

Critical Assessment of the Legal Philosophy of the Right to Be Forgotten

Pr. Ali LatrecheAdrar- Université – Algeria ; ali.latreche@univ-adrar.edu.dz
ORCID iD: 0009-0008-3536-4126**Pr. Zebiri Ramdane**Adrar- University – Algeria ; zebiri_ramdane@univ-adrar.edu.dz
ORCID iD : 0000-0002-1208-7268**Dr: Mechid Mohammed**Oran 2- University – Algeria; mdmechid@gmail.com
ORCID iD: 0009-0003-4286-945X

Abstract

This study elucidates the digital "right to be forgotten" as a profound paradigm shift redefining the ontological relationship between the human subject and absolute technological memory. Operating within a dialectical tension, this prerogative serves as an advanced extension of privacy that empowers individuals especially vulnerable children to reclaim informational sovereignty and safeguard human dignity against permanent digital documentation. Conversely, its enforcement remains strictly relative, intersecting with competing democratic imperatives, including freedom of expression, the public's right to know, and the preservation of collective historical consciousness. Furthermore, the practical efficacy of digital oblivion is severely constrained by systemic technical impediments, such as borderless internet networks and the rise of Artificial Intelligence, where "algorithmic memory" perpetuates automated decisions even after raw data is expunged. Synthesizing Paul Ricoeur's concept of "just memory" and Jürgen Habermas's public sphere, the study concludes that enhancing this right requires a qualitative transition from rigid codification toward a dynamic framework of legal proportionality, integrating legislative evolution with technological advancements like "privacy by design" to achieve a vital temporal equilibrium.

Keywords: The Right to Be Forgotten; Algorithmic Memory; Proportionality and Balancing; Informational Sovereignty; Just Memory; Privacy by Design.

Introduction

The evolution of the right to be forgotten within the digital ecosystem cannot be comprehended in isolation from the profound transformations affecting the nature of the relationship between human beings and their memory. Indeed, humanity has transitioned from entities possessing the inherent capacity to forget to beings existing within an unforgetting digital memory. Throughout this trajectory, the right to be forgotten has transcended being a mere legal mechanism for data

¹ Received: June 12, 2026; Accepted: July 23, 2026; Published: August 24, 2026



erasure; it has manifested as a complex philosophical and legal dilemma. This dilemma revolves around the boundaries of technological hegemony over human autonomy, and the extent to which the law can recalibrate the equilibrium between digital retention and human oblivion.

On the one hand, the right to be forgotten manifests as a constitutive mechanism for safeguarding human dignity. It empowers individuals to exercise control over their personal data and to expunge the remnants of a digital past that could impede their social reintegration or inflict persistent psychological harm. On the other hand, this right engenders serious concerns regarding the potential infringement upon collective memory, freedom of expression, and the right to information. Consequently, it operates as a qualified right, contingent upon a meticulous balancing act among competing interests.

Within this framework, the significance of a critical approach becomes evident. Such an approach transcends merely highlighting the merits of this right, seeking instead to analyze its limitations and problematic dimensions, both in terms of practical application and efficacy against the technical and legal challenges imposed by the digital environment. Furthermore, this approach necessitates envisioning the evolutionary prospects of this right, particularly in light of the emergence of Artificial Intelligence (AI) and Big Data. These innovations have reshaped the very concept of digital memory, rendering oblivion far more complex than previously conceived.

Accordingly, this chapter aims to provide a comprehensive critical reading of the legal philosophy underlying the right to be forgotten. This is achieved by scrutinizing its advantages and drawbacks, analyzing its efficacy, and prognosticating its development. Ultimately, this reflects the law's continuous endeavor to adapt to rapid digital transformations while guaranteeing a balanced protection of fundamental human rights. From this perspective, this research will be structured into two primary chapters:

- Chapter One: An Evaluative Analysis of the Right to Digital Oblivion: Merits and Drawbacks
- Chapter Two: The Efficacy of the Right to Be Forgotten and Its Developmental Prospects

Chapter One: An Evaluative Analysis of the Right to Digital Oblivion: Merits and Drawbacks

Discourse surrounding the right to be forgotten in the digital era cannot be confined within a simplistic binary framework that reduces this right to a mere legal mechanism for privacy protection. Rather, it must be conceptualized as a complex phenomenon situated at the intersection of legal, philosophical, and social dimensions. This right, which emerged in tandem with the confrontation against a perpetual digital memory, harbors a profound paradox: it operates simultaneously as an instrument for liberating individuals from their past and a potential means for reconstructing or obscuring that very past.

On the one hand, the right to be forgotten emerges primarily as a humanistic mechanism aimed at restoring the equilibrium between the individual and their digital memory, enabling them to transcend past transgressions, reclaim their dignity, and foster social reintegration. Consequently, it constitutes a natural extension of the right to privacy, and an advanced expression of temporal control over digital identity. On the other hand, these merits give rise to profound dilemmas, raising fundamental questions about its boundaries; particularly given its conflict with other equally vital rights, such as freedom of expression, the public's right to know, and the preservation of historical memory. It is here that the qualified nature of this right becomes apparent, as it cannot be absolute without undermining the overarching equilibrium of the legal order.

Accordingly, an evaluation of the right to be forgotten necessitates a dual critical approach. This approach entails highlighting its merits on the one hand, and exposing its inherent risks on the other, within an analytical framework aimed at understanding this right in its complex reality rather

than its superficial manifestation. From this perspective, this chapter will be analyzed in accordance with the following subdivision:

- Section One: The Merits of the Right to Be Forgotten Online for Individuals
- Section Two: The Drawbacks of the Right to Be Forgotten Online for Individuals
- Section Three: The Merits of the Right to Be Forgotten Online for Children

Section One: The Merits of the Right to Be Forgotten Online for Individuals

The operationalization of the right to be forgotten within the digital sphere by compelling or incentivizing tech giants such as Google, Apple, Microsoft, Amazon, and Meta to adopt an effective collaborative approach toward the erasure of personal data upon data subjects' requests; is poised to catalyze a radical transformation in the architecture of the digital environment. This environment has historically subverted privacy, shifting it from a secluded, protected domain into an exposed, perpetually documented space.

From a legal perspective, this trajectory is anchored in the developments established by the General Data Protection Regulation (GDPR), which institutionalized the 'right to erasure' as a direct extension of the right to privacy, thereby empowering individuals to reclaim control over their personal data. Furthermore, this operationalization reflects a paradigm shift from the logic of data ownership by platforms to the principle of individual informational sovereignty. Under this framework, personal data is conceptualized as an extension of human dignity rather than mere monetizable digital assets subject to commercial exploitation.

From a philosophical perspective, the operationalization of this right reconfigures the relationship between human beings and their digital memory. It positions forgetting as a fundamental human right rather than a technical anomaly. Although permanent digital memory offers meticulous documentation, it can metamorphose into a coercive instrument that freezes and imprisons individuals within their past, thereby impeding the reconstruction of their identity. Consequently, the right to be forgotten serves as a mechanism to restore equilibrium between the collective memory of the digital society and the individual's inherent right to transformation and renewal.

Grounded in this conceptualization, several core advantages of operationalizing this right can be delineated:

- Redrawing the legal and ethical boundaries between private and public life, thereby preventing the illicit encroachment of the digital sphere into the individual's personal domain.
- Mitigating the negative psychological ramifications associated with the continuous circulation of obsolete data, which can trigger anxiety, social stigmatization, or mental distress.
- Rehabilitating the psychological and social framework of the individual by granting them an opportunity to reconstruct their self-image independent of past errors or distorted data.
- Empowering individuals to redress moral harm caused by the perpetual reminder of historical events, thereby fostering symbolic justice within the digital sphere.
- Curbing the indefinite retention of personal data over time and restricting its continued dissemination outside its original context.
- Reorganizing the private digital space under a structured legal framework that ensures data controllability rather than chaotic, unregulated flow.
- Restoring the natural right to informational self-determination, serving as an intrinsic extension of the rights to privacy and human dignity.

- Contributing indirectly to the reduction of cybercrimes, specifically those linked to extortion, defamation, and reputational damage, by minimizing the availability of exploitable or archaic content.

Accordingly, the right to be forgotten cannot be regarded merely as a technical procedure for data erasure. Rather, it signifies a profound paradigm shift in the philosophy of digital justice, predicated on restoring human agency in the face of absolute digital memory and recalibrating the equilibrium between technological evolution and the protection of the human essence of privacy.

Through the application of the comparative method, it becomes evident that the European Union's General Data Protection Regulation (GDPR) stands as the definitive global framework that has successfully operationalized these core merits, compelling an incontrovertible alignment from major internet conglomerates.

Section II: The Disadvantages of the Right to Be Forgotten Online for Individuals

In strictly legal terms, the right to be forgotten cannot be conceptualized as an absolute rule or a prerogative of an unconditional nature; rather, it is a relative right subject to the logic of balancing competing rights and freedoms within the digital sphere. Indeed, the protection of privacy cannot be achieved in isolation from the preservation of freedom of expression and the right of access to information, a dynamic that necessitates the adoption of a balancing approach based on proportionality rather than outright negation. The General Data Protection Regulation (GDPR) institutionalized this conceptual framework by recognizing the right to erasure, while simultaneously introducing explicit derogations, particularly when data processing remains imperative for journalistic, legal, or public interest purposes.

From a philosophical perspective, this restriction reflects a profound tension between collective memory and individual oblivion. While the individual strives to turn the pages of their past, society remains determined to preserve historical facts as an integral component of its history and identity. Consequently, the right to be forgotten is not to be construed as an obliteration of history, but rather as a regulatory mechanism governing its presence, thereby preventing it from morphing into an instrument of perpetual harm to the individual. Within this framework, the paramount limitations and adverse implications associated with the enforcement of this right can be delineated as follows:

- **Preservation of Historical Memory:** The retention of information constitutes an integral component of future generations' right to historical truth. Consequently, the erasure of certain data poses a potential infringement upon historical narratives and their chronological continuity.
- **Freedom of the Press and Media:** An over extensive application of the right to be forgotten may inadvertently curtail the operational capacity of journalists and media institutions, particularly regarding the reporting of events of profound public significance.
- **The Public's Right to Know:** Society maintains a legitimate interest in accessing specific information, most notably that which concerns public figures or matters impacting the public interest.
- **The Requisites of Criminal Justice:** The judiciary necessitates the preservation of data to track, investigate, and substantiate criminal offenses. Thus, data erasure can manifest as an impediment to uncovering the truth and dispensing justice.
- **International Security Cooperation:** Law enforcement agencies, such as Interpol², rely heavily on the exchange of information and data to track fugitive criminals; a mechanism that could be detrimentally impacted by a broad and unchecked enforcement of the right to be forgotten.

² Interpol is the acronym for the International Criminal Police Organization, an international body dedicated to coordinating cooperation among police agencies worldwide. Established in 1923, Interpol is headquartered in Lyon, France, and currently comprises over 190 member states, including Algeria. Its primary mandate does not entail direct, hands-on policing, but rather the facilitation of international security cooperation, particularly in

Accordingly, the core problematic does not reside in the formal recognition of the right to be forgotten itself, but rather in the demarcation of its boundaries and regulatory parameters. This is essential to strike a meticulous equilibrium between the protection of private life and the safeguarding of public interests. Any disproportionate expansion of this right may culminate in an unlawful erasure of memory, whereas its excessive restriction risks keeping individuals perpetual captives of their digital past. Consequently, the optimal solution lies in adopting a flexible, case-by-case approach governed by the strict legal rubrics of necessity, proportionality, and legitimate interest.

Section III: The Merits of the Online Right to Be Forgotten for Children

The enforcement of the right to be forgotten; specifically through mandating search engines and digital platforms to erase or disable access to hyperlinks that infringe upon privacy; acquires heightened significance when applied to children, given their status as digital actors lacking full legal and psychological capacity. Within the digital sphere, a child lacks the comprehensive ability to control the long-term repercussions of information published either about them or by themselves. Consequently, their privacy remains vulnerable to continuous and protracted violations. This vulnerability justifies the adoption of an enhanced protection framework compared to adults, transcending traditional safeguards toward a dual approach that is simultaneously proactive and retrospective.

From this perspective, the right to be forgotten is not merely a technical mechanism for content erasure; rather, it constitutes the legal embodiment of the principle of the "best interests of the child," as enshrined in the Convention on the Rights of the Child (CRC). Furthermore, it serves as an extension of the enhanced protection mandates enacted by contemporary personal data legislation, most notably exemplified by the General Data Protection Regulation (GDPR).

Within this context, the paramount legal, philosophical, and social advantages of enforcing this right for the benefit of children can be delineated as follows:

- **Redrawing the Legal and Ethical Boundaries:** Re-establishing the boundaries between the private and public lives of the child, thereby preventing the digital sphere from mutating into a domain of perpetual exposure of childhood.
- **Preventing Psychological Disorders:** Mitigating psychological distress resulting from the constant re-exposure to obsolete or offensive digital content, thereby bolstering the child's mental and physical well-being.
- **Reconstructing the Child's Psycho-Social Identity:** Restructuring the child's psychological and social framework by enabling them to construct an independent identity unburdened by past digital footprints.
- **Redressing Moral Injury:** Ameliorating the moral damages resulting from digital violations and granting the child an opportunity to regain psychological and social equilibrium.
- **Curtailing the Temporal Continuity of Digital Harm:** Limiting the temporal duration of digital injury by reducing the disseminability of offensive or harmful content across time and platforms.

combating transnational crimes, such as: Terrorism ; Human Trafficking ; Cybercrime ; Drug Trafficking ; Money Laundering ; Its core functions encompass ; Circulating notices regarding individuals wanted internationally by judicial authorities; Facilitating the global exchange of information among police agencies; Coordinating joint operations between member states; Providing international databases, such as biometric data, fingerprints, and stolen travel documents, inter alia.

Consequently, Interpol operates as a global coordination mechanism between sovereign states rather than an independent judicial or policing authority overriding national sovereignty. It epitomizes the conceptual framework of international security solidarity, necessitated by the increasingly transnational nature of contemporary crime. Conversely, however, this apparatus may inadvertently be leveraged for political purposes, in a manner that potentially impinges upon privacy rights.

- Reorganizing the Child's Digital Sphere: Restructuring the digital environment dedicated to children based on the logic of protection rather than the unrestricted dissemination of information.
- Enhancing Legal Recognition: Reinforcing the legal recognition of the child as a proactive rights-holder entitled to control their personal data, rather than a passive subject of data processing.
- Mitigating Digital Crimes Against Children: Contributing to the reduction of various modalities of digital crimes targeted at children by minimizing the availability of content that could be exploited for victimization or extortion.
- Countering Online Grooming: Combating online grooming offenses by reducing the digital footprint that could be leveraged to target vulnerable children.
- Curbing Online Sexual Exploitation: Limiting offenses related to online child sexual exploitation by erasing hyperlinks and content that facilitate access to victims or the re-exploitation of their images.
- Diminishing the Exploitation of Digital Privacy: Curtailing the ability of third parties to exploit children's digital privacy, thereby reinforcing the resilience of the digital sphere against infringements.

In conclusion, the right to be forgotten within the context of childhood is not to be understood merely as a technical prerogative, but rather as a profound philosophical paradigm shift in the concept of digital justice. It is fundamentally predicated on rehabilitating the child as a developing subject in maturation, entitled to a less hostile digital environment; one that is inherently capable of guaranteeing a healthy and secure development, far removed from the inequitable accumulation of an unyielding, permanent digital memory.

Chapter II: The Efficacy of the Right to Be Forgotten and Its Developmental Prospects

This chapter examines the degree of efficacy characterising the right to be forgotten within the digital environment, conceptualising it as one of the most prominent manifestations of the evolution of personal data protection in the contemporary era. This is particularly manifested in light of the institutionalisation of this right under Article 17 of the General Data Protection Regulation (GDPR), which serves as a statutory mechanism empowering individuals to govern their personal data and secure the erasure of information that has rendered inadequate, irrelevant, or excessive over time.³

This chapter aims to analyze the structural limitations of this right by elucidating the impediments that obstruct its enforcement. These obstacles manifest either at the technological level inherent to the unforgiving, permanent nature of the internet; or at the juridical level, arising from the intricate and delicate equilibrium that must be maintained among the right to privacy, freedom of expression, and the public right of access to information.⁴

Furthermore, it seeks to examine the viable mechanisms for bolstering the protection of digital privacy, whether through the evolution of the legislative framework or via the adoption of advanced technological solutions that facilitate a more robust governance of personal data. This exploration is contextualized within the pragmatic problematics associated with the inherent difficulty of absolute erasure from the digital memory, let alone the challenges posed by the transnational proliferation of data across borders.⁵ Within this trajectory, the right to be forgotten emerges as a pivotal legal response to the concept of an "unforgiving internet" that acts as a source of distress for many individuals. This right profoundly reflects the intrinsic human need to reconstruct one's digital

³ Chaudhary, A. The Right to Be Forgotten under GDPR: Legal Scope and Practical Challenges. *International Journal For Multidisciplinary Research (IJFMR)*, 7(4). (2025).

⁴ Jure Globocnik, "The Right to Be Forgotten Is Taking Shape," *GRUR International* 69, no. 4 (2020): 380–392.

⁵ Chaudhary, *Ibid.*, p. 124.

identity, unburdened by past transgressions or informational data that have rendered obsolete and irrelevant.⁶

Furthermore, this chapter outlines a forward-looking perspective on the future trajectory of the right to be forgotten within the digital memory landscape, amid the rapid and exponential proliferation of artificial intelligence and big data. Within this matrix, the overarching problematic is no longer confined to the mere deletion of data from traditional websites or search engines; rather, it has expanded into highly intricate challenges concerning the persistent systemic footprints of this data within ever-evolving algorithmic frameworks, and most notably, emergent quantum technologies. This profound technological shift inevitably necessitates a fundamental reconceptualization of the very notion of digital oblivion within a perpetually mutating technical ecosystem.⁷

Section I: The Limits of the Efficacy of the Right to Be Forgotten within the Digital Environment

Notwithstanding the burgeoning significance of the right to be forgotten as a contemporary legal mechanism seeking to re-establish an equilibrium between an immutable, infinite digital memory and the individual's right to govern their self-image, identity, and privacy, this right provokes profound philosophical and juridical problematics that transcend mere technical enforcement difficulties. From a philosophical vantage point, the digital right to be forgotten directly collides with the concept of historical truth; which is intrinsically owned by the collective history of the nation rather than the individuals themselves; as well as the society's fundamental right to know⁸, consequently, it becomes entirely legitimate to question the validity of rewriting the past or concealing it from others, and whether digital oblivion constitutes a safeguard for personal dignity or a threat to a collective memory essential for shaping the public consciousness of societies.

From a psycho-legal and philosophical perspective, this right exposes a structural tension between conflicting fundamental rights, such as freedom of expression and the right of access to information on one hand, and the right to privacy and personal data protection on the other. This complexity is further exacerbated by the transnational nature of the digital sphere, which engenders intricate problematics regarding the conflict of laws and the sheer difficulty of enforcing judicial mandates upon influential global actors, such as tech conglomerates like Google and Amazon, *inter alia*; whose extraterritorial power and authority occasionally supersede those of sovereign governments and states.⁹

Moreover, the technical ontology of digital data, predicated on its infinite replicability and rapid, ubiquitous dissemination, renders digital oblivion a relative concept rather than an absolute one. Consequently, this right may devolve into a mere reduction of visibility rather than an actual erasure of information. Herein lies a profound empirical paradox induced from reality: the more legal frameworks strive to enforce oblivion, the more the digital memory exhibits resistance driven by social dynamics, as this memory is fundamentally anchored in permanence and accumulation.

Accordingly, the efficacy of the digital right to be forgotten cannot be conceptualized in isolation from a pragmatic, realistic reconceptualization of the relationship among humans, technology, and society, as well as between digital memory and digital oblivion. This is imperative to secure a meticulous equilibrium between individual protection and the safeguarding of the public interest, within an inherently interdisciplinary approach that synthesizes law, philosophy, and technology.

Subsection I: The Technical Impediments to the Enforcement of the Right to Be Forgotten

⁶ Jure Globocnik, *Ibid.*, p. 385

⁷ Garg, S. et al. Formalizing Data Deletion in the Context of the Right to be Forgotten. 2020

⁸ Ricœur, P., *Memory, History, Forgetting*, University of Chicago Press, 2004, pp. 412–415

⁹ CJEU, *Google Spain SL v AEPD*, C-131/12, Judgment of 13 May 2014, paras. 81–85

The most prominent technical impediments obstructing the practical enforcement of the right to be forgotten are delineated as follows:

- **The Inherent Difficulty of Absolute Data Expunction:** The structural challenge of ensuring the complete and irreversible erasure of data from the wider digital environment.
- **The Proliferation of Internet-Published Data:** The phenomenon whereby published informational data seldom remains confined to its primary, original source.
- **Offline Replication and Redundant Storage:** The processes of replicating and archiving data across independent, non-networked storage media, which facilitates the perpetual availability of content online even if the primary source has been officially expunged.
- **Algorithmic Indexing and AI Integration:** The deployment of artificial intelligence algorithms by search engines to archive, index, and systematically log data within the global digital memory.
- **Uncontrollable Dissemination via Social Media Networks:** The systemic difficulty in governing the viral circulation of data across social platforms, rendering mere deletion from the initial source insufficient for achieving genuine, factual oblivion.
- **The Transnational Architecture of the Cyberspace:** The fundamentally borderless nature of the internet, which severely restricts the capacity for technical oversight over personal data that has mutated into a global asset, thereby undermining the feasibility of total expunction from the global digital matrix.

Subsection II: The Legal Impediments

The core problematic surrounding the dialectic between the digital right to be forgotten and the empirical reality of digital memory is not merely confined to the technological dimension; rather, it extends deeply into the legal realm. In various contexts, the right to be forgotten directly instigates¹⁰ a conflict with other fundamental rights and liberties, foremost among which are the freedom of expression and the right to information. Consequently, certain data slated for expunction from the digital memory may possess a profound public interest, particularly when concerning public figures, historical milestones, societal developments, or matters of significant import to domestic or international judiciaries. Herein emerges the pivotal query regarding the definitive boundaries demarcating the protection of digital privacy on one hand, and the preservation of press and media freedoms, alongside other justice-oriented and historical prerogatives, on the other.

Furthermore, the digital right to be forgotten poses an additional complex problematic relative to digital sovereignty across multiple dimensions, fundamentally driven by the inherently transnational architecture of the internet, whether facilitated via submarine cables or satellite networks. From the perspective of a state's digital sovereignty, a judicial or administrative mandate may be issued to expunge specific private digital data within a particular jurisdiction; yet, this data remains accessible in another state due to discrepancies in legislative frameworks or a lack of recognition regarding the equivalent standard of protection. Alternatively, the state wherein the private data remains¹¹ accessible may not be bound by any bilateral or multilateral cooperation agreements in this specific domain with the state that ordered the data expunction.

Section II: Mechanisms for Bolstering the Protection of Digital Privacy

Confronted with these structural impediments, the mere induction or deduction of technical solutions and fragmented legal amendments remains insufficient. Rather, it demands the

¹⁰ Oreste Pollicino & Marco Bassini, "Reconciling Right to Be Forgotten and Freedom of Information", *European Constitutional Law Review*, 2014

¹¹ CJEU, *Google LLC v Commission Nationale de l'Informatique et des Libertés (CNIL)*, C-507/17, Judgment of 24 September 2019.

foundational re-establishment of a conceptual framework for the right to be forgotten within a more comprehensive philosophical and juridical horizon. Consequently, the pursuit of mechanisms to enhance the efficacy of protection fundamentally presupposes an epistemological resolution regarding the core nature of this right: is it to be construed as an advanced extension of the right to privacy, or is it an expression of individual sovereignty over one's narrative identity within the digital temporality?¹² If the human being, as Paul Ricœur contends, is fundamentally a narrative being who continuously reconfigures their selfhood across time, then the right to be forgotten transmutes into an indispensable instrument for rewriting this autobiography. This mechanism functions in a manner that meticulously safeguards human dignity, thereby preventing the reduction of the individual to a past they have definitively transcended.¹³

From this perspective, legal mechanisms transcend a merely procedural nature, integrating instead into the framework of digital governance designed to equilibrate asymmetrical power dynamics specifically, the vulnerability of the individual versus the hegemony of digital platforms. This dynamic necessitates the development of flexible legal rubrics predicated on the principle of proportionality, whereby erasure requests are evaluated in light of meticulous criteria, such as the public interest, the temporality and recency of the information, and the legal status of the data subject (i.e., a private individual versus a public figure). Furthermore, it is imperative to reinforce the transnational enforceability of this right by fostering international cooperation and harmonizing global standards. This approach serves to mitigate the phenomenon of "the globalization of private life," which paradoxically leads to its fragmentation due to discrepancies among domestic legal systems.¹⁴

Regarding the technological trajectory, the overarching challenge must not be confined merely to the erasure of data; rather, it entails the radical reconfiguration of digital architectures themselves in accordance with an *ex-ante* approach of "Privacy by Design." This conceptual framework mandates that data protection be systematically integrated into the very core of technological systems from inception, rather than treated as a subsequent, remedial measure. Within this context, computational tools, such as artificial intelligence, can be strategically deployed to track data proliferation and facilitate the enforcement of judicial erasure mandates; or, at the very least, reduce data visibility; while rigorously ensuring transparency and accountability within the operations of these algorithmic systems.¹⁵

At its core, the endeavor to institutionalize the right to be forgotten reveals a profound paradigm shift in the function of legal philosophy itself: moving from being a mere instrument for behavioral regulation to functioning as a vital mechanism for restoring the ontological equilibrium between the human being and their digital memory. bound not -Consequently, law within this paradigm is duty¹⁶ merely to protect privacy through the rubric of digital data, but rather to safeguard the very possibility of oblivion as a fundamental prerequisite for liberty. Ultimately, it reinstates the human right to refuse being a perpetual captive of one's past within an unforgiving, unforgettable world.

Subsection I: Legal Remediation and Frameworks

These legal solutions must not be conceptualized merely as isolated technical or regulatory measures; rather, they should be construed as the concrete embodiment of a deeper paradigm shift within contemporary legal philosophy. Within this framework, law transitions from the doctrine of passive protection to the doctrine of rights-based empowerment of the individual within the digital sphere. Consequently, the explicit statutory codification of the right to data erasure or the

¹² Court of Justice of the European Union (CJEU), *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González*, Case C-131/12, Judgment of 13 May 2014

¹³ Paul Ricœur posits that personal identity is not an immutable datum, but is rather constructed through narration, which imparts coherence to life across time, wherein the self is configured by organizing the events of existence into a meaningful narrative.

¹⁴ Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, 2019

¹⁵ Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2010

¹⁶ Mireille Hildebrandt, *Law for Computer Scientists and Other Folk*, Oxford University Press, 2020

restriction of data processing does not merely safeguard privacy; it fundamentally establishes what can be conceptualized as "individual informational sovereignty"; meaning the individual's intrinsic capacity to govern the dissemination of various narratives and meanings associated with them within the digital domain.¹⁷

From this perspective, expanding the scope of obligations to encompass diverse digital actors reflects a growing juridical recognition that authority in the digital era is no longer the exclusive monopoly of the state. Rather, it has rendered decentralized and distributed among private actors¹⁸ who possess immense capacity to shape both the social and symbolic realities of individuals. This dynamic necessitates subjecting these private entities within the digital sphere to the doctrine of expanded legal liability, thereby preventing them from mutating into unchecked centers of power operating outside regulatory oversight, and ensuring their reintegration into the matrix of constitutional legitimacy.¹⁹

Furthermore, reinforcing this right with effective oversight mechanisms and independent regulatory bodies aligns with the foundational philosophy of the "digital rule of law." Within this paradigm,²⁰ the legislature does not merely declare rights abstractly but ensures their practical, substantive enforceability. The institutionalization of independent authorities marks a critical transition from abstract trust in digital actors to the logic of institutional accountability. This structural shift bolsters public confidence in the digital legal ecosystem and rectifies the power asymmetry between individuals and digital platforms. At its core, these remedial frameworks reveal a fundamental redefinition of the function of law itself in codifying and modulating digital relations in tandem with technological evolution. Consequently, law evolves into an instrument for redistributing power within the cyberspace, ensuring that technology does not degenerate into a mechanism of hegemony over humanity and society,²¹ but remains instead a domain where human dignity is preserved, and individual liberty to govern one's identity and data is robustly safeguarded.

Subsection II: Technological Remediation and Architecture

Technological instruments must not be reduced to their purely instrumental dimension; rather, they ought to be understood within a broader philosophical and juridical horizon that reconceptualizes the relationship between law and technology as two intertwined normative systems organizing the cyberspace. Consequently, the deployment of encryption methods and data governance frameworks does not merely represent a series of technical solutions; it reflects a transition toward what can be conceptualized as "normative regulation by design" as previously elucidated; wherein technology itself becomes the structural vehicle for legal values, thereby embodying the principles of privacy²² protection within its internal architecture. This perfectly aligns with the landmark thesis "Code is Law" formulated by Lawrence Lessig, who contends that the code constitutes a regulatory²³ framework governing human behavior within cyberspace with an authority equivalent to traditional law; and occasionally, with greater efficacy. This stems from the fact that code predeterminedly dictates what is permissible and what is precluded within the digital ecosystem; consequently, the technological architecture can manifest as a more effective instrument than the statutory rule in regulating digital conduct.

From this perspective, empowering the user to govern their data and comprehend its processing modalities does not merely reside within the logic of protection; rather, it exemplifies the institutionalization of individual autonomy in its digital dimension. In this manner, the individual is rehabilitated as a conscious, proactive actor within the data ecosystem, rather than a passive subject

¹⁷ Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, 2019

¹⁸ Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, 2019

¹⁹ Balkin, J. M., "Old-School/New-School Speech Regulation", 127 *Harvard Law Review*, 2014

²⁰ Black, J., "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", *Regulation & Governance*, 2008.

²¹ Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Edward Elgar, 2015

²² Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, 1999, pp. 68 -72

²³ Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

thereof. This framework robustly reinforces the concept of "comprehensible transparency" in²⁴ contradistinction to mere "formal transparency." Consequently, it rectifies the epistemic imbalance between the profound knowledge possessed by digital platforms and the systemic ignorance suffered by the user.

Regarding the technological alternatives to absolute expunction; such as anonymization, obfuscation, or de-indexing; they provoke a subtle philosophical problematic concerning the very ontology of oblivion: is forgetting the obliteration of existence, the prevention of access to it, or merely the mitigation of its accessibility? Consequently, it becomes manifest that digital oblivion is not an absolute act, but rather a relative, incremental process that reconfigures visibility instead of negating the informational data itself. This remediation reflects a pragmatic approach that accommodates the structural attributes of the digital environment²⁵, which is fundamentally predicated on proliferation and replication; furthermore, it embodies a meticulous equilibrium between two competing interests: the individual's right to fold the pages of their past and society's right to preserve its collective memory.

At its core, these methodologies reveal a paradigm shift in the function of legal protection moving from the doctrine of ex-post remediation following an infringement to the doctrine of ex-ante prevention prior to its occurrence. Within this framework, the statutory rule integrates with the technological instrument to construct a digital ecosystem that safeguards human dignity²⁶. Technology, in this context, is no longer conceptualized as an existential threat to rights, but rather as a viable catalyst for their manifestation, provided it remains tightly circumscribed by a legal logic that guarantees transparency, accountability, and the prevention of any deviation toward novel modalities of covert hegemony.

Section III: The Future Horizons and Developmental Prospects of the Right to Be Forgotten

The future trajectory of the right to be forgotten is inextricably linked to the adaptive capacity of legal systems to keep pace with rapid and exponential technological transformations, particularly in light of the profound evolution in artificial intelligence and big data analytics [INDEX]. These technologies are intrinsically predicated on the aggregation and processing of colossal volumes of personal data, thereby rendering the issue of data expunction for the purpose of oblivion far more complex than the mere removal of content from a specific website or search engine. This complexity arises because personal data may become deeply embedded within algorithmic models or utilized in machine learning processes that are inherently difficult to reverse or entirely erase. Consequently, this dynamic introduces the formidable problematic of what is conceptually recognized as "algorithmic memory."²⁷

Furthermore, the rapid evolution of artificial intelligence is fundamentally reshaping the very ontology of privacy. Within this paradigm, systemic risks are no longer confined to the mere dissemination of information; rather, they extend to the inference of novel data profiles about individuals through predictive analytics, persistent even after the primary, original data has been officially expunged. Consequently, this critical shift impels legal jurisprudence to underscore the imperative of expanding the scope of the right to be forgotten. It must evolve to encompass not merely data erasure, but also the strict curtailment of data reutilization or reconstruction within autonomous intelligent systems.²⁸

Within this context, the fundamental challenge emerges in striking a meticulous equilibrium between the prerequisites of technological innovation on one hand, and ensuring the substantive

²⁴ Lynskey, O., *The Foundations of EU Data Protection Law*, Oxford University Press, 2015, pp. 177–180

²⁵ iktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009, pp. 158-165

²⁶ Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Edward Elgar, 2015, pp. 200–203

²⁷ Garg, S., et al. (2020). Formalizing Data Deletion in the Context of the Right to be Forgotten. arXiv:2002.10635.

²⁸ Kohl, U. (2023). *The Right to Be Forgotten in Data Protection Law*. Cambridge University Press.

protection of fundamental human rights; foremost among which is the right to digital privacy on the other. Consequently, current national and international legislative frameworks, notwithstanding their profound significance, such as the General Data Protection Regulation (GDPR), may prove insufficient on their own to confront the technical complexities inherent to artificial intelligence [INDEX]. This limitation inevitably necessitates the adoption of novel, more agile and adaptive legal paradigms tailored to the perpetually shifting digital environment.²⁹

Subsection I: The Future of the Right to Be Forgotten in the Era of Artificial Intelligence

Artificial intelligence imposes qualitative challenges upon the right to be forgotten, which are not merely confined to the technological dimension but extend to resurrecting fundamental inquiries regarding the very nature of digital memory, digital identity, and justice within the digital era. Intelligent systems do not merely store data and information; rather, they reproduce, analyze, and infer novel semantic dimensions therefrom. This capability ensures that personal data; even post-expunction can resurface in the form of algorithmic inferences or predictive outcomes. Consequently, this dynamic mutates the problematic from the simple deletion of an informational datum into a profounder dilemma concerning the systemic footprint of information and its persistence within algorithmic structures.³⁰

From a philosophical perspective, the 'right to be forgotten' reflects an existential conflict between two antithetical rationales: the techno-logic of perpetual digital memory, and the human logic of forgetting, which serves as a fundamental prerequisite for self-reconstitution and transcending the past. As Paul Ricoeur posits, the human subject necessitates forgetting to reshape their identity, whereas digital systems tend to institutionalize the past, transmuting it into an indelible, immutable datum. Herein lies the peril of algorithmic determinism, which threatens to confine individuals³¹ within typologies predicated on historical data, thereby infringing upon the principle of human dignity and the freedom of personal development.

Jurisprudentially, this paradigm shift necessitates broadening the scope of the 'right to be forgotten' to encompass not merely raw data, but also the very models and decisions derived therefrom. Erasing data from a specific database does not ipso facto eliminate its residual impact on an artificial intelligence model trained upon it; a conundrum that gives rise to the so-called 'right to algorithmic forgetting'. Consequently, this demands the formulation of novel regulatory frameworks, such as mandating system retraining or adopting machine unlearning techniques aimed at expunging the footprint of specific data from intelligent models³².

Furthermore, this dynamic engenders profound dilemmas regarding digital justice, wherein archaic or inaccurate data may implicitly perpetuate discrimination or social stigmatization via algorithmic operations. At this nexus, the 'right to be forgotten' intersects with other foundational principles, such as the right not to be subject to purely automated decision-making, and the right to transparency and explanation, as enshrined in the General Data Protection Regulation (GDPR). Consequently, the right to be forgotten becomes integral to a broader, comprehensive matrix aimed at safeguarding the human subject from absolute technological memory, and restoring equilibrium between informational hegemony and the lived human experience.³³

Subsection II: Toward an Equilibrium Model between Privacy, Digital Memory, and Freedom of Expression

The future evolution of the 'right to be forgotten' cannot be predicated on the logic of the absolute erasure of digital memory; such an approach fundamentally contradicts the intrinsic function of memory as a vehicle for preserving collective knowledge and ensuring the continuity of historical

²⁹ Globocnik, J. (2020). The Right to Be Forgotten Is Taking Shape. *GRUR International*, 69(4), 380–392. Oxford University Press.

³⁰ Garg, S., et al. (2020). Formalizing Data Deletion in the Context of the Right to be Forgotten. *arXiv*.

³¹ Paul Ricoeur, *Memory, History, Forgetting* (Chicago: University of Chicago Press, 2004), p. 412.

³² Uta Kohl, *The Right to Be Forgotten in Data Protection Law* (Cambridge: Cambridge University Press, 2023), p. 85.

³³ Jure Globocnik, "The Right to Be Forgotten Is Taking Shape," *GRUR International* 69, no. 4 (2020): 380–392.

truth. Conversely, the unfettered circulation of information, absent regulatory safeguards, poses a grave infringement upon digital privacy, transmuting cyberspace into a permanent punitive memory that relentlessly stalks individuals with their past transgressions. Hence, the 'right to be forgotten'³⁴ emerges as a legal and philosophical mechanism aimed at orchestrating a delicate equilibrium between the imperatives of memory and the exigencies of forgetting between that which must be preserved and that which ought to be effaced.

From a philosophical perspective, this equilibrium mirrors a profound dialectic articulated by Paul Ricoeur, wherein a 'just memory' is inconceivable devoid of a certain measure of forgetting, just as an obliteration that culminates in the obfuscation of truth remains utterly unacceptable. Consequently, functional forgetting constitutes a vital prerequisite for self-reconstitution; nonetheless, it must remain tethered to ethical constraints that prevent it from degenerating into an instrument of factual denial or historical revisionism.³⁵ In the digital context, this dilemma becomes increasingly complex, given that technology inherently tends toward total archiving, thereby threatening to reduce the human subject to an entity permanently circumscribed by their digital past.

Jurisprudentially, this equilibrium finds its doctrinal foundation in judicial precedent, most notably in the jurisprudence of the Court of Justice of the European Union (the landmark *Google Spain* case, 2014). Therein, it was robustly affirmed that the 'right to be forgotten' is not an absolute right; rather, it is strictly contingent upon a proportionality test that balances it against the freedom of expression and the public's right to access information. This principle has further evolved within the framework of the General Data Protection Regulation (GDPR), which instituted a flexible, case-by-case approach [GDPR]. This approach is predicated on explicit criteria, including the intrinsic nature of the information, its degree of accuracy, the temporal lapse since its initial publication, and its substantive contribution to a debate of public interest, in tandem with the legal status of the data subject: whether a private individual or a public figure.³⁶

This methodology reveals a qualitative shift in legal philosophy, transitioning from a jurisprudence of rigid codification to a jurisprudence of balancing, wherein controversies are settled not by abstract statutory texts, but through the weighing of competing values in light of the specificities of each case. Furthermore, this aligns seamlessly with Habermas's conceptualization of the public sphere, which mandates the unfettered circulation of information, yet strictly within a normative framework that safeguards human dignity and fundamental rights³⁸. Accordingly, the 'right to be forgotten', in its evolved manifestation, aims not to obfuscate historical truth or curtail the freedom of the press, but rather to mitigate the disproportionate repercussions of the digital past upon the present. This calibrated mechanism enables the human subject to reconstruct their identity without repudiating facts intrinsically tied to the public interest. Ultimately, it signifies the right to re-establish a temporal equilibrium between past and present, thereby guaranteeing that digital memory does not degenerate into a mechanism of perpetual hegemony, and conversely, that forgetting does not serve as a subterfuge for escaping accountability.

Conclusion

In ultimate synthesis, the digital 'right to be forgotten' transpires not as a mere technical mechanism for data erasure, but as a profound paradigm shift redefining contemporary digital jurisprudence and existential philosophy. This study has demonstrated that this prerogative represents a dual-faceted construct: on one hand, it serves as an advanced extension of privacy that empowers individuals to reconstruct their self-image and safeguards human dignity from the psychological weight of permanent digital documentation. On the other hand, its enforcement remains strictly

³⁴ Ricœur, P., *Memory, History, Forgetting*, University of Chicago Press, 2004, pp. 444–448.

³⁵ Ricoeur, P. (2004). *Memory, History, Forgetting*. University of Chicago Press.

³⁶ Court of Justice of the European Union (2014). *Google Spain SL v. AEPD and Mario Costeja González*, Case C-131/12.

³⁷ Globocnik, J. (2020). *The Right to Be Forgotten Is Taking Shape*. GRUR International, 69(4), 380–392.

³⁸ Habermas, J., *The Structural Transformation of the Public Sphere*, MIT Press, 1989, pp. 27–30.

relative, inherently intersecting with competing democratic imperatives such as freedom of expression, the public's right to know, and the preservation of collective historical memory. Notably, this balance assumes a heightened normative sensitivity regarding children, transmuting the right from a conventional legal safeguard into a proactive, remedial instrument designed to insulate childhood development from the hazards of perpetual digital exposure.

Furthermore, this investigation underscores that the efficacy of digital oblivion is severely constrained by systemic technological impediments. The internet's infrastructure predicated on infinite replication and uncontrollable transnational networks directly challenges traditional legal instruments anchored in territorial sovereignty. This complexity is further exacerbated by the rise of artificial intelligence and big data analytics. Consequently, the legal dilemma is no longer confined to raw data; it extends to algorithmic models that perpetuate automated decisions even after primary sources are expunged. Therefore, enhancing this right necessitates a holistic synthesis of legal evolution and technological advancement, primarily through institutionalizing 'privacy by design' and fostering global cyber-cooperation.

Ultimately, the right to be forgotten reflects a qualitative evolution in legal philosophy, transitioning from the doctrine of absolute certainty to a framework of proportionality. It remains an evolving legal project open to continuous refinement. The fundamental challenge resides not in the methodology of total obliteration, but in the governance of an unforgiving technological memory ensuring that the human subject does not become a perpetual captive of their digital past, while simultaneously guaranteeing that societies do not forfeit their historical consciousness.

References

- Court of Justice of the European Union (CJEU), *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González*, Case C-131/12, Judgment of 13 May 2014
- CJEU, *Google Spain SL v AEPD*, C-131/12, Judgment of 13 May 2014
- CJEU, *Google LLC v Commission Nationale de l'Informatique et des Libertés (CNIL)*, C-507/17, Judgment of 24 September 2019.
- Court of Justice of the European Union (2014). *Google Spain SL v. AEPD and Mario Costeja González*, Case C-131/12.
- Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2010
- Balkin, J. M., "Old-School/New-School Speech Regulation", 127 *Harvard Law Review*, 2014
- Black, J., "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", *Regulation & Governance*, 2008.
- Chaudhary, A. The Right to Be Forgotten under GDPR: Legal Scope and Practical Challenges. *International Journal For Multidisciplinary Research (IJFMR)*, 7(4). (2025).
- Garg, S. et al. Formalizing Data Deletion in the Context of the Right to be Forgotten. 2020
- Garg, S., et al. (2020). Formalizing Data Deletion in the Context of the Right to be Forgotten. *arXiv:2002.10635*.
- Globocnik, J. (2020). *The Right to Be Forgotten Is Taking Shape*. GRUR International, 69(4),. Oxford University Press.
- Habermas, J., *The Structural Transformation of the Public Sphere*, MIT Press, 1989.
- Iktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009.

Jure Globocnik, "The Right to Be Forgotten Is Taking Shape," GRUR International 69, no. 4 (2020)

Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, 2019

Jure Globocnik, "The Right to Be Forgotten Is Taking Shape," GRUR International 69, no. 4 (2020): 380–392.

Kohl, U. (2023). *The Right to Be Forgotten in Data Protection Law*. Cambridge University Press.
Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, 1999.

Lynskey, O., *The Foundations of EU Data Protection Law*, Oxford University Press, 2015.

Mireille Hildebrandt, *Law for Computer Scientists and Other Folk*, Oxford University Press, 2020

Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Edward Elgar, 2015

Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Edward Elgar, 2015

Paul Ricoeur, *Memory, History, Forgetting* (Chicago: University of Chicago Press, 2004), p. 412.

Ricoeur, P. (2004). *Memory, History, Forgetting*. University of Chicago Press

Uta Kohl, *The Right to Be Forgotten in Data Protection Law* (Cambridge: Cambridge University Press, 2023), p. 85