologically, it combines a doctrinal review of open-access academic literature with a normative and jurisprudential analysis. The study argues that the right to be forgotten is not equivalent to erasing history or a general power of censorship, but rather a right to protect personal data aimed, above all, at limiting the disproportionate and targeted search of inaccurate, decontextualized, irrelevant, or excessive information. In Spain, the model has received explicit recognition and relatively stable criteria based on the GDPR, Organic Law 3/2018, and the Costeja case law. In Peru, although Law 29733 does not explicitly address it, the current framework has evolved through administrative regulations, constitutional jurisprudence, and the regulations approved by Supreme Decree 016-2024-JUS, which incorporates de-indexation. It is concluded that the Peruvian system still requires more precise legislative formulation and a more consistent balancing test against freedom of expression.

Keywords: Right to be Forgotten; Personal Data Protection; Search Engines; Freedom Of Expression; Deindexing.

Resumen

El derecho al olvido se ha convertido en una de las respuestas jurídicas más relevantes ante la conservación indefinida de datos personales en Internet. Este artículo analiza su contenido, sus límites y las condiciones para su ejercicio desde una perspectiva comparativa entre España y Perú. Metodológicamente, combina una revisión doctrinal de la literatura académica de acceso abierto con un análisis normativo y jurisprudencial. El estudio sostiene que el derecho al olvido no equivale a borrar la historia ni a un poder general de censura, sino que es un derecho a la protección de los datos personales destinado, sobre todo, a limitar la búsqueda desproporcionada y selectiva de información inexacta, descontextualizada, irrelevante o excesiva. En España, el modelo ha recibido un reconocimiento explícito y criterios relativamente estables basados en el RGPD, la Ley Orgánica 3/2018 y la jurisprudencia del caso Costeja. En Perú, aunque la Ley 29733 no lo aborda explícitamente, el marco actual ha evolucionado a través de reglamentos administrativos, jurisprudencia constitucional y las normas aprobadas por el Decreto Supremo 016-2024-JUS, que incorpora la desindexación. Se concluye que el sistema peruano aún requiere una formulación legislativa más precisa y una prueba de ponderación más coherente frente a la libertad de expresión.

Palabras Clave: Derecho al Olvido; Protección de Datos Personales; Motores de Búsqueda; Libertad de Expresión; Desindexación.

Introduction

Digital memory has altered the relationship between time, reputation, and access to information. In the analog world, an old news item could remain in physical archives without causing intense and lasting harm to the person involved. However, on the internet, automated indexing, name-based searches, and the constant replication of content transform past data into ubiquitous, easily accessible, and potentially decontextualized information. This technological shift explains why the so-called right to be forgotten has gone from being a doctrinal debate to becoming a central institution of contemporary data protection law (Corral Talciani, 2017; Moreno Bobadilla, 2019).

However, the right to be forgotten cannot be understood as an unlimited power to erase true facts from the public sphere. Its legal formulation raises a structural tension between informational self-determination, privacy, honor, freedom of expression, the right to inform, and the public interest in preserving the memory of relevant events. Comparative literature insists that the issue is not about choosing abstractly between privacy and information, but rather about defining criteria for weighing information to distinguish between information whose digital persistence is legitimate and that whose massive and targeted exposure becomes disproportionate over time (Leturia, 2016; Muñoz, 2015; Valdivia Aguilar, 2022).

The aim of this article is to examine the content of the right to be forgotten and compare its reception in Spain and Peru. This comparison is useful because the Spanish model, framed within the European Union, represents one of the most developed formulations of the right to be forgotten, especially since the case of Google Spain SL and Google Inc. v. Spanish Data Protection Agency and Mario Costeja González, decided by the Court of Justice of the European Union on May 13, 2014 (Court of Justice of the European Union, 2014). Also, because the Peruvian case reveals a more fragmented normative and jurisprudential process, although it is now more developed than some previous approaches suggested, due to the entry into force of the new Regulations of Law 29733 on March 31, 2025 (Ministerio de Justicia y Derechos Humanos, 2024).

The central argument is that the right to be forgotten should be understood as a specific power for the protection of personal data, primarily aimed at limiting the disproportionate and targeted access of certain information online, not as an autonomous and unrestricted right to rewrite the past. Based on this premise, Spain offers an explicit and relatively well-established model, while Peru currently has a relevant constitutional, administrative, and regulatory framework, but still lacks a legislative and jurisprudential structure as detailed as Spain's. This article is developed through a doctrinal review of open-access academic literature and an analysis of relevant regulations and case law.

Conceptual Delimitation of the Right to be Forgotten

Legal scholars are not unanimous regarding the nature of the right to be forgotten. One perspective presents it as a contemporary derivation of the right to privacy; another situates it within the fundamental right to the protection of personal data; and a third argues that, rather than a new autonomous right, it is a specific technique for safeguarding against the digital persistence of personal information (Corral Talciani, 2017; Leturia, 2016; González Rincón, 2020). This last approach is particularly useful because it avoids excessive conceptual expansion and, at the same time, explains why its scope is related to the circulation of personal data in digital environments.

In operational terms, the right to be forgotten manifests itself primarily on three levels. The first is the deletion or cancellation of data when its processing lacks a legitimate basis or is no longer necessary. The second is delisting, that is, the exclusion of a person's name from search results. The

third is the updating or contextualization of information when total deletion would be disproportionate, but the current presentation creates an inaccurate or incomplete image of the affected person. This distinction is important because, as legal scholars have emphasized, not every digital memory problem requires the disappearance of content from its original source; in many cases, it suffices to limit its visibility by name or incorporate subsequent information that prevents a misleading interpretation of the past (Maqueo Ramírez, 2019; Ortiz Mesías & Viollier, 2021).

Thus, the right to be forgotten should not be confused with the right to erase historically occurring events or with a power of private censorship. Its legal justification lies, rather, in preventing the logic of search engines from transforming old, inaccurate, irrelevant, or decontextualized facts into a kind of permanent public identity. The harm does not necessarily stem from the original content, but from its new form of circulation: a search by name offers a structured, persistent, and simplified profile of the person, which increases the impact on their private life, social opportunities, and personal development (Moreno Bobadilla, 2019; Muñoz, 2015).

Comparative legal scholarship also highlights that time plays a central, but not exclusive, role. The passage of time does not, in itself, erase the public relevance of information, although it does necessitate its reevaluation. A fact may have been truthful and relevant at the time of its publication and yet become unsuitable for widespread public exposure years later. This occurs, for example, when the news concerns debts that have already been paid, closed cases, unconfirmed accusations, or minor events that are no longer of current interest. However, when it comes to serious crimes, acts related to corruption, the exercise of power, public safety, or public figures, the public interest in accessing the information may remain or even prevail (Cetina Presuel & Gutiérrez Atala, 2022; Leturia, 2016).

From a dogmatic perspective, the right to be forgotten primarily protects natural persons, because the core of the issue is linked to dignity, privacy, reputation, and the free development of personality. Information concerning legal entities can be protected through other means, but it is not based on the same anthropocentric foundation that characterizes this right. To that extent, the right to be forgotten appears closely related to the processing of identifiable data and how such data is linked to a person's name online (González Rincón, 2020; Maqueo Ramírez, 2019).

Privacy, Data Protection and Freedom of Expression

The central problem with the right to be forgotten lies not only in defining what information is bothersome or harmful to a person, but also in establishing when it is legally legitimate to limit its dissemination or accessibility. This is because this right operates at the intersection (and sometimes point of conflict) between privacy and freedom of expression. If formulated too broadly, it risks becoming a silencing mechanism; if formulated too narrowly, it can render data protection in the digital sphere meaningless (Muñoz, 2015; Valdivia Aguilar, 2022).

Privacy and data protection are not equivalent, although they are closely related. The former protects a sphere of personal privacy and autonomy; the latter grants control over the collection, circulation, use, and destination of information that identifies a person. On the internet, this difference becomes especially relevant: information may not belong to the most intimate core of private life, and yet its massive, indexed, and permanent processing can still be harmful to the data subject. Hence, several authors insist that the right to be forgotten should be considered primarily from the perspective of informational self-determination and not only from that of traditional privacy (Franco García & Quintanilla Perea, 2020; Moreno Bobadilla, 2019).

On the other hand, freedom of expression and the right to information fulfill a crucial institutional function in democratic societies. They protect public debate, criticism, journalistic investigation, and the preservation of news archives. From this perspective, any form of suppression or de-indexing can affect not only those who publish the information but also the public interested in accessing it. The debate, therefore, is not limited to a bilateral conflict between individuals and search engines but also involves journalists, media outlets, digital archives, and internet users (Cetina Presuel & Gutiérrez Atala, 2022; Ortiz Mesías & Viollier, 2021).

The specialized literature has proposed some relatively consistent weighting criteria. These include: the accuracy of the information; the timeliness or relevance of the news story; the seriousness of the event; the public or private role of the person involved; the connection of the information to debates of collective importance; the existence of a final conviction or, conversely, mere accusations or inconclusive investigations; and how the information appears in search engines, especially when the search is conducted by proper name (Leturia, 2016; Muñoz, 2015). These criteria allow us to distinguish between the legitimate preservation of public memory and disproportionate digital exposure.

The field of journalism has highlighted an additional point: the difference between memory and archive. Journalistic archives are essential for reconstructing historical events, monitoring power, and ensuring the integrity of the information record. However, contemporary indexing changes the nature of this archive, as it no longer requires contextual searching but instead offers immediate, hierarchical, and easily reconfigurable results. Therefore, some authors propose less drastic solutions than deletion, such as partial anonymization, news updates, the addition of supplementary information, or de-indexing limited to name-based searches (Cetina Presuel & Gutiérrez Atala, 2022).

In the inter-American sphere, the debate has been particularly sensitive. Some legal scholars warn that an uncritical importation of the European model could generate restrictions incompatible with regional standards of freedom of expression. From this perspective, the right to be forgotten would only be admissible if its design incorporates strict safeguards against indirect censorship and if the balancing of interests recognizes the importance of the principle of maximum disclosure when matters of public interest are at stake (Franco García & Quintanilla Perea, 2020; Valdivia Aguilar, 2022). This caution is especially important in Latin America, where the fight against corruption, organized crime, and abuses of power gives access to information a unique institutional relevance.

The Spanish Model

Spain is the most influential reference point in the Spanish-speaking world for the study of the right to be forgotten. The turning point was the case of Google Spain SL and Google Inc. v. Spanish Data Protection Agency and Mario Costeja González (case C-131/12), decided by the Court of Justice of the European Union on May 13, 2014 (Court of Justice of the European Union, 2014). The case originated when Mario Costeja requested that links to 1998 publications relating to a property auction due to social security debts no longer appear on Google. The information had been lawfully published at the time, but the affected party argued that the matter had been resolved and was no longer relevant.

The significance of the ruling lies in several points. First, the Court of Justice held that a search engine operator processes personal data when it collects, records, organizes, and makes available personal information contained on third-party websites. Second, it affirmed that the search engine operator can be held responsible for this processing, even if it is not the original author of the content. Third, it maintained that, under certain circumstances, the affected individual can request the removal of links from the search results obtained using their name, even if the information remains lawfully published

on the original source. With this, the Court clarified that the legal issue was not limited to the initial legality of the publication but also extended to the new form of accessibility generated by the search engine (González Rincón, 2020; Maqueo Ramírez, 2019; Martínez Otero, 2015).

Legal scholars have observed that Costeja did not recognize a “right to erase history,” but rather a right to object to nominative indexing when the persistence of the link between name and information is no longer compatible with the data protection framework. In other words, the main effect of the case was de-indexing, not the removal of the news item from the media outlet's archive. This distinction remains fundamental to understanding the subsequent evolution of the European model (Corral Talciani, 2017; Leturia, 2016).

The next step was regulatory. Regulation (EU) 2016/679, known as the General Data Protection Regulation (GDPR), enshrines in its Article 17 the right to erasure or “right to be forgotten” (European Parliament and Council of the European Union, 2016). This recognizes the data subject's right to obtain from the controller the erasure of personal data without undue delay when, among other circumstances, the data are no longer necessary for the purpose of the processing, consent is withdrawn, or the processing is unlawful. At the same time, the article itself establishes explicit limitations, particularly when the processing is necessary for exercising the right to freedom of expression and information, compliance with legal obligations, reasons of public interest, or for archiving, research, or legal defense purposes.

In Spain, Organic Law 3/2018 further developed this framework. Article 93 specifically regulates the right to be forgotten in internet searches and recognizes the right of every person to have search engines remove from the results lists obtained from their name any links containing information that is inadequate, inaccurate, irrelevant, outdated, or excessive, or that has become so over time. Article 94 extends this logic to social networks and equivalent services. The law thus confirms the key idea of the Spanish model, that the right to be forgotten operates primarily on the accessibility of data in digital environments and not necessarily on the original existence of the content (Jefatura del Estado, 2018).

This design has several advantages. First, it distinguishes between deletion and de-indexing. Second, it incorporates relatively clear normative criteria: suitability, accuracy, relevance, updating, excess, time elapsed, and public interest. Third, it expressly acknowledges that searches by proper name are particularly harmful because they allow for the construction of a digital identity that can be easily exploited by third parties. Fourth, it preserves an explicit space for freedom of information, so that the weighting is not always presumed in favor of the requester (Martínez Otero, 2015; Moreno Bobadilla, 2019).

However, the Spanish model does not provide automatic or absolute protection for the claimant. Subsequent practice shows that de-indexing depends on the specific circumstances. When the information is of current public interest, is linked to public figures, or is necessary for democratic debate, the request may be rejected. Even in certain cases, the most balanced response is not the removal of the result, but rather the contextualization of the available information to reflect the subsequent evolution of the case. This reveals a significant maturity of the system: the right to be forgotten is conceived as a mechanism for fine-tuning the balance between digital memory, data protection, and freedom of information, not as an instrument of indiscriminate erasure.

The Peruvian Model

In Peru, the starting point remains constitutional. Article 2, paragraph 6, of the Constitution recognizes the right to prevent public or private computer services, whether computerized or not, from providing information that affects personal and family privacy. This is further supported by Article 2, paragraph 7, which protects privacy, honor, and reputation (Congreso Constituyente Democrático, 1993). Based on this, Law 29733, the Personal Data Protection Law, established the general framework for data protection in the country in 2011 (Congreso de la República del Perú, 2011). However, the law did not expressly use the expression “right to be forgotten,” which for years led to the argument that its recognition depended on a broad interpretation of the rights of cancellation, objection, and rectification (Franco García & Quintanilla Perea, 2020).

That diagnosis, while correct in its origin, now requires updating. Indeed, the new Regulations of Law 29733, approved by Supreme Decree No. 016-2024-JUS and in force since March 31, 2025, introduced significant changes (Ministerio de Justicia y Derechos Humanos, 2024). Article 3, paragraph 7, defines de-indexing as the process by which a URL or specific content is removed or excluded from search engine results. Furthermore, Article 82 regulates the deletion or cancellation of data when it is no longer necessary or relevant, and Article 86.5 stipulates that, when personal data is processed online, the exercise of the right to object may include de-indexing. This means that the Peruvian legal system can no longer be simply described as lacking regulatory tools to address the digital exposure of personal data.

Nevertheless, Peruvian development remains less explicit and less refined than its Spanish counterpart. Law 29733 does not contain specific regulations on the right to be forgotten in internet searches, similar to Articles 93 and 94 of the Spanish Organic Law. Peruvian progress has resulted more from a combination of constitutional grounds, administrative regulations, the activities of the National Authority for the Protection of Personal Data, and constitutional jurisprudence. It is, therefore, a model of indirect or functional recognition, not a detailed legislative enshrinement (Franco García & Quintanilla Perea, 2020).

Administrative practice was important even before the new regulations. In Directorial Resolution No. 045-2015-JUS/DGPDP, the administrative authority upheld a citizen's complaint and ordered Google to block certain information related to a criminal case that had already been dismissed. The significance of this decision lies in its recognition that the search engine's activity involves the processing of personal data and, consequently, may be subject to protective obligations. Subsequent decisions, such as Directorial Resolution No. 2377-2018-JUS/DGTAIPD-DPDP, emphasized the importance of the passage of time, the continued journalistic interest, and the potential status of the affected individual as a public figure (Dirección de Protección de Datos Personales, 2018; Dirección General de Protección de Datos Personales, 2015).

The most significant legal precedent is the Constitutional Court's ruling in Case No. 03041-2021-PHD/TC, Miguel Arévalo Ramírez (Judgment 119/2022). In its eleventh paragraph, the Court stated that the right to be forgotten guarantees the elimination, suppression, or removal of information related to personal data that, normally linked to a person's name, can be found through search engines and that, even if it was accurate at the time, ceases to be so (or ceases to be entirely so) due to new factual or legal circumstances. The Court linked this protection to informational self-determination, honor, good reputation, privacy, and the free development of personality (Tribunal Constitucional del Perú, 2022).

However, the Court also emphasized that the right to be forgotten is not absolute and can conflict with freedom of information. In paragraphs 13 and 14, it expressly indicated this need for harmonization and ultimately rejected the claim because the disseminated information related to drug trafficking and terrorism investigations, matters it considered to be of the highest relevance and public interest. Furthermore, it noted that the plaintiff had not proven the information to be false in the required manner. The ruling, therefore, is ambivalent: it conceptually recognizes the right, but at the same time adopts a restrictive solution regarding matters of high public interest.

The main lesson from the Peruvian case is twofold. On the one hand, it confirms that the right to be forgotten now has sufficient constitutional and jurisprudential recognition to be addressed in habeas data proceedings. On the other hand, it demonstrates that the balancing of rights in Peru is still in a consolidation phase. Unlike the Spanish model, where nominative de-indexing has more clearly defined normative criteria, the Peruvian system still relies heavily on case-by-case interpretation, with greater uncertainty surrounding the standards of admissibility, the burden of proof on the applicant, and the relationship between personal data, freedom of information, and the social function of archives.

Comparative Analysis Between Spain and Peru

A comparison between Spain and Peru reveals structural similarities, but also crucial differences. In both systems, the right to be forgotten is linked to the protection of personal data and cannot be understood without reference to privacy and freedom of information. Likewise, search engines occupy a central position in both contexts, because the typical harm arises not simply from the existence of the content, but from its accessibility, intensified by name-based searches. However, the density of regulations and the sophistication of the balancing criteria are not equivalent.

In Spain, the right to be forgotten is expressly and specifically recognized. The GDPR regulates the right to erasure, and Organic Law 3/2018 establishes a differentiated regime for internet and social media searches. This explicitness reduces uncertainty and allows the discussion to be channeled toward relatively predictable criteria: adequacy, accuracy, relevance, currency, excessiveness, the passage of time, and public interest. In Peru, however, Law 29733 still does not expressly formulate the right to be forgotten, although the new regulations do incorporate de-indexing and allow it to be exercised through the right to object. This represents significant progress, but it still does not equate to the regulatory clarity of the Spanish system.

A second difference concerns the specific object of the protection. In Spain, the emphasis is clearly on the removal of links from search results obtained using a person's name, that is, on the dimension of delisting or name-based deindexing. In Peru, although the current regulations already recognize deindexing, the conceptual framework remains more closely tied to the traditional rights of cancellation and objection. This can lead to interpretive overlaps between data suppression, content blocking, removal of results, and information updates, making it more difficult to precisely define the appropriate measure in each case (Franco García & Quintanilla Perea, 2020; González Rincón, 2020).

The third difference relates to the balance between data protection and freedom of information. The Spanish model starts from the premise that a person can request de-indexing even when the source content remains lawful but requires an evaluation of the nature of the information, the time elapsed, the sensitivity of the data, and the public role of the affected individual. In Peru, recent constitutional jurisprudence has shown a strong inclination to preserve dissemination when the information is linked to serious crimes, politics, or public safety. This caution is understandable within the Latin American context, but it risks leaving intermediate cases underprotected, where the impact is serious and the

current public relevance is low or questionable (Valdivia Aguilar, 2022; Ortiz Mesías & Viollier, 2021).

A fourth difference lies in the institutional process. In Spain, the path from requesting the data controller to filing a complaint with the data protection authority and potentially undergoing judicial review is more established. In Peru, although there is also an administrative route before the ANPD (National Data Protection Authority) and a constitutional route through habeas data, the coexistence of these procedures does not yet offer such a stable framework. The requester may face doubts about the competent authority, the exact remedy to request, and how to prove the current impropriety of the dissemination.

Despite these differences, there is a significant convergence: in both Spain and Peru, the right to be forgotten can no longer be understood as simply the removal of content. In both systems, the central issue is the relationship between names, search engines, digital accessibility, and proportionality. Furthermore, both legal systems recognize that the legal response must distinguish between legitimate social memory and excessive name-based exposure. This convergence suggests that Peru is in a stage of functional approximation to the European model, although it has not yet reached the same level of regulatory precision. The following table summarizes the main points of comparison between both models:

Table 1

Comparative Framework of the Right to Be Forgotten

<i>Aspect</i>	<i>Spain</i>	<i>Peru</i>
<i>Main source</i>	<i>GDPR, Article 17, and Organic Law 3/2018, Articles 93 and 94.</i>	<i>Constitution, Law 29733 and Regulations approved by DS 016-2024-JUS; administrative and jurisprudential development.</i>
<i>Object of protection</i>	<i>Suppression and, above all, de-indexing of results linked to the affected person's name.</i>	<i>Deletion, cancellation and opposition; from 2025 the regulation expressly includes de-indexing.</i>
<i>Eligibility criteria</i>	<i>Suitability, accuracy, relevance, updating, excess, time and public interest.</i>	<i>Need or relevance of the data, opposition to processing on the internet, time, accuracy and public relevance.</i>
<i>Level of consolidation</i>	<i>Express and relatively stable model.</i>	<i>Functional and consolidating model.</i>
<i>Balance with freedom of information</i>	<i>Explicit weighting with reference to the public role of the affected party and the public interest.</i>	<i>Even more case-by-case consideration; the public interest may prevail with particular force in cases of serious crime.</i>

Note. Own elaboration.

In summary, Spain exhibits a more explicit and specialized protection regime, while Peru has moved towards a functional formulation of the right to be forgotten, especially since the regulatory shift of 2025, but still needs greater regulatory density and more uniform decision criteria.

Comparative Analysis Between Spain and Peru

Peru's main challenge is to transform the current indirect recognition into a clearer and more predictable legal framework. The regulatory incorporation of de-indexation has been an important step forward, but it does not replace the need for more precise legislation. Explicit recognition in Law 29733 would help define its scope, obligated parties, grounds for application, procedural safeguards, and possible measures, preventing the institution from relying solely on constitutional or administrative inferences.

A second challenge is to construct a specific weighting test. Comparative experience suggests that it is not enough to generically invoke public interest or privacy. It is necessary to articulate concrete criteria: accuracy of the data; degree of currency; public role of the affected party; nature of the act; existence of a final conviction or simple investigation; passage of time; purpose of the archive; actual impact on the life of the applicant; and possibility of less intensive measures than deletion, such as updating, contextualization or limited de-indexing (Cetina Presuel & Gutiérrez Atala, 2022; Leturia, 2016; Muñoz, 2015).

A third challenge is preventing the right to be forgotten from being used as a mechanism for private censorship. The intervention of search engines and digital platforms cannot translate into opaque, purely business-driven decisions devoid of any challenge. It is necessary to design minimum due process rules: sufficient justification, notification when appropriate, the possibility of review, and differentiation between information of public interest and manifestly harmful or inaccurate content. Data protection must not become a parallel avenue for removing legitimate scrutiny from public affairs (Ortiz Mesías & Viollier, 2021; Valdivia Aguilar, 2022).

A fourth challenge is addressing particularly sensitive categories. Information about minors, victims, individuals acquitted or under investigation without formal charges, as well as data disseminated for purely sensationalist purposes, requires enhanced protection standards. Similarly, the contemporary digital environment presents new problems related to automated profiling, algorithmic replication, permanent data capture, and the cross-border circulation of content. Therefore, the regulation of the right to be forgotten should not be limited to the traditional logic of search engines but rather engage with a much more complex digital ecosystem.

Ultimately, the fundamental challenge is cultural and institutional. The right to be forgotten can only function properly if it is embedded within a broader policy of personal data protection, digital literacy, journalistic responsibility, and public transparency. Neither the maximalist approach of erasure nor the rigidity of absolute memory offers satisfactory solutions. What is needed is an institutional framework capable of distinguishing between the legitimate preservation of collective memory and unnecessary digital exposure that ends up fixing a person in a past that no longer describes, or no longer adequately describes, their current situation.

Conclusions

The right to be forgotten is a legal response to the changes brought about by digital memory. Its purpose is not to deny history, but to correct the disproportionate effects of the permanent, massive, and nominative accessibility of personal information on the internet. Therefore, it is best understood not as an absolute right to erase past events, but as a specific protective measure within the broader right to the protection of personal data.

The Spanish model shows a more robust development. The Costeja case, Article 17 of the GDPR, and Articles 93 and 94 of Organic Law 3/2018 form a regulatory and jurisprudential structure that clearly distinguishes between deletion and de-indexing, recognizes the role of search engines, and requires weighing the public interest, the nature of the data, the time elapsed, and the social role of the data subject.

The Peruvian case presents a more nuanced scenario than could be described years ago. Although Law 29733 does not expressly enshrine the right to be forgotten, the current legal framework has advanced significantly: administrative practice recognized the impact of search engines early on; the Constitutional Court defined the right to be forgotten in the Miguel Arévalo Ramírez case; and the Regulations approved by Supreme Decree No. 016-2024-JUS expressly incorporated de-indexing and linked it to the right to object online. In this sense, it is no longer accurate to assert that there is no legal basis whatsoever for this concept in Peru.

Despite this, the Peruvian system still requires greater legislative precision, more uniform standards for weighing grievances, and procedural safeguards to prevent both the underprotection of the affected individual and private censorship of information of public interest. The challenge is not to mechanically import the European model, but to adapt it to a constitutional framework that simultaneously preserves informational self-determination, freedom of expression, and the demands of democratic debate.

Disclosures

Funding

Self-Funded.

Conflict of Interest

The authors declare they have not conflict of interests.

Use of AI

Google Translate was used for language editing (Spanish/English) and ChatGPT for proofreading and the elaboration of the list of References in APA 7. The authors reviewed the manuscript and assume full responsibility for it.

References

- Cetina Presuel, R., & Gutiérrez Atala, F. J. (2022). The limits of memory and the news: Archival journalism, law, ethics, and the right to be forgotten. *Revista de Comunicación*, 21(1), 67–92. <https://doi.org/10.26441/RC21.1-2022-A4>
- Congreso Constituyente Democrático. (1993). *Constitución Política del Perú*. <https://www.gob.pe/institucion/presidencia/informes-publicaciones/196158-constitucion-politica-del-peru>
- Congreso de la República del Perú. (2011). *Ley N.º 29733, Ley de Protección de Datos Personales*. <https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733>

- Corral Talciani, H. (2017). El derecho al olvido en internet: Antecedentes y bases para su configuración jurídica. *Revista Jurídica Digital UANDES*, 1(1), 43–66. <https://doi.org/10.24822/rjduandes.0101.3>
- Court of Justice of the European Union. (2014). *Judgment of the Court (Grand Chamber) in Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (ECLI:EU:C:2014:317). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131>
- Dirección de Protección de Datos Personales. (2018). *Resolución Directoral N.º 2377-2018-JUS/DGTAIPD-DPDP. Expediente N.º 011-2018-PTT.* <https://cdn.www.gob.pe/uploads/document/file/605996/RD-2377-2018-DPDP.pdf>
- Dirección General de Protección de Datos Personales. (2015). *Resolución Directoral N.º 045-2015-JUS/DGPDP. Expediente N.º 012-2015-PTT.* https://hiperderecho.org/wp-content/uploads/2016/06/datos_personales_google_olvido_1.pdf
- European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.* <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Franco García, D., & Quintanilla Perea, A. (2020). La protección de datos personales y el derecho al olvido en el Perú. A propósito de los estándares internacionales del Sistema Interamericano de los Derechos Humanos. *Derecho PUCP*, (84), 271–299. <https://doi.org/10.18800/derechopucp.202001.009>
- González Rincón, A. C. (2020). Aproximación a la configuración jurídica del derecho al olvido en Internet: Un análisis a partir de la sentencia del TJUE vs Google. *Boletín Mexicano de Derecho Comparado*, 1(156), 1449–1475. <https://doi.org/10.22201/ijj.24484873e.2019.156.15159>
- Jefatura del Estado. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* *Boletín Oficial del Estado*, 294, 119788–119857. <https://www.boe.es/eli/es/lo/2018/12/05/3/con>
- Leturia, F. J. (2016). Fundamentos jurídicos del derecho al olvido: ¿Un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos derechos fundamentales? *Revista Chilena de Derecho*, 43(1), 91–113. <https://doi.org/10.4067/S0718-34372016000100005>
- Maqueo Ramírez, M. S. (2019). El derecho al olvido digital desde la perspectiva de la Unión Europea y la viabilidad de su extrapolación al caso de México. *Latin American Law Review*, 1(3), 79–97. <https://doi.org/10.29263/lar03.2019.04>
- Martínez Otero, J. M. (2015). El derecho al olvido en Internet: Debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja. *Revista de Derecho Político*, (93), 103–142. <https://doi.org/10.5944/rdp.93.2015.15139>
- Ministerio de Justicia y Derechos Humanos. (2024). *Decreto Supremo N.º 016-2024-JUS, Decreto Supremo que aprueba el Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales.* *Diario Oficial El Peruano.* <https://busquedas.elperuano.pe/dispositivo/SE/2349653-1>
- Moreno Bobadilla, Á. (2019). The right to be forgotten: A gap between Europe and United States. *Revista de Comunicación*, 18(1), 259–276. <https://doi.org/10.26441/RC18.1-2019-A13>

- Muñoz, A. M. (2015). Eliminación de datos personales en internet: El reconocimiento del derecho al olvido. *Revista Chilena de Derecho y Tecnología*, 4(2), 215–261. <https://doi.org/10.5354/0719-2584.2015.37426>
- Ortiz Mesías, L., & Viollier, P. (2021). Repensando el derecho al olvido y la necesidad de su consagración legal en Chile. *Revista Chilena de Derecho y Tecnología*, 10(1), 77–109. <https://doi.org/10.5354/0719-2584.2021.56482>
- Tribunal Constitucional del Perú. (2022). *Sentencia 119/2022. Expediente N.º 03041-2021-PHD/TC, Miguel Arévalo Ramírez*. <https://tc.gob.pe/jurisprudencia/2022/03041-2021-HD.pdf>
- Valdivia Aguilar, T. G. (2022). Nuevos derechos en el sistema interamericano de derechos humanos: ¿Debe importarse el “derecho al olvido” de la Unión Europea? *Anuario Mexicano de Derecho Internacional*, 22(22), 431–476. <https://doi.org/10.22201/ijj.24487872e.2022.22.16958>