IRSHAD International Journal of Law and Policy | Volume: 3, Issue: 3
2025

The Right to be Forgotten in the Digital Age: A Comparative Analysis of Legal Practice in the EU, USA, Russia, And Uzbekistan

Pulatov Temurbek*
Tashkent State University of Law

Jalolova Khafiza**
Tashkent State University of Law

Abstract

This article provides a comprehensive examination of the right to be forgotten, comparing its legal foundations, interpretations, and enforcement across four jurisdictions: the European Union, the United States, the Russian Federation, and the Republic of Uzbekistan. It explores how cultural values, constitutional principles, and political environments shape the practical scope of data-erasure provisions and delisting requests in each setting. Through a comparative legal methodology, the research draws on statutes, court rulings, academic publications, and advocacy group reports to illustrate the delicate balance between privacy protection and freedom of expression. The analysis gives particular attention to the General Data Protection Regulation in the European Union, state-level privacy laws in the United States, legislative amendments in Russia, and evolving data-protection norms in Uzbekistan. Key findings highlight the influence of differing legal cultures, institutional structures, and enforcement mechanisms on the efficacy of the right to be forgotten, while also addressing the potential misuse of erasure requests to stifle public-interest information. The article concludes by considering prospects for cross-border cooperation and the continued evolution of data-protection frameworks amid rapidly changing technologies.

Keywords: Right to be Forgotten, Data Protection, GDPR, Privacy Law, Comparative Law, Uzbekistan, Digital Rights

APA Citation:

Pulatov, T., & Jalolova, K. (2025). The Right to be Forgotten in the Digital Age: A Comparative Analysis of Legal Practice in the EU, USA, Russia, And Uzbekistan. *International Journal of Law and Policy, 3* (3), 1-16. https://doi.org/10.59022/ijlp.301

I. Introduction

The exponential growth of digital technologies has magnified the reach and persistence of personal data, prompting legal scholars and policymakers to grapple with how best to protect individuals' privacy interests. One increasingly prominent solution is the so-called right to be forgotten, which grants data subjects the ability, under certain circumstances, to request the erasure or delisting of personal information from online sources (Kohl, 2023). This right has sparked considerable debate in jurisdictions around the world, as its interpretation implicates core tensions between privacy and freedom of expression (Dror-Shpoliansky & Shany, 2021). On one hand, the right to be forgotten offers individuals a mechanism to counterbalance perpetual online memory, particularly when outdated or misleading information lingers in ways that harm reputation or personal development.

On the other hand, civil society organizations argue that overly broad erasure mandates can restrict essential public records and suppress valid journalistic, academic, or civic investigations. These concerns highlight the delicate interplay between individual rights and the collective good in digital environments, where a single jurisdiction's rules may have extraterritorial consequences. Moreover, this right interacts with the commercial interests of internet intermediaries such as search engines, which often shoulder the burden of evaluating and acting upon erasure requests (Alessi, 2017). In practice, the wide variation in national laws and legal cultures has led to inconsistent outcomes, fueling calls for greater harmonization. Nonetheless, local specificities persist, reflecting the diverse constitutional values and historical contexts in each legal system. By situating the right to be forgotten within its comparative global context, this article aims to illuminate both its theoretical foundations and the practical challenges of effective implementation (AllahRakha, 2025).

In the European Union, the right to be forgotten is most closely associated with Article 17 of the General Data Protection Regulation (GDPR), which codifies the conditions under which data subjects can request the removal of personal data (European Parliament & Council, 2016). This explicit legal provision emerged partly in response to the Court of Justice of the European Union's ruling in Google Spain SL v. AEPD and Mario Costeja González, where the court held that search engines function as data controllers. As a result, individuals can demand delisting of links to content that is "inadequate, irrelevant or no longer relevant," subject to various exemptions for freedom of expression, historical archiving, and public interest. Despite this clarity, EU Member States exhibit divergent enforcement approaches, reflecting localized judicial interpretations and enforcement priorities of national Data Protection Authorities.

Additionally, private search engines become the arbiters of whether a request meets GDPR thresholds, raising questions about transparency, due process, and

potential overclocking. Meanwhile, critics note that digital footprints often persist in cached archives or across social media platforms, limiting the practical efficacy of erasure. Consequently, although the EU model stands out for its robust legislative basis, stakeholders continue to debate the scope and global reach of delisting orders. These debates underscore how the right to be forgotten operates at the nexus of legal clarity and technological complexity, with outcomes shaped by institutional design and market forces (Erdos, 2021).

The United States presents a stark contrast to the EU, given its emphasis on freedom of speech and its more fragmented legal framework for data protection. At the federal level, no statute mirrors the GDPR's Article 17, and courts have historically been reluctant to compel removals of lawfully published information, citing First Amendment protections. Nonetheless, certain states, led by California, have introduced narrower provisions that approximate elements of the right to be forgotten, such as granting minors the ability to remove their own online postings (Voss & Houser, 2019).

The California Consumer Privacy Act (CCPA) further allows residents to request deletion of personal data, although it contains multiple exceptions for legal compliance, security, and other legitimate business interests. These isolated initiatives do not form a cohesive national policy, and courts typically prioritize the constitutional interest in preserving access to archives and historical records. Consequently, an individual's success in seeking data erasure depends heavily on contextual factors, including the type of information in question and the prevailing interpretation of free speech norms. Observers note that the U.S. approach reflects deep-seated constitutional traditions, even as privacy advocates campaign for stronger federal regulations. Though incremental changes are underway in various states, a holistic American right to be forgotten remains elusive.

Russia adopted a statutory measure commonly characterized as an RTBF law in 2015, primarily through Federal Law No. 264-FZ amending earlier legislation on information and IT protection. This law grants individuals the right to request that search engines remove links to information deemed "irrelevant," "outdated," or "in violation of the law," thereby mirroring certain European principles. However, legal analysts caution that the Russian law lacks the detailed exceptions and procedural guarantees found in the GDPR, giving rise to concerns about potential overreach or censorship. Additionally, observers point to limited transparency in how Roskomnadzor, the body tasked with media and communications oversight, interprets and enforces these provisions.

Critics argue that public figures may exploit the law to stifle criticism or silence disclosures about corruption and human rights abuses. Given the sparse availability of consistent judicial decisions or official removal data, it remains challenging to assess the law's broader social impact. Notwithstanding these uncertainties, Russia's RTBF-like framework underscores how normative ideals of data privacy can be reframed in

ways that diverge from Western liberal conceptions. In practice, domestic political considerations, centralized oversight, and the ambiguity of key legal terms can create an environment where legitimate privacy claims and attempts at censorship intermix. As a result, the Russian experience underscores the fluid boundary between personal privacy and broader public interests, revealing how a right intended to empower individuals can become entwined with state-driven content regulation (Peters, 2015).

Uzbekistan offers a contrasting example of a jurisdiction where data-protection norms remain nascent, shaped by recent reforms aimed at modernizing the legal framework. Enacted in 2019, the Law on Personal Data outlines general privacy principles but stops short of establishing a fully-fledged right to be forgotten akin to the EU's (Republic of Uzbekistan, 2019). Nonetheless, it provides mechanisms for correcting or deleting inaccurate data, hinting at an eventual progression toward more explicit erasure rights. Implementation is overseen by multiple agencies, though detailed procedures for challenging refusals or for applying public interest exemptions are not widely documented.

The evolving nature of Uzbekistan's digital governance, sometimes referred to under broader "Digital Uzbekistan" initiatives, suggests a willingness to adopt international best practices while accommodating local regulatory goals. However, critics warn that without robust transparency guarantees and independent judicial review, erasure rights could be abused to suppress material critical of authorities or politically influential actors. These conditions underscore the fluid dynamic at play, as emerging legal systems adapt global privacy discourses within local cultural, political, and infrastructural contexts. Such adaptation highlights the interplay between normative aspirations for data protection and pragmatic constraints in legislating and enforcing new digital rights.

In drawing these four jurisdictions into a single comparative lens, it becomes apparent that the right to be forgotten cannot be divorced from a society's underlying constitutional ethos. The EU's approach prioritizes data-subject empowerment within a unified legislative framework, even if enforcement remains decentralized among Member States. By contrast, the United States emphasizes freedom of expression, limiting broad erasure mandates and allowing only targeted statutes, primarily at the state level. Russia occupies a middle ground in theory, adopting a delisting procedure that ostensibly parallels the EU's, yet critics argue that its opaque implementation risks chilling public discourse.

Uzbekistan's journey reflects the challenges of building robust data-protection rules in a developing regulatory environment, where there is potential for both progressive policies and abuses of power. These variations underscore that the right to be forgotten is not merely a legal instrument but a prism through which broader societal values and power relationships are refracted. While some principles, such as respect for personal dignity, resonate across jurisdictions, the mechanisms for balancing such dignity against collective transparency differ markedly. Understanding

these variations is crucial for policymakers, scholars, and internet intermediaries seeking to navigate the global patchwork of data-erasure rights.

Accordingly, the remainder of this article explores the materials and methods deployed in analyzing each jurisdiction's relevant statutes, case law, and policy discussions, followed by detailed findings on the contours of the right to be forgotten in practice. The discussion then synthesizes these findings into broader insights about the interplay of law, technology, and social values, shedding light on the various ways in which erasure requests can be fulfilled, denied, or misappropriated. By investigating areas of convergence and divergence, the study highlights prospects for cross-border collaboration and warns of the potential for conflicts where legal systems impose extraterritorial delisting mandates.

Ultimately, the analysis reveals that a one-size-fits-all model for personal data erasure is difficult to achieve, given the uniqueness of constitutional frameworks and societal norms. Nonetheless, mutual learning among jurisdictions may help refine procedures, strengthen safeguards, and moderate the risk of abuse. From a methodological standpoint, the article draws on a mixture of primary sources such as legislation and court rulings and secondary commentary from scholarly journals, advocacy reports, and policy briefs. This dual approach illuminates both the formal structures of the right to be forgotten and the lived realities of those attempting to invoke it. With this context in place, the next section outlines the methodological underpinnings of the comparative analysis, setting the stage for a deeper examination of results.

II. Methodology

This study adopts a comparative legal framework to examine how the right to be forgotten is defined, implemented, and contested in the European Union, the United States, Russia, and Uzbekistan. Comparative analysis is particularly suitable because it highlights how distinct legal traditions conceptualize privacy, the public interest, and the role of government regulation. By focusing on four jurisdictions, the research captures a range of cultural and constitutional values, thereby demonstrating how a single legal concept can manifest differently across contexts. The core data set comprises legislative texts, judicial opinions, and guidance documents from regulatory bodies, supplemented by reports from nongovernmental organizations and scholarly articles in law journals.

Official legislative portals and databases, including EUR-Lex, Congress.gov, pravo.gov.ru, and lex.uz, were consulted to ensure accuracy and currency. Notable judicial rulings, such as Google Spain, Martin v. Hearst Corp. (2015), and various data-protection enforcement decisions, provided interpretive insight into the real-world application of erasure provisions. Additionally, this article integrates policy briefs from organizations like Access Now and ARTICLE 19 to contextualize human rights considerations. By combining primary and secondary sources, the research

develops a multidimensional picture of how the right to be forgotten operates on paper and in practice.

A critical aspect of the methodology involved identifying recurring themes across jurisdictions, such as the relationship between erasure rights and freedom of expression, the scope of delisting obligations, and the existence of exceptions for historical or journalistic content. These themes were used to structure the analysis, ensuring that parallel issues were examined in each legal system. While the EU's GDPR was reviewed in detail through its official text and relevant case law, U.S. materials were gathered from both federal sources and state-level statutes, including the California Consumer Privacy Act. For Russia, the focus was on Federal Law No. 264-FZ and secondary commentaries highlighting the ambiguity and potential for censorship.

Uzbekistan's Law on Personal Data was assessed alongside official declarations of the nation's modernization and digital governance agenda. Through this approach, the research systematically traced each statute's evolution, interpretive documents, and real or potential enforcement challenges. Such triangulation was necessary to account for gaps, given that some court decisions or administrative practices are not fully disclosed publicly. Moreover, analyzing reports from advocacy groups shed light on the human impact of the right to be forgotten, illuminating cases where erasure demands may stifle significant public information. By collating these diverse materials, the study built a robust basis for comparison.

In evaluating how local courts or regulatory agencies handle requests for data removal, the methodology paid close attention to procedural safeguards, appeals mechanisms, and transparency requirements. For instance, the EU typically defers to national Data Protection Authorities to decide complaints, supported by the overarching framework of the European Data Protection Board, whereas U.S. enforcement often hinges on a mix of private litigation and state-level consumer protection agencies. Russia's reliance on Roskomnadzor raises unique questions about independence and the potential for political influence, while Uzbekistan's distributed oversight structures remain relatively untested.

By cataloging these institutional differences, the study clarifies how certain jurisdictions provide stronger checks against misapplication of erasure rights, whereas others lack clear channels for appeal or public transparency. Additionally, technical documents and guidance on implementing delisting procedures especially from major search engine providers helped illustrate how decisions are made in practice. The topic of extraterritoriality also formed a key part of the analysis, given that courts in the EU have grappled with whether delisting orders should extend beyond European domains. Identifying where each legal system stands on this issue reveals potential flashpoints in cross-border data governance. This lens demonstrates how the right to be forgotten can create friction with competing jurisdictions that either do not recognize its legitimacy or prioritize free speech differently. Such conflicts underscore the necessity

of international dialogue and possibly harmonized principles to manage a right with inherently global ramifications.

Methodologically, it was also crucial to probe the sociopolitical contexts in which each jurisdiction's law operates. In Russia, for example, the law's implementation must be understood against a backdrop of tightened state control over media and online discourse, which has implications for the sincerity of privacy protections. Meanwhile, Uzbekistan's legal reforms are part of broader modernization efforts that may introduce advanced data-protection measures or, alternatively, constrain free expression under certain circumstances. By integrating academic critiques and investigative reports, the analysis attends to the possibility that official narratives about privacy rights may mask deeper power imbalances.

This holistic reading of legal texts situated within local political and cultural realities enables a more precise evaluation of whether the right to be forgotten is implemented ethically and effectively. Furthermore, it helps distinguish between laws that genuinely protect citizens' privacy and those potentially exploited to silence dissent or manipulate online narratives. While such critiques also apply, in differing degrees, to the EU and the United States, they are especially pronounced in jurisdictions where media pluralism is limited. By foregrounding these considerations, the methodology aims to avoid a purely doctrinal lens that overlooks the lived realities of legislative enforcement.

Ethical considerations in this study are minimal, as the research uses publicly available sources and does not involve human subjects or personal data collection. Nevertheless, efforts were made to confirm the reliability of cited materials and to account for potential biases in advocacy group reports or government statements. Where conflicting accounts of particular cases or laws arose, the analysis either sought corroboration from multiple sources or indicated the contested nature of the information. Such transparency is pivotal when addressing a topic as potentially politicized as data erasure, where stakeholders may have strong incentives to shape public perception.

Additionally, the comparative approach recognizes that legal systems evolve, and new amendments, court rulings, or policy shifts may influence the interpretation of the right to be forgotten after the research is completed. To accommodate these dynamic elements, the study focuses on legal developments and case law up to 2025, acknowledging that subsequent shifts might alter the conclusions drawn here. Finally, the presentation of results aims to maintain clarity and impartiality, outlining both the strengths and limitations of each jurisdiction's model. This balanced perspective sets the stage for the subsequent discussion of findings.

The mixed-method comparative design facilitates a structured yet context-sensitive examination of the right to be forgotten. Legislative texts and official rulings anchor the analysis in positive law, while secondary commentary and NGO reports provide interpretive depth, highlighting the real-world impact of erasure demands. By

grouping observations into thematic clusters such as freedom-of-expression clashes, enforcement mechanisms, and extraterritorial scope the research can systematically compare and contrast developments in the EU, the United States, Russia, and Uzbekistan. These findings are then synthesized to uncover broader patterns and recurring issues, including potential misuses of the right to be forgotten to sanitize reputations or stifle public debate.

Given that the practice of data erasure often involves private intermediaries responding to user requests, the methodology also includes a brief assessment of corporate transparency reports and self-regulatory guidelines. This multi-faceted perspective not only reflects the complexity of the right but also underscores the importance of robust oversight in preventing unintended consequences. With the methodology established, the article now turns to presenting the results, offering a detailed look at the legislative frameworks, institutional structures, and key controversies in each jurisdiction. These results highlight the interplay of law, politics, and technology, laying the groundwork for the subsequent discussion. Having clarified the methodological approach, the next section delves into the specific outcomes of this comparative inquiry.

III. Results

Comparative analysis underscores how the European Union maintains the most detailed statutory basis for the right to be forgotten, anchored by Article 17 of the General Data Protection Regulation. This legislation codifies the ability of data subjects to request erasure in scenarios such as data no longer being necessary for the original purpose or when consent is withdrawn. Notably, exceptions exist for freedom of expression, legal obligations, and archival or public interest reasons, reflecting an effort to balance privacy with broader societal values. Data Protection Authorities in each Member State enforce these provisions, guided by frameworks established by the European Data Protection Board and further refined by the Court of Justice of the European Union.

Although this structure suggests a high degree of harmonization, differences still emerge among national regulators interpreting the scope of delisting. In practice, major search engines receive thousands of erasure requests weekly, leading to evolving internal guidelines on how to process them. Critics argue that delegating these judgments to private entities raises accountability concerns, especially when content of significant public interest is at stake. Nonetheless, supporters of the EU approach emphasize that a codified right to be forgotten is preferable to a piecemeal system, given that it offers citizens a clear legal pathway to address ongoing harm from outdated or misrepresentative data (de Bruin, 2022).

In the United States, legal precedents diverge from the European norm due to constitutional protections of speech under the First Amendment, which often override privacy claims. No federal law parallels Article 17 of the GDPR, although some state

laws provide narrower mechanisms for data deletion, especially concerning minors. The California Consumer Privacy Act (CCPA) goes further by granting residents the right to request deletion of personal data held by certain businesses, yet it includes exceptions for data required to fulfill legal or contractual obligations.

Consequently, the scope and strength of these erasure rights vary depending on the nature of the data, the entity controlling the data, and the relevant state's legislative environment. When disputes arise, courts typically weigh privacy interests against the public benefit of open archives, particularly regarding lawfully published news articles or historical records. The patchwork nature of U.S. data protection thus produces uneven outcomes, occasionally frustrating individuals who seek comprehensive online erasure. Meanwhile, privacy advocates argue for broader protections, though any such reforms face strong opposition from civil-liberties groups and media organizations wary of censorship. These dynamics place the United States at the forefront of the global debate over how to reconcile personal privacy with free speech (Myers, 2016).

Russia's 2015 adoption of a right-to-be-forgotten law indicates an attempt to replicate aspects of the EU model, but the legislative language and enforcement methods differ significantly. Search engines are obliged to remove links considered outdated or inapplicable, though criteria for determining relevance are not always transparent. Roskomnadzor, the federal body overseeing media and communications, manages complaints, but observers note concerns about undue political influence in decision-making. Reports suggest that some high-profile requests originate from public figures wishing to erase negative coverage, raising worries that the law could facilitate selective censorship. While there may be legitimate privacy interests at stake, the ambiguity surrounding enforcement frameworks and minimal disclosure of statistical data hinder external scrutiny.

Additionally, the law's references to information that violates "other legislative requirements" open the door to broad interpretations that may impinge on investigative journalism or dissenting viewpoints. Critics emphasize that the right to be forgotten, as implemented in Russia, risks conflating privacy protection with instruments of state control. Despite these issues, some Russians have successfully removed outdated or irrelevant information that no longer represents their current circumstances, indicating at least partial adherence to the principle of data erasure. Nonetheless, the line between legitimate privacy and manipulative delisting remains difficult to draw, exemplifying the complexity of applying the right to be forgotten in contexts where freedom of expression is constrained.

In Uzbekistan, the Law on Personal Data (No. ZRU-547) provides a general framework for individuals to correct or delete erroneous data, although it does not articulate an explicit right to be forgotten similar to the GDPR's Article 17. This law has been part of a wider modernization agenda, often referred to as "Digital Uzbekistan," aimed at updating legal and administrative structures to align with international standards. Enforcement, however, is relatively untested, and little case

law exists to clarify how courts should respond to disputes over data erasure or delisting requests. Multiple agencies share oversight responsibilities, which can lead to bureaucratic fragmentation and a lack of clear guidelines for citizens who seek data removal. International observers have pointed out that reforms to bolster data privacy might inadvertently be used to limit public disclosure if politically sensitive information is targeted.

Furthermore, the legal framework is not fully harmonized with global norms, leaving questions about whether Uzbekistan will formally adopt a broader right to be forgotten in the future. Some civil society organizations advocate for stronger procedural safeguards and transparency requirements, believing these measures could prevent abuses and strengthen trust in digital governance. Officials, for their part, often highlight the necessity of fostering robust e-government services that protect privacy while enabling data-driven innovation. This dual emphasis reflects the tensions inherent in legislating data erasure rights within a transitioning political and legal system. At present, Uzbekistan remains a developing arena for data protection, where the potential for an expanded right to be forgotten hinges on future legislative and judicial developments.

Beyond these formal frameworks, practical outcomes depend on how legal norms intersect with broader social and technological contexts. Implementation of the EU's right to be forgotten, for instance, depends heavily on the internal protocols of search engines, which must evaluate requests on a case-by-case basis. The actual decisions to delist content often rest with private compliance teams applying guidelines derived from court rulings and regulatory advice. In the United States, the mosaic of privacy statutes and strong free speech traditions place individuals in a position of navigating multiple jurisdictions and standards, with success rates varying significantly. Meanwhile, Russia's experiences suggest that legal language alone does not guarantee a balanced approach; instead, political realities and administrative practices shape outcomes.

Uzbekistan's current system underscores how nascent laws can lead to uncertainty, as the lack of robust precedential rulings complicates the actual exercise of any right to erasure. In each jurisdiction, the tension between ensuring personal control over data and protecting public interest data is a recurring theme. Additionally, the issue of extraterritorial delisting arises when content is hosted outside a jurisdiction's territory, complicating enforcement across global internet infrastructure. These varied contexts reveal that the efficacy of the right to be forgotten is not solely determined by legal texts but also by institutional capacities, political cultures, and the global reach of online services.

A further dimension of the results pertains to potential abuses of the right to be forgotten. Data-subjects sometimes request erasure not only to remove inaccurate information but also to hide relevant details about criminal, financial, or professional misconduct. In the EU, this concern has prompted calls for more stringent public-

interest exceptions, as data controllers must balance personal reputational rights with the public's entitlement to knowledge about matters of importance. The United States, due to strong free speech safeguards, is less vulnerable to such abuses in formal terms; yet limited data-deletion rights at the state level could still be leveraged selectively.

In Russia, the relative opacity surrounding who requests content removal and under what justification could facilitate politically motivated or reputation-based censorship. Uzbekistan, given its stage of legislative development, may face similar risks if clarity about exceptions and public oversight remains insufficient. Ultimately, these findings indicate that robust procedural guidelines, transparency reports, and oversight mechanisms are necessary to distinguish valid privacy claims from attempts to distort public memory. Without such safeguards, the right to be forgotten can unintentionally become an instrument of private or governmental censorship.

Taken as a whole, the results highlight a tapestry of legal strategies, institutional variables, and sociopolitical factors that define how each jurisdiction applies or interprets the right to be forgotten. The EU stands out for its explicit legal framework and relatively developed enforcement system, though it still contends with discrepancies among Member States. The United States maintains a free speech-centric perspective that restricts the scope of data erasure mandates, albeit with emerging pockets of consumer privacy legislation. Russia's model aligns nominally with the EU but can be subverted by political forces, while Uzbekistan's approach remains in flux, shaped by nascent reforms. Across all four jurisdictions, balancing data-subject rights with transparent public records remains a central concern. Additionally, extraterritorial disputes underscore the challenges posed by a global internet, where one state's request for delisting may collide with another's free speech norms or limited recognition of a right to be forgotten.

IV. Discussion

The findings suggest that the right to be forgotten is not a monolithic concept but rather a fluid legal construct that takes on different forms depending on constitutional priorities, enforcement practices, and cultural attitudes. In the European Union, explicit codification through the GDPR has supported robust data-subject rights, tempered by specific exemptions that reflect a broader tradition of balancing personal privacy with public transparency. Yet, disputes about global delisting reveal tensions between national sovereignty and the borderless nature of online speech, making it difficult to consistently apply erasure mandates outside EU territory.

The United States, in contrast, underscores how decentralized governance and entrenched free speech norms can limit the expansion of data-erasure rights, creating a patchwork environment where success depends on specific state statutes or contexts. The American reluctance to endorse an EU-style right to be forgotten ties directly to the perceived risk of rewriting history and inhibiting investigative journalism. Although consumer privacy legislation is gradually gaining traction, any federal

measure akin to Article 17 would likely face significant constitutional hurdles, illustrating the persistence of cultural and legal divides.

Meanwhile, Russia exemplifies how legislation resembling a right to be forgotten can be leveraged in ways that contravene its stated goal of privacy protection, raising questions about political influence and insufficient checks. Taken together, these insights reveal that legislative formalities, while important, do not alone determine outcomes; institutional independence, transparency, and accountability also shape how erasure rights function in practice (AllahRakha, 2024). Notably, one of the most contested aspects across jurisdictions pertains to carving out sufficient exceptions for socially valuable information. In the EU, Article 17(3) of the GDPR attempts to limit unwarranted deletions by preserving journalistic freedoms, academic research, and the public interest in records of criminal or political significance. However, operationalizing these exceptions can be complex, as search engines and regulators often navigate ambiguous or context-dependent scenarios.

In Russia, vague statutory language can hinder clarity about what constitutes "irrelevant" information, thereby opening the door to subjective interpretations that favor powerful interests. Uzbekistan's legislation does not yet offer a refined delineation of public-interest exceptions, leaving the practical balancing act to future guidelines or precedents. The United States, by centering free speech as a baseline, generally sidesteps the question of how to define exceptions, but in doing so, it also limits data subjects' ability to expunge harmful or obsolete personal information. These varied approaches demonstrate that regulating the right to be forgotten necessitates careful legal drafting and robust procedural oversight. Where laws are imprecise, they risk either excessive censorship or inadequate protection of personal privacy, underscoring the pivotal role of nuanced legal structures and independent adjudication (AllahRakha, 2023).

The complexities identified in implementing the right to be forgotten are further amplified by technological factors. Even in the EU, where delisting is well established, search engines struggle with the logistical challenges of evaluating large volumes of removal requests. The presence of mirrored sites, archived pages, and social media reposts complicates the notion of truly eliminating information from the internet. Similar patterns emerge in Russia, although fewer formal constraints on state intervention mean that content can sometimes be blocked or removed more comprehensively if deemed unlawful. In the United States, the limited scope of erasure rights means many of these technical issues surface primarily in private negotiations with data holders or in the context of specific consumer privacy statutes.

Uzbekistan, with its developing digital infrastructure, may confront such challenges as internet usage expands and more citizens become aware of data-protection rights. In all cases, the interplay between legal mandates and online platforms underscores the importance of clarifying the responsibilities and liabilities of intermediaries. Without clear guidelines, companies may adopt erratic or overly

cautious approaches, potentially suppressing lawful content to avoid legal risks. Such self-regulation by private entities can inadvertently undermine democratic values, unless balanced by procedural safeguards and transparent oversight. As the volume and velocity of online data grow, these technological dimensions of the right to be forgotten are poised to become even more pronounced.

A recurring concern in all four jurisdictions involves the possible misuse of erasure rights for reputation laundering, whereby individuals seek to eliminate documentation of legitimate wrongdoing or controversies. While the EU's exceptions aim to limit such scenarios, critics argue that the policy sometimes leads to the suppression of information that, although outdated, retains public relevance. In the United States, the combination of strong press freedoms and narrower erasure laws means abusers find it harder to leverage formal mechanisms for that purpose, although takedown notices and private settlement pressures can still create chilling effects. Russia's experience indicates that the application of a right to be forgotten in a politically controlled environment allows powerful actors to shape public discourse by sidelining inconvenient historical facts.

Uzbekistan's relative inexperience with data-erasure requests means the law's potential for misuse remains untested, yet the risk endures if procedural safeguards are not established. These patterns imply that a right initially championed as a privacy measure can, in less transparent contexts, morph into a tool for censorship. Indeed, when minimal accountability surrounds delisting processes, or when courts cannot freely evaluate the merits of removal requests, the boundary between legitimate data protection and manipulative erasure erodes. Such misuse risks undermining the normative appeal of the right to be forgotten, turning an ostensibly benevolent privacy remedy into a mechanism for concealing corruption, unethical conduct, or other matters of public concern.

Comparative analysis also illuminates opportunities for cross-border cooperation or at least mutual learning among legislators, regulators, and technology companies. The EU's approach, with its structured exceptions and case-law guidance, could offer insights for states or nations that wish to refine delisting procedures while respecting free expression. In turn, the U.S. emphasis on safeguarding historical and journalistic integrity highlights the need for robust free speech protections, even within a privacy-centric framework. Russia's model shows how gaps in clarity and independence can compromise the stated goals of data protection, serving as a cautionary tale about conflating privacy with broader content regulation. Uzbekistan's nascent system underscores that newly established legal regimes should incorporate transparency, defined procedures, and judicial review from the outset, rather than retrofitting such safeguards later.

These reciprocal lessons indicate that, although national sovereignty complicates uniform rules, shared best practices or bilateral agreements might mitigate conflicts when erasure requests cross international boundaries. Some proposals even

envision global standards for privacy and data portability, though these remain aspirational given deep-seated legal and cultural differences. Nonetheless, the convergence of digital markets and the cross-border nature of online speech make a purely isolationist approach untenable, especially when a single search engine may operate under multiple, sometimes conflicting, data-regulation regimes. By seeking dialogue and alignment where feasible, regulators could help ensure that the right to be forgotten evolves responsibly, balancing personal privacy with the legitimate needs of open societies.

Altogether, the discussion confirms that the right to be forgotten stands at the intersection of complex legal, political, and technological forces. Its diverse manifestations in the EU, the United States, Russia, and Uzbekistan exemplify how each jurisdiction's unique constitutional ethos influences the balance between privacy rights and freedom of expression. Legislative detail alone does not guarantee fair implementation, as demonstrated by the Russian experience, nor does a strong free speech culture necessarily address all privacy harms, as seen in the United States. In a rapidly changing digital environment, ongoing judicial interpretations, policy amendments, and societal debates will continue to reshape the contours of data erasure.

Understanding the nuances of each jurisdiction's practices fosters a deeper appreciation of how legal instruments function in real-world contexts, with outcomes ranging from genuine privacy protection to potential censorship. The subsequent section presents final reflections on these issues, synthesizing the lessons gleaned from this comparative inquiry. By situating these findings in the broader arena of global data governance, the article endeavors to highlight both the promise and the peril of granting individuals the ability to rewrite their digital footprints. Ultimately, the conclusions aim to inform a balanced path forward, attentive to the needs of personal autonomy, freedom of expression, and societal accountability.

Conclusion

The right to be forgotten traverses legal landscapes shaped by divergent constitutional principles, cultural values, and enforcement capacities. In the European Union, explicit statutory provisions help citizens invoke data-erasure rights while still recognizing key public-interest limitations. The United States underscores how free speech considerations can heavily constrain robust privacy mandates, leaving data subjects reliant on state-specific laws. Russia's model reveals the pitfalls of vague legal language and limited institutional checks, which may enable censorship under the guise of privacy. Uzbekistan, for its part, is still forging its path in data governance, illustrating both the potential and the risks associated with emerging digital rights. Despite these differences, all four jurisdictions struggle to delineate the boundary between legitimate privacy protections and the public's interest in transparent historical and journalistic records. As data volumes grow and digital

footprints expand, the demand for balanced, equitable models of information governance will intensify.

Where official transparency is robust and judicial independence is secure, the right to be forgotten can function as an effective remedy against unfair online stigmatization. Conversely, in contexts where political pressures dominate or where no clear legal safeguards exist, attempts at privacy reform risk enabling censorship and historical revisionism. The complexity of cross-border data flows also suggests that purely national approaches will invariably face jurisdictional conflicts. Nonetheless, incremental progress can emerge through shared dialogues, policy experimentation, and heightened public awareness of digital rights. In balancing these competing interests, the true potential of the right to be forgotten will hinge on thoughtful legislative design, consistent regulatory oversight, and ongoing engagement with emerging technologies. Achieving that balance is a collective challenge, underscoring the need for legal innovation, comparative research, and transparency in governance. Ultimately, striking a proportionate equilibrium between privacy and collective memory remains both a pressing and an open-ended endeavor.

The debate over the right to be forgotten therefore epitomizes broader questions about how societies regulate and preserve knowledge in the digital age. While legal frameworks differ widely, common themes include the tension between individual autonomy and the public good, the role of private intermediaries in shaping online discourse, and the complexity of enforcing erasure across international boundaries. By examining the European Union, the United States, Russia, and Uzbekistan, this article has highlighted critical lessons and cautionary tales that may inform future reforms. Whether through court rulings, legislative amendments, or administrative guidelines, each jurisdiction will likely revisit the contours of data erasure as internet technologies evolve. Yet, the convergence of policy debates and civic demands suggests that the right to be forgotten will remain central in discussions of digital privacy and free expression. Such prominence underscores the need for nuanced lawmaking, diligent oversight, and active public engagement.

Bibliography

Alessi, S. (2017). *Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation*. *Emory International Law Review, 32*(1), 145. Retrieved from https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1186&context=eilr

AllahRakha, N. (2023). Regulatory barriers impacting circular economy development. *International Journal of Management and Finance, 1*(2). https://doi.org/10.59022/ijmf.29

AllahRakha, N. (2024). Rethinking digital borders to address jurisdiction and governance in the global digital economy. *International Journal of Law and Policy, 2*(1). https://doi.org/10.59022/ijlp.124

AllahRakha, N. (2025). National policy frameworks for AI in leading states. *International Journal of Law and Policy, 3*(1), 38–51. https://doi.org/10.59022/ijlp.270

de Bruin, R. (2022). A comparative analysis of the EU and U.S. data privacy regimes and the potential for convergence. *Hastings Science & Technology Law Journal, 13*(2), 127–168. https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1115&context=hastings_science_technology_law_journal

Dror-Shpoliansky, D., & Shany, Y. (2021). It's the end of the (offline) world as we know it: From human rights to digital human rights – A proposed typology. *European Journal of International Law, 32*(4), 1249–1282. https://doi.org/10.1093/ejil/chab087

Erdos, D. (2021). The 'right to be forgotten' beyond the EU: An analysis of wider G20 regulatory action and potential next steps. *Journal of Media Law, 13*(1), 1–35. https://doi.org/10.1080/17577632.2021.1884947

Kohl, U. (2023). The right to be forgotten in data protection law and two Western cultures of privacy. *International and Comparative Law Quarterly, 72*(3), 737–769. https://doi.org/10.1017/S0020589323000258

Myers, C. (2016). Digital immortality vs. "the right to be forgotten": A comparison of U.S. and E.U. laws concerning social media privacy. *Romanian Journal of Communication and Public Relations, 16*(3), 47–60. https://doi.org/10.21018/rjcpr.2014.3.175

Peters, A. (2015). *Corruption and human rights* (Working Paper No. 20). Basel Institute on Governance. https://www.mpil.de/files/pdf4/Peters_Corruption_and_Human_Rights20152.pdf

Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: Providing a competitive advantage for U.S. companies. *American Business Law Journal, 56*(2), 287–344. https://doi.org/10.1111/ablj.12139