

THE RIGHT TO BE FORGOTTEN VS. THE RIGHT TO HISTORY: A COMMUNICATIONAL CONFLICT BETWEEN PERSONAL DATA PROTECTION AND THE PRESERVATION OF PUBLIC DIGITAL ARCHIVES

Andrii Lyseiuk

National Academy of the Security Service of Ukraine

Kyiv, Ukraine

<https://orcid.org/0000-0002-9026-1188>

andrii_lyseiuk@sci-univ.com

ABSTRACT. This article examines the escalating legal and philosophical conflict between the individual’s right to be forgotten (RTBF) and the societal imperative to preserve a complete and accessible historical record, conceptualized here as the “right to history.” The central problem is framed not as a simple clash of legal principles but as a profound communicational conflict over who controls the narrative of the past in an age of digital permanence. Employing a methodology that combines comparative legal analysis with a communicational framework approach, this article dissects the legal architecture of the RTBF, with a particular focus on the European Union’s General Data Protection Regulation (GDPR) (European Parliament and Council of the European Union, 2016). It argues that current legal frameworks, while aiming to protect individual dignity, pose significant challenges to the integrity of public digital archives, thereby threatening journalistic freedom, the principle of open justice, and the core mission of cultural heritage institutions (Vavra, 2018). The analysis reveals how the RTBF has evolved from a tool for mediating access to information into a mechanism for altering the primary source material of history itself. The article concludes by rejecting a simple binary opposition between these rights and proposes a nuanced, context-aware balancing framework. This multi-factor framework offers specific criteria—including the nature of the information, the role of the individual, the passage of time, the original context of publication, and the medium of the archive—to reconcile the legitimate claims of individual data subjects with the non-negotiable societal need for a preserved, searchable, and reliable past.

Keywords: Right to be Forgotten, Right to History, GDPR, Digital Archives, Data Protection, Freedom of Expression, Legal Communication.

1. INTRODUCTION

1.1 The Digital Panopticon and the Erasure Imperative: A Contemporary Case Study

In July 2023, the Grand Chamber of the European Court of Human Rights (ECtHR) delivered a judgment that sent a tremor through newsrooms, archives, and libraries across Europe. In the case of *Hurbain v. Belgium*, the court upheld a decision compelling the publisher of *Le Soir*, a prominent Belgian newspaper, to anonymize a decades-old article in its digital archive (ARTICLE 19, 2016). The article, originally published in 1994, detailed a fatal car accident for which a doctor had been found responsible (ARTICLE 19, 2016; *Hurbain v. Belgium*, 2023). In 2008, the newspaper digitized its archives, making the article accessible online. Two years later, the doctor, arguing the article’s continued availability was damaging his reputation, requested its removal or anonymization (*Hurbain v. Belgium*, 2023). The

final ruling in his favor marked a pivotal escalation in the war over memory. It moved the battleground beyond the now-familiar territory of delisting search engine results to the direct, retroactive alteration of the historical record itself (ARTICLE 19, 2016; Hurbain v. Belgium, 2023). This case serves as a perfect microcosm of the intractable conflict at the heart of this article: the collision between an individual's desire to escape the perpetual gaze of the digital panopticon and society's need to preserve the integrity of its public archives.

The Hurbain case is not an anomaly but the logical extension of a principle that has gathered formidable legal force over the past decade. Early instances, such as the delisting of news reports from Google about a Scottish football referee, Dougie McDonald, who had lied about a penalty decision, demonstrated how public figures could leverage the nascent „right to be forgotten” (RTBF) to manage their online reputations (Hern, 2024). However, the direct editing of a newspaper's archive represents a far more profound intervention. It is a shift from a „filter” model, which merely curtails pathways to information, to an „edit” model, which alters the primary source. This evolution dramatically raises the stakes, transforming a debate about access to history into a debate about the power to rewrite it.

1.2 From Ephemeral to Eternal: The Permanence of Information in the Digital Age

The demand for a right to be forgotten is a direct consequence of a fundamental technological transformation. In the pre-digital era, information was largely ephemeral. A newspaper article yellowed and faded, a local broadcast was fleeting, and records of past indiscretions were often buried in dusty courthouse basements, protected by what legal scholars have termed „practical obscurity” (Bollinger & Callamard, 2021). The effort required to unearth past information was a natural check on its persistence. The internet has obliterated this condition. It has converted information from a state of natural decay to one of perpetual existence (Rosen, 2012; „The Right to be Forgotten,” n.d.). Every photograph, status update, news report, and public record now lives „forever in the cloud,” instantly accessible and searchable from anywhere in the world (Rosen, 2012; „The Right to be Forgotten,” 2025).

This digital permanence has created a new kind of prison, a „digital panopticon” where individuals can be „perpetually or periodically stigmatized as a consequence of a specific action performed in the past” („Right to be forgotten,” n.d., p. 231). The internet has become, in effect, a universal and disorganized public archive, one that never forgets and rarely contextualizes (Rosen, 2012). It is this technological reality—the shift from an ephemeral to an eternal public record—that has fueled the legal and ethical demand for an „eraser,” a mechanism to reclaim control over one's digital past and shape one's future narrative (Rosen, 2012).

1.3 The Core Polemic: A Communicational Struggle for Narrative Control

This article posits that the conflict between the right to be forgotten and the preservation of public archives is not merely a technical legal dispute to be resolved by placing one right higher in a hierarchy than another. It is, more fundamentally, a communicational conflict. It is a struggle over who wields the authority to write, edit, curate, and ultimately erase the narratives that constitute our collective memory and historical record. This is a clash between

two potent and legitimate sets of fundamental rights. On one side stands the individual's right to dignity, privacy, and data protection—the right to informational self-determination. On the other stands the collective's right to freedom of expression, the right to receive and impart information, and the right to access a complete and unvarnished historical account („Right to be forgotten,” n.d.; Rosen, 2012; De Baets, 2016; Faisal, 2021).

The core question is this: Should history be an immutable record, open to all for interpretation and scrutiny, or should it be a mutable narrative, subject to editing and redaction by the individuals it depicts? This is not just a question for lawyers and judges; it strikes at the heart of how we, as a society, understand the relationship between truth, memory, accountability, and forgiveness in the digital age. The resolution of this communicational struggle will determine the very nature of the public record for generations to come.

1.4 Conceptual Foundations

To analyze this conflict, a clear understanding of the two principal concepts is essential.

The Right to be Forgotten (RTBF) is the right of an individual to request the removal of personal data from online platforms, databases, and, most notably, search engine results (Rosen, 2012; Cloudflare, n.d.). It is not an absolute right to erase all traces of one's past. Rather, it applies under specific conditions, typically when the information in question is deemed „inadequate, irrelevant or no longer relevant, or excessive” in relation to the purposes for which it was processed („Right to be forgotten,” n.d.).

Its modern legal genesis lies in the 2014 landmark ruling of the Court of Justice of the European Union (CJEU) in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (St. Mary's Law Journal, 2016; „The Right to be Forgotten,” 2025; Boto, 2014). This judicial precedent was subsequently codified and expanded within Article 17 of the EU's General Data Protection Regulation (GDPR), where it is formally titled the „right to erasure” (Hurbain v. Belgium, 2023; „Right to be forgotten,” n.d.; „The Right to be Forgotten,” 2025; European Parliament and Council of the European Union, 2016).

Crucially, the RTBF must be distinguished from the traditional right to privacy. The right to privacy historically protects information that is not in the public domain—facts about one's private life that have not been disclosed. The RTBF, in contrast, primarily concerns revoking or limiting public access to information that was at one point lawfully and publicly known („Right to be forgotten,” n.d.). This distinction is vital. It reframes the RTBF from being a simple shield for privacy into a sword for active reputational management. It is a tool that allows individuals to curate their public-facing narrative by pruning away undesirable elements of their past, thus moving far beyond the traditional confines of data protection into the realm of narrative control (Rosen, 2012; „Right to be forgotten,” n.d.).

Juxtaposed against the individualistic RTBF is what this article terms the „Right to History.” This is not a formally codified, singular right but a composite principle derived from a constellation of fundamental rights and societal imperatives. It is the collective right of a society to create, preserve, and access a complete, accurate, and reliable record of its past.

Its philosophical and legal underpinnings can be traced to the Universal Declaration of Human Rights (UDHR), particularly the rights to freedom of expression and information (Article 19), the right to education (Article 26), and the right to academic freedom, which is

essential for historical research (De Baets, 2009; „Responsible History,” 2008). This concept is powerfully articulated in the field of transitional justice, where the „right to know the truth about past abuses” is seen as a critical step toward justice and a bulwark against the recurrence of atrocities (De Baets, 2009; „Entangled History,” 2021).

The Right to History is not an esoteric concern for professional historians alone; it is the bedrock of democratic accountability. It empowers journalism, which provides the „first rough draft of history,” ensures the transparency of open justice, and underpins the mission of cultural archives to serve as society’s memory keepers (Mayer-Schönberger, 2011; Vavra, 2018). It is the right that protects the historical record from „amnesia and falsification” by those who would prefer a more convenient version of the past (De Baets, 2009; De Baets, 2008). This right is fundamentally collective. While individuals benefit from an accessible and truthful history, the right itself serves a societal function. The conflict is therefore asymmetrical: it pits an individual’s desire for personal narrative control against a collective’s structural need for an uncontrolled, authentic historical record. This asymmetry reframes an erasure request not as a mere act of privacy, but as an act that diminishes a shared public resource.

1.5 Thesis Statement

This article argues that the conflict between the ‚right to be forgotten’ and the ‚right to history’ cannot be resolved through a simple legal hierarchy of rights, but requires a dynamic, context-dependent communicational framework. This framework must move beyond the binary opposition of privacy versus speech to analyze the specific communicative functions of the information in question. It must balance an individual’s legitimate interest in dignity and informational self-determination against the non-negotiable societal necessity of a preserved, searchable, and reliable public archive, which serves as the bedrock of democratic accountability and collective memory.

1.6 Article Roadmap

The argument will proceed in five subsequent parts. Section 2 provides a deep analysis of the legal architecture of the Right to be Forgotten, tracing its origins and deconstructing its codification in the GDPR and key European court decisions. Section 3 presents the case for the imperative of history, defending the role of journalistic, judicial, and cultural archives as essential pillars of a democratic society. Section 4 conducts a comparative analysis of the divergent legal and philosophical models of the European Union and the United States, highlighting the points of friction. Section 5 moves from critique to construction, proposing a novel multi-factor reconciliatory framework designed to bring clarity and principle to the balancing act. Finally, Section 6 concludes by summarizing the findings, reflecting on the broader implications for democracy and collective memory, and suggesting avenues for future research in this critical and rapidly evolving field.

2. THE LEGAL ARCHITECTURE OF THE RIGHT TO BE FORGOTTEN

The Right to be Forgotten, as it exists today, is not a monolithic doctrine but a complex legal edifice constructed over time through judicial interpretation and legislative action. Its architecture reveals a profound shift in legal thinking, adapting traditional privacy concepts to the challenges of the digital age. Understanding this structure, from its doctrinal foundations to its procedural complexities and jurisdictional disputes, is essential to grasping its impact on the public archive.

2.1 Doctrinal Genealogy: From *Droit à l'Oubli* to Digital Erasure

The intellectual roots of the RTBF are often traced to the French concept of *le droit à l'oubli*, or the „right of oblivion“ (Rosen, 2012; „The Right to be Forgotten,” 2025). Historically, this was a relatively narrow legal principle connected to the social rehabilitation of criminals. It allowed an individual who had served their sentence and been rehabilitated to object to the prominent republication of the facts of their past conviction (Rosen, 2012). The purpose was not to erase history but to facilitate social reintegration by preventing a past mistake from perpetually defining a person’s life („Return of a Forgotten Right,” 2019).

The digital revolution radically decontextualized and expanded this idea. The internet’s perfect memory transformed *le droit à l'oubli* from a specific remedy for ex-convicts into a generalized desire for reputational control applicable to anyone and any type of information. The modern RTBF is invoked not just for spent criminal convictions, but for outdated news of financial troubles, embarrassing photographs, unflattering personal details, or any information an individual deems „no longer relevant“ (Rosen, 2012; „Right to be forgotten,” n.d.; „The GDPR’s ‚right to be forgotten,’” 2024). This conceptual leap represents a profound morphing of legal doctrine: a narrow right aimed at social reintegration has become a sweeping power to curate one’s digital identity, with far-reaching consequences that its originators could never have envisioned.

2.2 The Foundational Precedent: A Deep Analysis of *Google Spain SL v. Costeja González*

The catalyst for the modern RTBF was the CJEU’s 2014 landmark judgment in *Google Spain* (St. Mary’s Law Journal, 2016; Boto, 2014; „Return of a Forgotten Right,” 2019). The case was brought by Mario Costeja González, a Spanish national who discovered that a Google search for his name prominently returned links to two newspaper articles from 1998 detailing the auction of his repossessed home to settle social security debts (Ball, 2014; „Re-writing History,” 2014). The debt had long since been resolved, and Mr. Costeja argued that the continued accessibility of this information via a simple name search was an infringement of his privacy (Boto, 2014).

The CJEU’s ruling was groundbreaking and established the core tenets of the modern RTBF. Its reasoning can be broken down into three critical holdings:

1. Search Engines as „Data Controllers”: The Court determined that a search engine operator, by finding, indexing, storing, and making data available to users, engages in the

„processing” of personal data. Crucially, it found that the operator „determines the purposes and means” of this processing, and therefore qualifies as a „data controller” under the then-operative Data Protection Directive 95/46/EC (Boto, 2014; St. Mary’s Law Journal, 2016). This was a momentous step, as it imposed the full weight of EU data protection law directly onto intermediaries like Google, which had long argued they were mere conduits of information published by others.

2. **Extraterritorial Application:** The Court held that even though Google Inc. was a U.S.-based company, EU data protection law applied. The presence and activities of its Spanish subsidiary, Google Spain, which promoted and sold advertising space targeting Spanish inhabitants, created a sufficient link to establish jurisdiction (Boto, 2014). This assertion of extraterritorial reach set the stage for future conflicts between EU privacy law and the legal norms of other nations.

3. **The Balancing Test and the Presumption of Erasure:** The heart of the ruling was the Court’s balancing of fundamental rights. It weighed the data subject’s rights to privacy and data protection, enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights, against the economic interest of the search engine and the general interest of the public in accessing the information. In a decisive move, the Court established a powerful presumption: it ruled that the data subject’s rights „override, as a rule,” the interests of the search engine operator and the public (Boto, 2014; Post, 2018). This presumption could only be rebutted in specific cases, such as when the individual plays a role in public life, where there is a „preponderant interest of the general public” in having access to the information (Boto, 2014). For ordinary individuals and information deemed „inadequate, irrelevant or no longer relevant, or excessive,” the default position became delisting („Re-writing History,” 2014).

The global impact of Google Spain was immediate and profound. It effectively created a new right for over 500 million Europeans and forced global technology companies to establish massive compliance infrastructures to handle tens of thousands of delisting requests (Post, 2018; „The Right to be Forgotten,” 2025; EPIC, 2020). Ironically, the ruling also produced a textbook example of the „Streisand effect,” as the legal battle to have a 16-year-old local newspaper notice forgotten made Mario Costeja González and his past debts famous across the globe (Ball, 2014).

2.3 Subsequent Jurisprudence: Refining, Expanding, and Contesting the Right

In the years following Google Spain, European courts have continued to grapple with the scope and limits of the RTBF, creating a complex and sometimes contradictory body of case law.

The right has been significantly expanded beyond its original application to search engines. The most consequential case is *Hurbain v. Belgium*, where the ECtHR found that requiring a newspaper to anonymize an article in its own digital archive did not violate the publisher’s freedom of expression (ARTICLE 19, 2016; *Hurbain v. Belgium*, 2023). This extended the logic of the RTBF from the intermediary to the original publisher, a far more direct intervention into the historical record. Similarly, in *Biancardi v. Italy*, the ECtHR held a journalist civilly liable for refusing to de-index tags related to an old news article, broadening the category of

actors who could be held accountable for ensuring „forgetfulness” (Granja, 2022).

At the same time, courts have sought to clarify the procedural obligations of those implementing the right. In its 2022 judgment in TU, RE v. Google LLC (C-460/20), the CJEU addressed the difficult question of allegedly inaccurate information (Hurbain v. Belgium, 2023; Gstrein, 2022). It ruled that when a data subject provides relevant and sufficient evidence of clear inaccuracy, the search engine must grant the de-referencing request. However, in cases where the inaccuracy is not obvious, the search engine is not obligated to act as an arbiter of truth. Instead, it must simply add a warning to the search results notifying users of the ongoing dispute (Gstrein, 2022). This decision reflects the judiciary’s unease with forcing private companies into a quasi-judicial role of fact-finding.

Finally, jurisprudence has also limited the right, confirming it is not absolute. In the Manni case, the CJEU ruled against an individual who sought to have his name erased from a public company register after a past bankruptcy. The Court found that the public interest in ensuring „legal certainty and fair trading” through a transparent register outweighed the individual’s data protection rights (Hurbain v. Belgium, 2023). This case serves as an important reminder that where information serves a clear, legally mandated public function, the RTBF can be defeated.

2.4 Codification and Complexity: Deconstructing Article 17 of the GDPR

The principles developed in Google Spain were formally codified and elaborated upon in Article 17 of the General Data Protection Regulation (GDPR), titled „Right to erasure („right to be forgotten)”” (Hurbain v. Belgium, 2023; „Right to be forgotten,” n.d.; European Parliament and Council of the European Union, 2016). A close reading of this text reveals the inherent tensions and complexities of the right.

Article 17(1) lays out specific grounds upon which a data subject can demand the erasure of their personal data „without undue delay.” These include situations where: the data is no longer necessary for the purpose for which it was collected; the data subject withdraws consent (where consent was the legal basis for processing); the data subject objects to the processing and there are no overriding legitimate grounds; the data was unlawfully processed; or the data must be erased to comply with a legal obligation („The GDPR’s ,right to be forgotten,” 2024; European Parliament and Council of the European Union, 2016; „Right to erasure,” n.d.). This list provides a clear set of triggers for the right to be invoked.

The true battleground of the RTBF lies in Article 17(3), which outlines the critical exemptions where the right to erasure does not apply. Erasure can be refused if the processing of the data is necessary for:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation... or for the performance of a task carried out in the public interest...;
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes... (European Parliament and Council of the European Union, 2016; „Right to erasure,” n.d.; „The Right to be Forgotten,” 2025).

These exemptions are the legal firewall intended to protect journalism, the public record, and historical archives. However, their language is broad and their application has proven

to be inconsistent and highly contentious. The central conflict of this article—the Right to be Forgotten versus the Right to History—is fought in the ambiguous space of these exemptions. Who decides when a news article is „necessary” for freedom of expression, or when an archival record serves the „public interest”? The GDPR provides no clear hierarchy or detailed guidance for this balancing act.

The GDPR places the initial burden of adjudicating these complex requests squarely on the shoulders of the data controller (European Parliament and Council of the European Union, 2016; „The GDPR’s ‚right to be forgotten,’” 2024). Upon receiving an erasure request, a company like Google or a newspaper publisher has one month to investigate the claim, weigh the competing fundamental rights, and issue a decision („Respect individuals’ rights,” n.d.; European Parliament and Council of the European Union, 2016). This process effectively privatizes a form of censorship. It forces commercial entities, whose primary incentives are economic, to make profound, quasi-judicial decisions about the scope of free speech and the public interest (Fomperosa Rivero, 2017; Fomperosa Rivero, 2017).

This privatization is compounded by the immense financial risk involved. The GDPR carries staggering penalties for non-compliance, with fines reaching up to 4% of a company’s annual global turnover (Rosen, 2012). Faced with a legally ambiguous request, the most economically rational decision for a company is often to err on the side of caution and delete the content, rather than risk a ruinous fine and expensive litigation. This creates a powerful systemic bias towards erasure—a „chilling effect” that prioritizes risk aversion over the robust defense of the public’s right to know (Rosen, 2012; „Right to be forgotten,” n.d.). This problem has been exacerbated by recent developments, such as a Swedish court ruling that led Google to stop notifying publishers when their content is delisted, shrouding the entire process in even greater opacity and removing any opportunity for the original publisher to contest the decision (Hern, 2024).

2.5 The Sovereignty Dilemma: Extraterritoriality and the Google v. CNIL Ruling

A final layer of complexity in the RTBF’s architecture is its geographical reach. Given the borderless nature of the internet, does a delisting order issued in Europe apply only to European users, or must it be enforced globally? This question brought the EU’s expansive view of privacy into direct conflict with the sovereignty and legal traditions of other nations, particularly the speech-protective principles of the United States.

France’s data protection authority, the CNIL, took an aggressive stance, insisting that for the RTBF to be effective, Google must remove links from all versions of its search engine worldwide (Fomperosa Rivero, 2017; Van Calster, 2020). The dispute culminated in the 2019 CJEU case *Google v. CNIL* (C-507/17). The Court delivered a nuanced but ultimately cautious ruling. It held that, under current EU law, there is no obligation for a search engine operator to apply a de-referencing order globally (Van Calster, 2020; „EU right to be forgotten,” 2019).

However, the Court mandated that the order must be applied to all EU-based versions of the search engine (e.g., google.fr, google.de, google.es). Furthermore, it required operators to implement „sufficiently effective measures,” such as geo-blocking, to „seriously discourage” users within the EU from accessing the delisted content through non-EU domains (e.g., google.com) (Van Calster, 2020; „EU right to be forgotten,” 2019).

Critically, the CJEU left a door open. It stated that while EU law does not mandate global delisting, it also does not prohibit it. The Court affirmed the competence of a national authority or court within an EU member state to order a global de-listing on a case-by-case basis, after conducting its own balancing of rights according to national standards (Van Calster, 2020). This decision avoids a direct, universal clash with other legal systems like that of the U.S., but it creates the potential for significant legal fragmentation and ongoing, case-by-case conflicts over sovereignty in the digital sphere (Fomperosa Rivero, 2017; Van Calster, 2020). The „relevance clock” established in *Google Spain*—the principle that information’s value decays over time and is judged by the subject’s present circumstances—remains a core, and fundamentally anti-historical, tenet of this legal architecture. It imposes a temporal bias that devalues the past, judging historical facts not on their accuracy at the time, but on their desirability in the present, a logic that runs directly counter to the principles of archival and journalistic integrity.

3. THE IMPERATIVE OF HISTORY: DEFENDING THE PUBLIC DIGITAL ARCHIVE

While the legal architecture of the Right to be Forgotten is built upon the laudable goal of protecting individual dignity, its implementation poses a direct and growing threat to another fundamental pillar of democratic society: the public archive. This archive is not a single institution but a distributed network of knowledge repositories—journalistic archives, judicial records, and cultural heritage collections—that together form our collective memory. The imperative to preserve this archive is not a nostalgic preference but a structural necessity for accountability, truth, and social learning. The RTBF, by empowering individuals to selectively erase parts of this record, risks undermining its very foundation.

3.1 The Role of Journalism: The „First Rough Draft of History”

News archives have long been understood as the „first rough draft of history” (Mayer-Schönberger, 2011). They provide a contemporaneous, dated record of events, decisions, and public discourse that is indispensable for future researchers, policymakers, and citizens seeking to understand the past. The RTBF threatens this vital function in two distinct ways: by creating a chilling effect on future reporting and by compromising the integrity of existing archives.

The threat of facing erasure requests, takedown demands, and potentially ruinous litigation creates a palpable chilling effect on journalism (Rosen, 2012; „Right to be forgotten,” n.d.). Publishers, particularly smaller, independent outlets, may become increasingly timid, shying away from controversial but necessary investigative work to avoid the legal and financial risks (Rosen, 2012; CIMA, 2018). The starkest illustration of this danger is the case of *PrimaDaNoi*, an Italian news outlet that was reportedly forced to shut down after being inundated with 240 legal demands for erasure, 40 of which ended in court (ARTICLE 19, 2016). When the cost of maintaining an archive becomes prohibitive, the „first rough draft of history” may never be written at all.

Even more insidious is the threat to the integrity of existing archives. The precedent set in *Hurbain v. Belgium*, which forced a newspaper to anonymize a past article, transforms

journalists from recorders of history into its retroactive censors (ARTICLE 19, 2016; „European court extends ‚right to be forgotten,‘” 2023). Requiring news organizations to go back and alter their own legitimate publications erodes the authenticity of the archive and destroys its value as a reliable primary source (Mayer-Schönberger, 2011). It places journalists in the Orwellian position of having to „un-publish” the truth, a task that runs counter to their core professional ethics (Mayer-Schönberger, 2011). This process not only harms the public’s right to know but also creates an information asymmetry. The RTBF, while presented as a tool for the common person, is disproportionately beneficial to the powerful and wealthy, who possess the resources to pursue litigation and have the greatest incentive to „varnish” their public records (CIMA, 2018; Ball, 2014). This „elite capture” of the right allows those with influence to sanitize their past, while the histories of ordinary people remain raw and unedited, further entrenching societal power imbalances (CIMA, 2018).

3.2 The Principle of Open Justice

A cornerstone of the rule of law in democratic societies is the principle of open justice. This principle dictates that court proceedings and their resulting records should be publicly accessible. This transparency is crucial for several reasons: it ensures judicial accountability, allows for public scrutiny of the justice system, deters misconduct, and provides the body of precedent upon which the common law evolves (Tobin & Walz, 2015). The digitization of court records has made this principle more meaningful than ever, allowing for widespread access and analysis.

The Right to be Forgotten poses a direct challenge to open justice. A significant portion of erasure requests concern past criminal convictions, even those that are „spent” or resolved („Right to be forgotten,” n.d.; „Return of a Forgotten Right,” 2019; Conklin v. Sloss, 1978). While the goal of rehabilitation for former offenders is a legitimate and important societal value, erasing the public record of their convictions is a fraught solution. It pits the individual’s desire to move on against the public’s interest in knowing the background of individuals, especially those who may enter positions of public trust or responsibility (Tobin & Walz, 2015; „Return of a Forgotten Right,” 2019).

This conflict extends to the very tools of legal research. Online legal databases, which are essential for lawyers, judges, and scholars, are being targeted. For example, the Indian legal database Indian Kanoon was ordered by a High Court to remove a judgment that revealed the identity of a rape victim (Legal Heirs vs. Custodian, 2025). While the motive—protecting the victim—is understandable, the method—altering the public legal record—is perilous. If court judgments can be selectively edited or removed from databases, the integrity of the entire body of case law is compromised, making legal research unreliable and precedent harder to track („Return of a Forgotten Right,” 2019). This creates a conflict between two distinct models of forgetting. The original *droit à l’oubli* was based on a rehabilitative model, where society purposefully „forgets” a past crime to allow for reintegration (Rosen, 2012; „Return of a Forgotten Right,” 2019). The archival model, which underpins open justice, is based on preservation for the sake of accountability and knowledge. Applying the logic of rehabilitative forgetting to the archival space of public court records is a category error

that misunderstands the fundamental purpose of a public archive, which is not to make individuals feel better, but to provide an unvarnished record for the benefit of the collective.

3.3 Cultural and Historical Archives

Beyond journalism and law, the core mission of state archives, national libraries, museums, and other cultural heritage institutions is to preserve a complete and authentic record of society for the benefit of future generations (Vavra, 2018; „Archives in the Digital Age,” 2021; „The Right to Be Forgotten,” 2025). These institutions operate under a professional ethic of preservation and access, serving as the long-term memory of a nation and a culture.

The GDPR’s archival exemption, found in Article 17(3)(d), is the primary legal shield for these institutions („The Right to be Forgotten,” 2025; Vavra, 2018). It explicitly states that the right to erasure does not apply when data processing is necessary for „archiving purposes in the public interest, scientific or historical research purposes.” However, the expansive logic of the RTBF and the litigious climate it fosters create significant uncertainty and risk. Archivists are increasingly faced with the dilemma of balancing their professional duty to preserve and provide access against the potential legal and financial risks of hosting digitized collections that contain personal data (Vavra, 2018; „The Right to Be Forgotten,” 2025).

The challenge is particularly acute for „born-digital” records and large datasets used in digital humanities and social science research. Personal information may be deeply interwoven within these records, making complete erasure technically challenging, prohibitively expensive, and scientifically damaging, as removing individual data points could corrupt the integrity of the entire dataset („The Right to Be Forgotten,” 2025; Vavra, 2018). Furthermore, the archival principle of acquiring records often predates the modern concept of granular consent for every potential future use. Expecting archives to retroactively secure consent for millions of historical documents is an impossible standard that would effectively paralyze their mission (Culbertson & Lanthorne, n.d.).

3.4 The „Varnishing History” Argument

Synthesizing these threats to journalism, justice, and cultural heritage leads to the most profound critique of the Right to be Forgotten: its potential to create a sanitized, unreliable, and ultimately false historical record. Critics have forcefully argued that an overzealous application of the RTBF amounts to a form of digital censorship and the „rewriting of history” (Rosen, 2012; „Re-writing History,” 2014; Vavra, 2018).

When individuals are empowered to selectively remove unfavorable but truthful information from the public sphere, the result is not a more humane society, but a less honest one. This process creates „memory holes” in the digital record, leaving behind a varnished and curated version of the past that is stripped of its difficult and inconvenient truths (Edwards, 2017; Mayer-Schönberger, 2011). Such a system is ripe for abuse by the powerful. Politicians can erase records of past scandals, corporations can scrub evidence of malfeasance, and criminals can whitewash their histories, all under the guise of protecting personal data (CIMA, 2018; „The Right to be Forgotten,” 2024). This undermines the very

basis of public accountability.

Ultimately, a society that cannot trust its own records loses its capacity for collective learning and critical self-reflection. The RTBF, by prioritizing individual comfort over historical integrity, risks fostering a culture of historical amnesia. It threatens to create a digital world where the past is not a source of wisdom to be grappled with, but a source of embarrassment to be erased (De Baets, 2016). An unreliable past cannot serve as a guide for the future.

4. A COMPARATIVE ANALYSIS: EU VS. U.S. APPROACHES

The global debate over the Right to be Forgotten is dominated by two starkly contrasting legal and philosophical paradigms: the rights-based model of the European Union and the speech-protective model of the United States. This divergence is not a mere technical disagreement over legal rules; it reflects fundamentally different conceptions of the relationship between the individual, the state, and the public sphere. Understanding this clash is crucial to appreciating the difficulty of achieving a global consensus and the high stakes involved for multinational technology companies that must navigate both systems.

4.1 The EU Model: Dignity, Data Protection, and the Primacy of the Individual

The European approach to the RTBF is grounded in a deep-seated legal tradition that places a high value on human dignity and personality rights (Byrum, 2017; Post, 2018). This „dignitarian” perspective views the protection of an individual’s private sphere and personal data as a prerequisite for their flourishing and full participation in society. The legal framework, from the early Data Protection Directive to the modern GDPR and the Charter of Fundamental Rights of the European Union, is built upon the principle of „informational self-determination”—the idea that individuals should have meaningful control over data concerning them (Byrum, 2017; Fabbrini & Celeste, 2020).

European jurisprudence consistently reflects this prioritization. In landmark cases like *Google Spain* and *Hurbain v. Belgium*, courts have demonstrated a clear tendency to weigh the fundamental rights of the individual to privacy (Charter, Art. 7) and data protection (Charter, Art. 8) more heavily than the more abstract public interest in information or the economic interests of data controllers (Fomperosa Rivero, 2017; Post, 2018; „European court extends „right to be forgotten,” 2023). The result is a legal system that creates a presumption in favor of the individual’s request for erasure, placing the burden on the data controller or the public to justify the continued dissemination of the information. This approach can be seen as reflecting a „communitarian” model of democracy, where the state and the legal system have a positive duty to protect individuals from certain harms inflicted within the public sphere to ensure their dignity is upheld.

4.2 The U.S. Model: The First Amendment, Public Concern, and the Primacy of Speech

In sharp contrast, the United States model is overwhelmingly speech-protective, rooted in the exceptionally robust guarantees of the First Amendment to the U.S. Constitution (Rosen, 2012; „Right to be forgotten,” n.d.; St. Mary’s Law Journal, 2016; Nunziato, 2018). The American legal system has, for all practical purposes, „flatly rejected” the notion of a broad, European-style Right to be Forgotten (St. Mary’s Law Journal, 2016). The prevailing legal and cultural tradition strongly favors the public’s „right to know” and protects the

publication of truthful information, especially when that information is a matter of public concern or is contained within public records (Rosen, 2012; Tobin & Walz, 2015).

This stance is solidified by a long line of Supreme Court and lower court precedents. Cases like *Cox Broadcasting Corp. v. Cohn*, which affirmed the media's First Amendment right to publish information (in that case, a rape victim's name) obtained from public court records, establish a high constitutional barrier against punishing truthful speech (Tobin & Walz, 2015). Similarly, the influential case of *Sidis v. F-R Publishing Corp.* rejected the argument that a public figure's newsworthiness fades with the passage of time, establishing a principle that is often summarized as „once public, always public“ (St. Mary's Law Journal, 2016). While U.S. tort law does recognize a limited right to privacy, claims for public disclosure of private facts are exceedingly difficult to win, especially when the information is truthful and deemed „newsworthy“ (St. Mary's Law Journal, 2016; *Melvin v. Reid*, 1931). This approach reflects a more „libertarian“ or „republican“ model of democracy, which prioritizes a wide-open and largely unregulated public sphere, trusting that an informed citizenry, armed with more speech rather than less, is the ultimate check on power and the best path to truth.

4.3 The Clash: Analyzing Legal and Philosophical Friction

The collision of these two models creates significant legal and philosophical friction, particularly for the global technology platforms that operate in both jurisdictions. The key points of conflict include:

- **Dignity vs. the Marketplace of Ideas:** The EU's use of human dignity as a justification for restricting speech clashes directly with the foundational U.S. theory of the „marketplace of ideas.“ In the American view, the proper response to harmful or offensive speech is not enforced silence (censorship), but countervailing speech and public debate (Byrum, 2017).
- **Public vs. Private Figures:** While both legal systems distinguish between public and private figures, the threshold for losing one's privacy is far lower in the U.S. Once an individual becomes involuntarily newsworthy (e.g., by being the victim or perpetrator of a crime), their claim to privacy is significantly weakened. The EU model, as seen in Costeja and Hurbain, provides much stronger protection for private individuals even when they are involved in matters of public record (St. Mary's Law Journal, 2016; Sartor, 2021).
- **Liability of Intermediaries:** The EU's classification of search engines as „data controllers“ makes them directly liable for the content they link to and forces them into an editorial role (Fomperosa Rivero, 2017). This is fundamentally at odds with U.S. law, most notably Section 230 of the Communications Decency Act, which generally immunizes online intermediaries from liability for content created by third parties.
- **The Extraterritoriality Impasse:** The friction becomes an outright conflict of laws in the context of extraterritoriality. An EU court order demanding the global delisting of content could require a U.S.-based company to violate the First Amendment by censoring information that is perfectly legal and constitutionally protected in the United States (Fomperosa Rivero, 2017; Van Calster, 2020). The *Google v. CNIL* decision was a pragmatic attempt to avoid a direct collision, but it leaves the potential for future conflicts unresolved (Van Calster, 2020). The following table provides a structured summary of these core distinctions.

Table 1: Comparative Analysis of EU and U.S. Legal Approaches

Feature	European Union Model	United States Model
Legal Basis	GDPR (Art. 17), EU Charter of Fundamental Rights (Arts. 7 & 8)	First Amendment to the U.S. Constitution
Core Protected Value	Human Dignity, Privacy, Data Protection	Freedom of Speech, Freedom of the Press
Philosophical Underpinning	Dignitarian / Communitarian Democracy	Libertarian / Republican Democracy
Status of Truthful Information	Can be removed if "irrelevant," "excessive," or "outdated"	Strongly protected, especially if a matter of public concern
Key Precedent	Google Spain SL v. Costeja González (2014); Hurbain v. Belgium (2023)	Cox Broadcasting v. Cohn (1975); Sidis v. F-R Pub. Corp. (1940)
Treatment of Public Figures	Reduced privacy rights, but still protected; strong protection for private individuals	Very limited privacy rights regarding matters of public concern
Liability of Intermediaries	Liable as "data controllers"	Generally immune from liability (e.g., Section 230)
Primary Remedy	Erasure / De-indexing (Injunctive Relief)	Monetary Damages (for torts like invasion of privacy)

Source: created by the author.

This deep philosophical divergence explains why simple legal „harmonization” between the EU and U.S. models is so challenging. It would require one side to abandon a core tenet of its democratic self-conception—either the state’s positive duty to protect individual dignity or the paramount importance of an unregulated public sphere (Sartor, 2021).

5. TOWARDS A RECONCILIATORY FRAMEWORK

The current legal landscape, characterized by a transatlantic philosophical divide and vague domestic balancing tests, is inadequate for resolving the complex communicational conflict between the Right to be Forgotten and the Right to History. The simple binary of „privacy versus speech” is a blunt instrument for a delicate task. What is needed is a more nuanced, structured, and principled approach that moves beyond this opposition to analyze the specific context and function of the information at issue. This section critiques the shortcomings of existing tests and proposes a multi-factor communicational framework designed to guide a more transparent and just reconciliation.

5.1 Critique of Current Balancing Tests

The balancing tests currently employed by courts and data controllers are often criticized for their vagueness and inconsistent application. The test articulated by the CJEU in Google Spain, which requires weighing the data subject’s fundamental rights against the „public interest,” has proven particularly problematic (Fomperosa Rivero, 2017). The term „public interest” is a notoriously amorphous concept, a legal black box that can be filled with any number of subjective considerations, leading to unpredictable outcomes (Van Calster, 2020). Furthermore, the court created a strong presumption in favor of erasure, making it difficult

for the public's right to know to prevail in many cases (St. Mary's Law Journal, 2016).

While subsequent jurisprudence, such as the ECtHR's decision in *Hurbain v. Belgium*, has introduced a more specific list of criteria (e.g., passage of time, public figure status, contemporary interest), these factors are still applied with considerable discretion and without a clear, overarching philosophy to guide their weighting (ARTICLE 19, 2023). This lack of a structured framework leaves crucial decisions in the hands of private companies that are incentivized to delete content or in the varying discretion of national judges, leading to a fragmented and often opaque system of ad hoc justice.

5.2 Proposing a Multi-Factor Communicational Framework

To remedy these shortcomings, this article proposes a structured, multi-factor framework. This framework is not merely a legal test but a tool for achieving what might be called „communicational justice.“ It shifts the central question from a simple clash of rights to a more nuanced inquiry: What is the communicative function and purpose of this information in this specific archival context? By focusing on the role the information plays, it allows for a more principled differentiation between, for example, a malicious private communication with no public value (like revenge pornography) and a public-facing communication essential for democratic accountability (like a news report on political corruption).

The framework consists of five core factors, each designed to elicit a specific set of contextual details that inform the final balancing act.

1. **The Nature of the Information:** This factor assesses the content itself. Is the data a record of a serious criminal conviction, sensitive health or financial information, a minor social embarrassment, or a publicly filed business record? („Return of a Forgotten Right,” 2019; Sartor, 2021). Information relating to serious crimes or matters of significant public concern would weigh heavily in favor of preservation, while highly sensitive personal data with little public relevance would weigh toward erasure.

2. **The Role of the Individual (Data Subject):** This factor examines the status of the person requesting erasure. Is the individual a public figure (a politician, CEO, celebrity) who has voluntarily sought public attention, or a private citizen who has been thrust into the public eye involuntarily? (Van Calster, 2020; St. Mary's Law Journal, 2016). The privacy expectations of a private citizen are reasonably higher than those of a public official, for whom public scrutiny is a necessary component of accountability.

3. **The Passage of Time:** This factor considers the time elapsed since the events in question and the information's initial publication (Granja, 2022). While time is a relevant consideration, its weight is not absolute and must be assessed in conjunction with the other factors. The relevance of a 20-year-old conviction may diminish for a private individual but may remain highly relevant for a politician seeking high office. For events of major historical significance, the passage of time may have little to no diminishing effect on their value.

4. **The Original Context and Purpose of Publication:** This crucial factor analyzes why the information was created and disseminated in the first place. Was it part of a journalistic investigation aimed at informing the public? A public court record meant to ensure judicial transparency? A government report? Or was it a voluntary social media post intended for a limited audience? (Google, n.d.; Tobin & Walz, 2015; De Baets, 2016). Information created

with a clear public-facing, accountability-driven purpose has a much stronger claim to permanence in the public archive.

5. The Medium of the Archive (The „Publisher“): This factor assesses the institutional mission and nature of the entity holding the data. Is the erasure request directed at a national library or official state archive with a legal mandate to preserve history? A major newspaper with a journalistic duty to maintain its archive? A court’s official records database? Or is it a commercial search engine, a social media platform, or a personal blog? (Vavra, 2018; „The Right to Be Forgotten,” 2025; Teixeira da Silva & Nazarovets, 2023). The claim for preservation is strongest for institutions whose core public mission is archival.

The following table operationalizes this framework into a practical tool for analysis, providing a structured rubric for decision-makers.

Table 2: Proposed Multi-Factor Framework for Adjudicating RTBF vs. Right to History Claims

Factor	Guiding Questions for Analysis	Weighting Towards Preservation (Right to History)	Weighting Towards Erasure (RTBF)
1. Nature of Information	What is the subject matter? Is it related to criminal activity, public safety, political speech, financial matters, or personal life? Is the information demonstrably false or accurate?	Information relates to serious crime, public health/safety, political conduct, or is part of a public legal proceeding.	Information is highly sensitive (health, sexuality), relates to a minor offense, is purely a private embarrassment, or is proven to be inaccurate.
2. Role of the Individual	Is the data subject a public figure, a limited-purpose public figure, or a private citizen? Did they voluntarily enter the public sphere?	The individual is a public official, a CEO, a celebrity, or has otherwise sought public influence.	The individual is a private citizen with no public role, especially if they are a minor or a victim of a crime.
3. Passage of Time	How long ago did the event occur? Has the information lost its contemporary relevance or does it retain historical/scientific value?	The event is recent, of significant historical importance, or part of an ongoing pattern of behavior.	A significant amount of time has passed, the issue has been resolved, and the individual has demonstrated rehabilitation.
4. Original Context & Purpose	Why was the information originally published? Was it for journalistic, judicial, academic, or governmental purposes? Or for personal expression/gossip?	Published by a legitimate news organization as part of public interest reporting, or is an official court/government record.	Published on social media voluntarily, on a gossip blog, or as part of a personal dispute without broader public interest.
5. Medium of the Archive	Who is the data controller? A national archive, a newspaper, a court, a search engine, or a social media platform? What is their public mission?	The controller is a public archive, library, museum, or court system with a mandate for preservation.	The controller is a social media platform, a data broker, or another commercial entity with no archival or journalistic mission.

Source: created by the author.

5.3 Technological Solutions: A Mediated Middle Ground

The resolution to this conflict need not be a binary choice between total preservation and total erasure. Technology itself offers a spectrum of remedies that can serve as a mediated middle ground, and the choice of remedy is itself a philosophical statement about the nature of memory (Vavra, 2018).

- **De-indexing vs. Removal:** The distinction is critical. De-indexing a page from a search engine is a less intrusive remedy than demanding the removal of the source content (Vilella & Ruffo, 2025). It restores a degree of „practical obscurity” without destroying the historical record. The framework should always prioritize the least restrictive means necessary to achieve a just balance. De-indexing embodies a philosophy of practical obscurity—history is preserved but made less prominent.

- **Anonymization and Pseudonymization:** Anonymization, as ordered in Hurbain, is a powerful tool but also a dangerous one (Vavra, 2018; NIST, 2015). It directly alters the historical record by removing key data points, potentially rendering it meaningless for future research. It embodies a philosophy of redaction. Its use should be reserved for the most exceptional of circumstances, where the harm to the individual is severe and demonstrable, and the historical value of their specific identity is negligible.

- **Contextualization and Updates:** A far superior and more constructive solution is to favor a „right to reply” or a „right to update.” Instead of erasing or redacting old news articles or records, archives could be technically equipped and legally encouraged to append updates, corrections, or links to more recent information (Bollinger & Callamard, 2021). For example, a news report about an arrest could be permanently linked to a subsequent article about the acquittal. This approach fully respects the integrity of the Right to History by preserving the original record, while also respecting the individual’s right to an accurate and up-to-date public portrayal. This embodies a philosophy of additive history, where the remedy for a problematic past is not less information, but more.

By adopting a structured framework and embracing more nuanced technological solutions, it is possible to move beyond the current impasse and forge a path that protects individual dignity without sacrificing the integrity of our collective memory.

6. CONCLUSION

The rapid evolution of the Right to be Forgotten from a niche legal theory into a powerful, globally contested principle of data protection law has placed modern societies at a critical juncture. The conflict between this individual right to control one’s digital past and the collective right to preserve a complete and accessible history is not a peripheral issue but a central challenge to the architecture of the digital public sphere. It forces a confrontation with fundamental questions about memory, accountability, dignity, and democracy in an age of informational permanence.

This article has argued that the tension between the RTBF and the Right to History must be understood as a communicational conflict over the control of historical narratives. The analysis of the RTBF’s legal architecture, particularly under the EU’s GDPR, reveals a system that, while born from the laudable goal of protecting individual dignity, has evolved in ways

that pose a direct threat to the public archive. Landmark cases, from Google Spain to *Hurbain v. Belgium*, demonstrate a trajectory from mediating access to information (delisting) to mandating its alteration at the source (anonymization). This evolution, coupled with a procedural framework that privatizes adjudication and incentivizes erasure, creates a significant chilling effect on journalism and undermines the principles of open justice and archival integrity.

The comparative analysis of the EU and U.S. models has shown that this is not merely a dispute over legal technicalities but a clash of deep-seated political philosophies regarding the proper balance between individual dignity and free expression in a democracy. The current, often vague, balancing tests have proven inadequate to resolve this conflict in a principled manner.

In light of this analysis, the central thesis of this article is reaffirmed: the conflict between the ‘right to be forgotten’ and the ‘right to history’ cannot be resolved through a simple legal hierarchy, but requires a dynamic, context-dependent communicational framework. Such a framework, as proposed herein, moves beyond the simplistic “privacy vs. speech” binary to analyze the specific communicative function of the information in question. By systematically considering factors such as the nature of the data, the role of the individual, the passage of time, the original purpose of publication, and the institutional mission of the archive, it becomes possible to balance an individual’s legitimate interest in informational self-determination against the non-negotiable societal necessity of a preserved, searchable, and reliable public record.

The stakes of this debate are immense. An overly expansive and crudely applied Right to be Forgotten risks creating a sanitized and unreliable public record, a “varnished history” that serves the powerful and erodes the foundations of democratic accountability. If the “first rough draft of history” can be retroactively edited upon request, and if public records of justice can be obscured, society’s ability to scrutinize power, learn from its mistakes, and hold individuals and institutions to account is dangerously diminished.

In the digital age, the public archive is our collective memory. Its integrity is paramount. A society that permits its memory to be fragmented and curated according to the preferences of individuals risks becoming a society without a stable, shared understanding of its own past. This erodes the common ground of fact upon which democratic discourse depends and threatens to leave future generations with a digital inheritance that is untrustworthy and incomplete. Striking the right balance is therefore not just a legal challenge, but a civic imperative.

This rapidly evolving field presents numerous avenues for future scholarly investigation.

First, the intersection of the RTBF with Artificial Intelligence and Large Language Models (LLMs) is a critical new frontier. The technical challenge of “machine unlearning”—forcing an AI model to truly “forget” data it was trained on—is immense and raises profound legal and ethical questions (Rempe, 2025; Vilella & Ruffo, 2025). Future research must explore whether the legal concept of erasure can be meaningfully applied to probabilistic systems and what new regulatory models are needed for AI governance.

Second, further work is needed on the development of international norms and legal instruments to manage the cross-jurisdictional conflicts highlighted by the EU-U.S. divide.

The current state of legal fragmentation is unsustainable for a global internet. Scholarship exploring potential treaty frameworks or models of regulatory cooperation is essential.

Third, this article has focused primarily on the EU and U.S. models. Rich comparative research is needed to understand how non-Western legal traditions are adapting or resisting the RTBF. In-depth studies of the emerging jurisprudence in countries like India, Brazil, Japan, and South Korea will provide a more global perspective on this challenge (Nunziato, 2018; „Not just one, many rights to be forgotten,” n.d.; Legal Heirs vs. Custodian, 2025; „Re-writing History,” 2014).

Finally, the technological solutions themselves require deeper interdisciplinary analysis. Research that combines legal, ethical, and computer science perspectives is needed to design and evaluate systems for contextualization, algorithmic forgetting, and privacy-preserving archival access that can better reconcile the competing values at stake (Vilella & Ruffo, 2025; Vavra, 2018).

Navigating the future of digital memory requires not only legal acumen but also historical wisdom and technological foresight. The challenge is to build a digital world that respects individual dignity without sacrificing the shared truths upon which a just and accountable society depends.

REFERENCES

- ARTICLE 19. (2016). Policy brief: The right to be forgotten. <https://www.article19.org/resources/policy-brief-the-right-to-be-forgotten/>
- Ball, J. (2014, May 14). Mario Costeja González: The man who fought Spain’s Google – and won. *The Guardian*. <https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten>
- Bollinger, L. C., & Callamard, A. (Eds.). (2021). *Regardless of frontiers: Global freedom of expression in a troubled world*. Columbia University Press. <https://scholarship.law.columbia.edu/books/361>
- Cloudflare. (n.d.). What is the right to be forgotten (RTBF)? Retrieved from <https://www.cloudflare.com/learning/privacy/right-to-be-forgotten/>
- De Baets, A. (2009). *Responsible history*. Berghahn Books. <https://doi.org/10.3167/9781845455415>
- De Baets, A. (2016). A historian’s view on the right to be forgotten. *International Review of Law, Computers & Technology*, 30(1-2), 94-105. <https://doi.org/10.1080/13600869.2015.1125155>
- 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.
- Fabbrini, F., & Celeste, E. (2020). The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, 21(S1), 55–65. doi:10.1017/glj.2020.14
- Faisal, K. (2021). Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions. *Security and Privacy*, 4(1), 2.
- Fomperosa Rivero, Á. (2017). Right to be forgotten in the European Court of Justice Google Spain case: The right balance of privacy rights, procedure, and extraterritoriality (European Union Law Working Paper No. 19). Stanford–Vienna Transatlantic Technology Law Forum.
- Hern, A. (2024, February 15). Google stops notifying publishers of ‘right to be forgotten’ removals from search results. *The Guardian*. <https://www.theguardian.com/technology/2024/feb/15/google-stops-notifying-publishers-of-right-to-be-forgotten-removals-from-search-results>
- Hurbain v. Belgium [GC], Application No. 57292/16, European Court of Human Rights, Judgment 4 July 2023. Retrieved from: <https://hudoc.echr.coe.int/eng?i=001-225814>
- Keller, D. (2018). The right tools: Europe’s intermediary liability laws and the EU 2016 General Data

Protection Regulation. *Berkeley Technology Law Journal*, 33(1), 287-340.

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU General Data Protection Regulation: A commentary/update of selected articles (Maastricht Faculty of Law Working Paper). SSRN. <https://doi.org/10.2139/ssrn.3839645>

Mayer-Schönberger, V. (2011). *Delete: The virtue of forgetting in the digital age*. Princeton University Press. 10.1515/9781400838455

Nunziato, D. C. (2018). The fourth year of forgetting: The troubling expansion of the right to be forgotten (Working paper). George Washington University Law School. https://scholarship.law.gwu.edu/faculty_publications/1356/.

Post, R. (2018). Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, 67(5), 981-1072.

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online*, 64, 88-92 .

Royston, S. W. (2016). The Right to Be Forgotten: Comparing U.S. and European Approaches. *St. Mary's Law Journal*, 48(2), 253.

Sartor, G. (2020). Artificial intelligence and human rights: Between law and ethics. *Maastricht Journal of European and Comparative Law*, 27(6), 705-719. <https://doi.org/10.1177/1023263X20981566> (Original work published 2020)

Tobin, C. D., & Walz, C. N. (2015). Right to be forgotten, expungement laws raise new challenges on the 40th anniversary of *Cox Broadcasting v. Cohn*. *Communications Lawyer*, 31(3), 4-10.

Vavra, A. (2018). The right to be forgotten: An archival perspective. *The American Archivist*, 81(1), 100-118. <https://doi.org/10.17723/0360-9081-81.1.100>

Vilella, S., & Ruffo, G. (2025). (De)-Indexing and the Right to be Forgotten. <https://doi.org/10.48550/arXiv.2501.03989>.