World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Data privacy and the right to be forgotten

Geraldine O. Mbah *

LL.B. University of Benin, Benin City, Nigeria.

World Journal of Advanced Research and Reviews, 2022, 16(02), 1216-1232

Publication history: Received on 13 September 2022; revised on 17 November 2022; accepted on 20 November 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.16.2.1079

Abstract

In the digital era, data privacy has become a critical issue as vast amounts of personal information are collected, processed, and stored by corporations, governments, and online platforms. The growing reliance on data-driven technologies, including artificial intelligence and big data analytics, has heightened concerns over the security and ethical handling of personal data. Amid these concerns, the *Right to Be Forgotten* (RTBF) has emerged as a legal and ethical concept aimed at granting individuals' greater control over their digital footprint. This right, enshrined in the European Union's General Data Protection Regulation (GDPR), allows individuals to request the removal of their personal data from search engine results and other online repositories when it is no longer relevant, necessary, or lawfully processed. While RTBF enhances personal autonomy and privacy, it presents significant challenges, including conflicts with freedom of expression, the practicality of enforcement across jurisdictions, and the implications for transparency in digital records. Additionally, the implementation of RTBF varies globally, with jurisdictions like the United States resisting its adoption due to strong protections for free speech. The tension between privacy rights and public interest necessitates a nuanced approach to data governance, incorporating technological solutions such as differential privacy and automated compliance mechanisms. As digital ecosystems expand, policymakers must balance privacy protections with the legitimate interests of businesses, media, and society at large. This paper explores the legal, ethical, and technical dimensions of RTBF, providing a comparative analysis of global frameworks and proposing policy recommendations to ensure effective data privacy governance in an increasingly interconnected world.

Keywords: Data Privacy; Right to Be Forgotten; GDPR; Digital Footprint; Freedom of Expression; Data Governance

1. Introduction

1.1. Background and Context

The rise of digital technology has fundamentally reshaped global economies, leading to an era where data is often regarded as the new oil. Rapid advancements in artificial intelligence, cloud computing, and big data analytics have enabled businesses, governments, and individuals to harness vast amounts of personal and behavioral data for decision-making and innovation [1]. With the proliferation of smartphones, smart devices, and social media platforms, individuals generate and share more personal information than ever before. This shift has created a highly data-driven economy where digital footprints influence everything from personalized marketing strategies to predictive analytics in various sectors, including healthcare, finance, and law enforcement [2].

However, as data collection practices grow more sophisticated, concerns over personal data security have intensified. The increasing frequency of data breaches, unauthorized surveillance, and identity theft incidents has heightened awareness about privacy risks associated with excessive data exposure. Major cybersecurity incidents, such as the Cambridge Analytica scandal and large-scale leaks of sensitive personal data, have demonstrated the vulnerabilities

* Corresponding author: Geraldine O. Mbah

inherent in data-driven systems [3]. These incidents have led to widespread debates on digital privacy, consumer rights, and the ethical responsibilities of corporations handling personal information [4].

Governments, corporations, and individuals all play crucial roles in safeguarding data privacy. Regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have established legal mechanisms to enhance personal data protection and grant individuals more control over their digital identities [5]. Meanwhile, corporations are increasingly under pressure to implement transparent data governance policies, encryption standards, and privacy-enhancing technologies to mitigate risks. At the individual level, users are adopting cybersecurity measures such as two-factor authentication, encrypted messaging apps, and privacy-focused web browsers to limit their digital exposure [6].

Despite these efforts, the challenge of balancing data-driven economic benefits with privacy rights remains a contentious issue. While data analytics drive innovation and business growth, excessive data collection and inadequate regulatory enforcement pose risks to civil liberties and digital autonomy. This dynamic has fueled the ongoing discussion on the Right to Be Forgotten (RTBF) as a potential solution to safeguard individuals' ability to control their personal data in an era of persistent digital records [7].

1.2. Significance of Data Privacy

The protection of personal data is crucial in preserving individual autonomy, safeguarding human dignity, and ensuring trust in digital systems. As more personal information is digitized, the risks associated with unauthorized access, profiling, and targeted surveillance continue to grow. Data privacy is not just a technical concern but an ethical and legal imperative that impacts various aspects of modern society, including human rights, economic stability, and national security [8].

From an ethical perspective, the exposure of personal data without consent violates the fundamental right to privacy. Individuals should have control over how their personal information is collected, stored, and shared. Unauthorized data collection practices, particularly those driven by artificial intelligence and algorithmic decision-making, raise concerns about discrimination, bias, and social inequalities [9]. For example, automated hiring processes that analyze candidates' online presence may inadvertently reinforce biases and compromise fairness in recruitment decisions [10].

Legally, data privacy is enshrined in various national and international regulations that aim to protect individuals from privacy violations and data exploitation. The GDPR, for instance, mandates that organizations obtain explicit consent before processing personal data and grants individuals the right to request data erasure under certain conditions. Similarly, data privacy laws in the United States, such as the CCPA, provide consumers with legal avenues to challenge the misuse of their personal information [11].

Beyond legal and ethical concerns, data exposure can have far-reaching societal implications. The widespread availability of personal data increases risks such as identity theft, reputational damage, and financial fraud. Additionally, unchecked data collection practices by tech companies and governments raise fears about mass surveillance, limiting freedom of expression and access to unbiased information [12]. As digital interactions become more pervasive, robust data privacy protections are essential to maintaining democratic values and personal security.

1.3. Introduction to the Right to Be Forgotten (RTBF)

The Right to Be Forgotten (RTBF) is a legal and philosophical concept that grants individuals the ability to request the removal of personal information from digital records under specific circumstances. Originating from privacy rights discourse, the RTBF gained prominence with the landmark *Google Spain SL v. Agencia Española de Protección de Datos* case in 2014, where the European Court of Justice ruled that search engines must remove links to outdated or irrelevant personal information upon legitimate request [13]. This ruling established the foundation for individuals to regain control over their digital presence, particularly in cases where personal data negatively impacts their reputation or well-being [14].

Since its legal recognition, RTBF has been incorporated into various data protection frameworks, most notably the GDPR, which provides explicit guidelines on the conditions under which individuals can exercise this right. Under GDPR Article 17, individuals can request data erasure if the information is no longer necessary for its original purpose, if consent is withdrawn, or if data processing is unlawful. However, exceptions exist, particularly in cases where public interest, freedom of expression, or legal obligations justify retaining the data [15].

Despite its legal adoption, RTBF remains highly controversial. Critics argue that enforcing data removal requests conflicts with fundamental rights such as freedom of speech and access to information. News organizations and search engines have voiced concerns that RTBF could be misused to suppress legitimate public records, creating a "memory hole" effect that alters historical accuracy [16]. Additionally, the global nature of digital information complicates enforcement, as different jurisdictions have varying interpretations of privacy laws. While the EU enforces RTBF strictly, other countries, including the United States, emphasize First Amendment protections, limiting its applicability in non-European regions [17].

As digital footprints become increasingly permanent, RTBF continues to spark debates on the balance between privacy rights and the public's right to access information. The evolution of this concept reflects broader tensions in digital governance, highlighting the need for nuanced policies that consider both individual privacy and societal transparency [18].

2. Theoretical foundations of data privacy and the right to be forgotten

2.1. Philosophical and Ethical Foundations

Privacy has long been recognized as a fundamental human right, deeply embedded in legal, philosophical, and ethical discourses. The right to privacy is enshrined in key human rights documents, such as Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, emphasizing that individuals should be protected from arbitrary interference with their personal lives [5]. In the digital age, where vast amounts of personal information are stored and shared online, the philosophical interpretation of privacy has evolved to include the right to control one's digital identity and the ability to manage how personal data is used and disseminated [6].

However, ethical dilemmas arise when balancing individual privacy rights with societal interests. Governments and corporations collect and process vast amounts of user data, often justifying such practices on the grounds of national security, fraud prevention, or economic benefits. This raises concerns about consent, as individuals often lack awareness or control over how their personal information is utilized. The ethical principle of autonomy dictates that individuals should have the right to make informed decisions about their personal data, yet many digital services operate on complex terms of use that obscure data practices, undermining genuine consent [7].

Another key ethical challenge is the trade-off between privacy and transparency. While privacy advocates argue that individuals should have control over their digital presence, journalists, historians, and legal professionals stress that information should remain accessible for the public interest. The Right to Be Forgotten (RTBF) exemplifies this tension, as requests for data removal can potentially conflict with the right to access truthful information, raising concerns about censorship and historical revisionism [8].

Additionally, ethical concerns arise regarding data bias and discrimination. AI-driven data collection systems often reinforce societal biases, affecting marginalized communities disproportionately. The lack of stringent ethical guidelines in digital privacy governance raises critical questions about accountability and fairness in data processing. As digital privacy becomes a cornerstone of modern human rights discussions, ethical frameworks must evolve to address these complexities while maintaining a balance between individual freedoms and collective interests [9].

2.2. Legal Foundations of Data Privacy

Data privacy is governed by a variety of legal frameworks that seek to protect individuals from unauthorized data collection and misuse. The General Data Protection Regulation (GDPR) of the European Union is one of the most comprehensive data privacy laws, granting individuals control over their personal information and mandating strict data protection requirements for organizations. Under GDPR, individuals can request the deletion of their data under the RTBF provision, provided it does not conflict with public interest or legal obligations [10].

Similarly, the California Consumer Privacy Act (CCPA) grants consumers the right to know what personal data is collected, the ability to opt out of data sales, and the right to request data deletion. While less stringent than GDPR, the CCPA represents a significant shift in U.S. data privacy regulations, emphasizing consumer empowerment and corporate accountability [11]. Other jurisdictions, such as Brazil with its Lei Geral de Proteção de Dados (LGPD) and Canada with the Personal Information Protection and Electronic Documents Act (PIPEDA), have implemented similar regulations, reflecting the growing global recognition of data privacy rights [12].

Comparative legal perspectives on RTBF highlight critical differences in how nations approach data erasure requests. The European Union strictly enforces RTBF, requiring search engines and online platforms to comply with user requests unless a strong public interest is demonstrated. However, in the United States, free speech protections under the First Amendment often override RTBF claims, limiting its applicability in American digital landscapes [13]. Countries such as Japan and India are gradually incorporating RTBF into their legal frameworks but face challenges in balancing privacy rights with information accessibility.

A major legal challenge in data privacy enforcement is jurisdictional complexity. Digital data flows transcend national borders, making it difficult to enforce privacy laws uniformly. Cases such as *Google v. CNIL* highlight the limitations of RTBF enforcement beyond the EU, as courts ruled that search engines are not obligated to apply RTBF globally, restricting its effectiveness in a borderless digital world [14]. This ongoing legal evolution underscores the need for international cooperation in developing harmonized data privacy standards that ensure robust yet fair protection for individuals [15].

2.3. Technological Aspects of Data Privacy

Technology plays a critical role in safeguarding data privacy, with encryption, anonymization, and access control serving as foundational mechanisms for protecting personal information. Encryption ensures that data remains secure during storage and transmission, preventing unauthorized access by encoding information in an unreadable format that requires decryption keys. Modern encryption standards such as Advanced Encryption Standard (AES) and Transport Layer Security (TLS) are widely used to secure sensitive data across various industries, from banking to healthcare [16].

Anonymization is another key privacy-enhancing technique, involving the removal of personally identifiable information (PII) to prevent data from being linked to specific individuals. Methods such as differential privacy, which injects statistical noise into datasets, help balance data usability with privacy protection. However, de-anonymization techniques have raised concerns, as researchers have demonstrated that anonymized datasets can often be re-identified when combined with external data sources, posing a significant challenge for ensuring long-term privacy [17].

Access control mechanisms further enhance data privacy by restricting user permissions based on authentication protocols. Role-based access control (RBAC) and multi-factor authentication (MFA) help organizations manage data access more securely, reducing the risk of unauthorized breaches. AI-driven cybersecurity tools are increasingly used to monitor and detect anomalous access patterns, providing an additional layer of security in protecting sensitive information [18].

Despite these advancements, ensuring complete erasure of digital footprints remains a major technological challenge. When individuals request data deletion under RTBF, complete removal is often difficult due to redundant storage in backup systems, distributed servers, and decentralized networks. Blockchain technology, with its immutable ledger system, further complicates data erasure, as stored transactions cannot be modified or deleted retroactively. This raises questions about how RTBF can be effectively enforced in decentralized ecosystems [19].

Additionally, search engine algorithms and data indexing create persistent records of online content, making it challenging to erase personal information permanently. Even when data is deleted from a specific platform, cached versions and third-party archives may still retain copies, limiting the effectiveness of RTBF implementation. As a result, researchers are exploring privacy-enhancing technologies such as "ephemeral computing," which designs systems where data expires automatically after a predefined period, reducing long-term exposure risks [20].

While technological advancements have improved data privacy protections, they also highlight the inherent limitations in achieving absolute digital erasure. Moving forward, the integration of privacy-by-design principles in software development, coupled with stronger regulatory enforcement, will be essential in ensuring that individuals retain control over their digital identities in an increasingly interconnected world [21].

3. Legal and regulatory landscape of the right to be forgotten

3.1. General Data Protection Regulation (GDPR) and RTBF

The General Data Protection Regulation (GDPR), introduced by the European Union (EU) in 2018, established one of the most comprehensive legal frameworks for data protection, with the Right to Be Forgotten (RTBF) as a core provision. Codified under Article 17, RTBF grants individuals the right to request the deletion of personal data when it is no longer necessary for its original purpose, when consent is withdrawn, or when data processing is unlawful. This legal

foundation is based on the principle that individuals should have control over their digital presence, especially in cases where outdated or irrelevant information harms their privacy or reputation [9].

Enforcement mechanisms under the GDPR require data controllers, such as search engines, social media platforms, and corporations, to assess RTBF requests on a case-by-case basis. Organizations must comply unless a legitimate exemption applies, such as the public interest in accessing information, journalistic freedom, or legal obligations. The European Data Protection Board (EDPB) provides guidelines to ensure uniform implementation across EU member states. Non-compliance can result in substantial fines—up to €20 million or 4% of a company's annual global revenue, whichever is higher [10].

For organizations, GDPR's RTBF introduces significant compliance challenges. Businesses operating in the EU or handling data of EU citizens must establish data governance frameworks to process erasure requests efficiently. This requires robust data management policies, as personal data may exist across multiple servers, backups, and third-party platforms. Additionally, verifying request legitimacy while preventing fraudulent claims adds complexity to implementation [11].

Another major challenge is handling conflicts between GDPR and jurisdictions with differing data retention laws. For example, financial institutions and healthcare providers are often required to retain records for regulatory compliance, even when individuals request data deletion. This conflict between privacy rights and statutory obligations creates legal uncertainties that organizations must navigate [12].

Despite these challenges, GDPR's RTBF has significantly influenced global data protection policies. Many countries outside the EU are using GDPR as a blueprint for their own privacy regulations, leading to increased adoption of RTBF in various legal systems [13].

3.2. RTBF in Non-EU Jurisdictions

3.2.1. United States: Conflicts with Free Speech Laws

Unlike the EU, the United States does not have a federal law granting RTBF. The First Amendment, which guarantees freedom of speech and press, often takes precedence over privacy claims. Courts have ruled that public interest in accessing truthful information outweighs individuals' rights to have their data removed. This is evident in cases involving news archives, where courts have consistently rejected attempts to erase publicly available content [14].

However, some states have taken steps toward strengthening privacy rights. The California Consumer Privacy Act (CCPA) grants residents the right to request deletion of personal data collected by businesses, though it does not apply to search engines or publicly available records. Legal scholars continue to debate whether a U.S. version of RTBF could be implemented without infringing on free speech protections [15].

3.2.2. Asia and Latin America: Emerging Regulations and Adaptation

Several Asian countries are adopting RTBF within broader data protection laws. Japan's Act on the Protection of Personal Information (APPI) includes provisions allowing individuals to request data deletion if it is deemed unnecessary or unlawfully obtained. However, enforcement remains inconsistent, as Japanese courts weigh privacy claims against press freedom and business interests [16].

In South Korea, the Personal Information Protection Act (PIPA) grants individuals the right to request the removal of personal data from search engines under certain conditions. This has led to an increasing number of successful erasure requests, particularly concerning outdated criminal records and defamation cases. Nonetheless, South Korea faces challenges in harmonizing RTBF with its strong commitment to transparency in governance [17].

Latin America has also seen a growing recognition of RTBF, influenced by GDPR. Brazil's Lei Geral de Proteção de Dados (LGPD) includes a right to deletion similar to GDPR's RTBF, though its enforcement is still evolving. Argentina and Mexico have incorporated RTBF-like provisions in their data protection laws, but the scope remains limited compared to EU standards. Enforcement challenges, particularly regarding digital platforms operating across multiple jurisdictions, hinder consistent implementation [18].

3.2.3. Africa and Developing Regions: Legal Gaps and Policy Developments

Many African and developing nations lag behind in implementing RTBF due to weak data protection laws and limited regulatory oversight. South Africa's Protection of Personal Information Act (POPIA) provides some privacy rights, but it does not explicitly recognize RTBF. Similarly, Nigeria's Data Protection Regulation (NDPR) includes provisions for data deletion but lacks strong enforcement mechanisms [19].

In developing regions, the primary challenge lies in balancing privacy rights with digital access. Many countries rely on foreign tech companies for internet services, limiting their ability to enforce national data privacy laws. Additionally, governments in some nations prioritize surveillance and data retention for security reasons, making RTBF difficult to implement effectively [20].

Despite these challenges, international advocacy groups and legal scholars are pushing for stronger privacy protections in developing nations. As global digital governance evolves, it is likely that more countries will incorporate RTBF principles into their data protection frameworks [21].

3.3. Controversies and Criticisms

RTBF remains one of the most debated aspects of modern data privacy laws. Critics argue that it conflicts with fundamental rights, particularly freedom of speech and access to information. Journalists and historians have expressed concerns that RTBF could be used to erase significant historical events, undermining public accountability. For example, public figures may attempt to remove controversial past statements or legal records, effectively altering the digital archive of history [22].

Another major criticism is the burden placed on search engines and online platforms. Google, for instance, has received millions of RTBF requests since GDPR's implementation, requiring it to assess each case individually. This process is resource-intensive and subjective, leading to inconsistencies in enforcement. Additionally, critics argue that granting private companies the power to determine whether information should be erased or retained sets a problematic precedent, as corporate interests may influence decision-making [23].

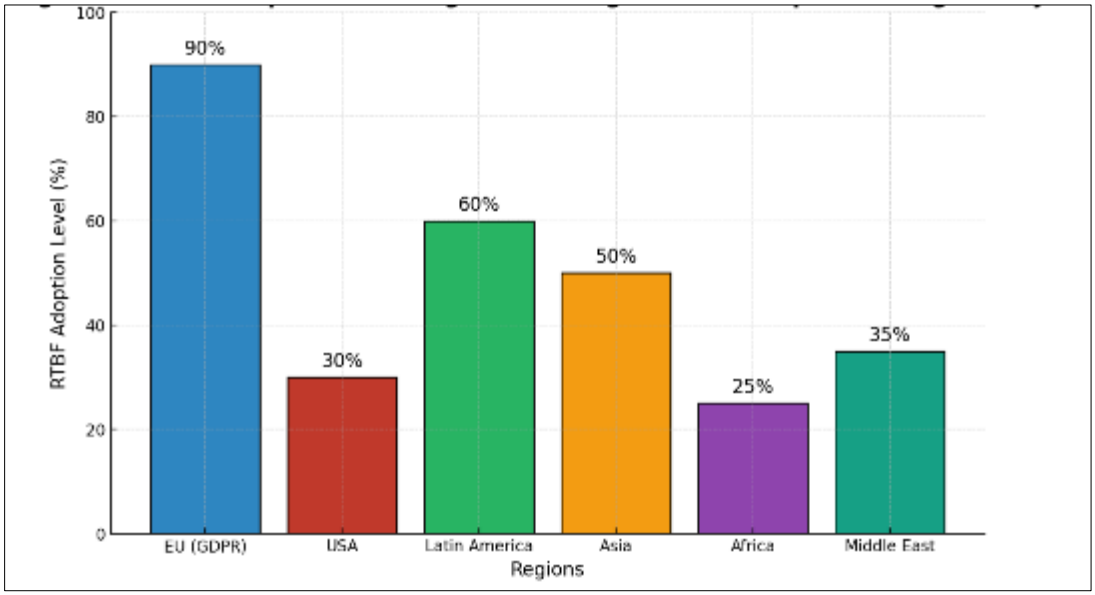

Figure 1 Global Adoption of the Right to Be Forgotten – A Comparative Legal Analysis

Moreover, RTBF does not guarantee complete data erasure. Even when search engines remove links, the original content often remains on the hosting website. This creates a loophole where information is still accessible through direct searches or alternative search engines that do not adhere to EU regulations. The effectiveness of RTBF is further limited in decentralized online spaces, such as blockchain networks, where data cannot be altered or deleted once recorded [24].

Despite these concerns, RTBF remains a vital component of digital privacy laws, offering individuals a means to reclaim control over their personal data. The challenge moving forward is striking a balance between privacy protection and

public interest. Legal scholars suggest refining RTBF by introducing clearer guidelines on when data deletion requests should be honored, ensuring that privacy rights do not infringe on essential freedoms [25].

Figure 1 illustrates the adoption of RTBF across different jurisdictions, highlighting variations in legal enforcement and policy development. While GDPR has set a global standard, significant disparities exist in how nations approach privacy rights, reflecting broader tensions between digital governance, free expression, and individual autonomy [26].

4. Technological challenges and implementation of RTBF

4.1. Technical Feasibility of RTBF

Implementing the Right to Be Forgotten (RTBF) presents significant technical challenges due to the interconnected nature of digital networks. In an era where personal data is distributed across multiple servers, platforms, and jurisdictions, completely erasing information from the internet is far more complex than simply deleting a record from a single database. The redundancy of digital storage systems means that even if data is removed from one platform, cached versions or mirrored copies may persist elsewhere, making enforcement difficult [12].

One of the primary challenges in RTBF implementation is the decentralized structure of the internet. When individuals submit RTBF requests, search engines such as Google can remove links to personal data from search results, but they cannot compel third-party websites to delete the original content. This creates a loophole where information remains accessible through direct searches, alternative search engines, or archived snapshots stored on services like the Wayback Machine [13].

Cloud computing further complicates RTBF enforcement. Cloud service providers store data across geographically dispersed servers, making it difficult to determine which jurisdiction's privacy laws apply. Even if a request is granted under the General Data Protection Regulation (GDPR), cloud backups and redundant storage systems may still retain copies of the data. Many cloud architectures use automated replication to ensure high availability, inadvertently prolonging the existence of personal information beyond the intended deletion date [14].

Additionally, blockchain technology poses a unique challenge to RTBF due to its immutable nature. Data recorded on blockchain ledgers cannot be modified or erased without invalidating the entire chain. While some privacy-focused blockchain solutions incorporate techniques like zero-knowledge proofs to limit data exposure, fully implementing RTBF in blockchain systems remains an open challenge [15].

From a technical standpoint, addressing these issues requires a combination of legal, procedural, and technological measures. Encrypted storage and ephemeral computing offer potential solutions by ensuring that data expires after a predefined period. Meanwhile, organizations can implement stricter access controls and automated data retention policies to minimize unnecessary long-term storage of personal information [16].

4.2. AI, Big Data, and RTBF

The rise of artificial intelligence (AI) and big data has intensified privacy concerns, making the enforcement of RTBF more challenging. AI-driven tracking systems collect, analyze, and categorize vast amounts of user data, often without explicit consent. From behavioral analytics to predictive profiling, AI-powered algorithms continuously aggregate personal information, raising significant privacy risks [17].

One of the primary concerns is that AI systems enable deep data mining, allowing companies to reconstruct deleted information from various sources. Even if a user successfully removes their data from a particular platform, AI models trained on previous interactions can infer missing details, effectively undermining RTBF efforts. This is particularly problematic in targeted advertising and recommendation engines, where historical data plays a crucial role in personalization [18].

Moreover, AI-powered surveillance tools used by governments and corporations for security and fraud detection continuously process vast amounts of personal data. Facial recognition systems, biometric databases, and automated decision-making tools rely on persistent data storage, making it difficult for individuals to erase their digital footprints entirely. These systems often operate outside traditional RTBF enforcement mechanisms, creating significant legal and ethical challenges [19].

Despite these concerns, AI also offers potential solutions for RTBF enforcement. Machine learning models can automate the detection and removal of personal information from search engines, social media platforms, and databases. AI-powered content moderation tools can identify sensitive data and flag it for deletion based on predefined criteria, streamlining compliance with privacy laws [20].

Another promising approach involves federated learning, where AI models are trained on decentralized data sources without exposing raw user data. By reducing centralized data retention, federated learning can enhance privacy protections while still allowing AI-driven services to function effectively. Implementing AI-driven encryption techniques, such as homomorphic encryption, further strengthens RTBF enforcement by ensuring that data remains inaccessible after deletion requests are processed [21].

In the evolving landscape of digital privacy, AI remains both a threat and a solution. While AI-driven tracking mechanisms pose significant challenges to RTBF, emerging technologies hold promise in automating data removal and enhancing privacy protections. Striking a balance between innovation and user rights will be critical in ensuring that AI-driven data ecosystems respect individuals' right to control their personal information [22].

4.3. Case Studies on RTBF Implementation

4.3.1. Google Spain Case: Landmark Decision and Implications

The *Google Spain SL v. Agencia Española de Protección de Datos* (2014) case was a turning point in the legal recognition of RTBF. The European Court of Justice (ECJ) ruled that individuals could request search engines to delist links containing personal data if the information was outdated, irrelevant, or excessive. This decision established that search engines act as data controllers under GDPR, making them responsible for processing RTBF requests [23].

The case involved a Spanish citizen, Mario Costeja González, who requested the removal of outdated financial records that appeared in Google search results. The ECJ ruled in his favor, compelling Google to delist the content while allowing the original newspaper article to remain online. This set a legal precedent that RTBF applies to search engines, not content publishers, balancing privacy rights with freedom of information [24].

Since the ruling, Google has processed millions of RTBF requests, though implementation remains complex. Search engines assess requests based on factors such as the public interest in accessing information, the individual's role in public life, and the nature of the content. While GDPR governs RTBF enforcement within the EU, global implementation remains inconsistent, with Google only applying RTBF removals to searches conducted within European domains [25].

4.3.2. Other Relevant Legal Cases and Rulings

Several other cases have further shaped RTBF jurisprudence. In *NT1 & NT2 v. Google LLC* (2018), the UK High Court ruled in favor of one claimant requesting data removal while rejecting another, demonstrating that RTBF claims must be evaluated individually. The court emphasized that RTBF should not be used to erase legitimate public records, reinforcing the principle that privacy rights must be weighed against public interest [26].

In France, *Google v. CNIL* (2019) clarified that RTBF does not have global applicability. The ECJ ruled that Google was only required to remove search results within the EU, limiting the extraterritorial reach of GDPR. This ruling acknowledged the challenges of enforcing RTBF across different jurisdictions, as privacy laws vary significantly worldwide [27].

These cases illustrate the evolving nature of RTBF, highlighting ongoing debates about privacy, free expression, and the global enforcement of digital rights. While legal frameworks provide mechanisms for individuals to regain control over their online presence, the effectiveness of RTBF continues to depend on technological advancements, judicial interpretations, and international cooperation [28].

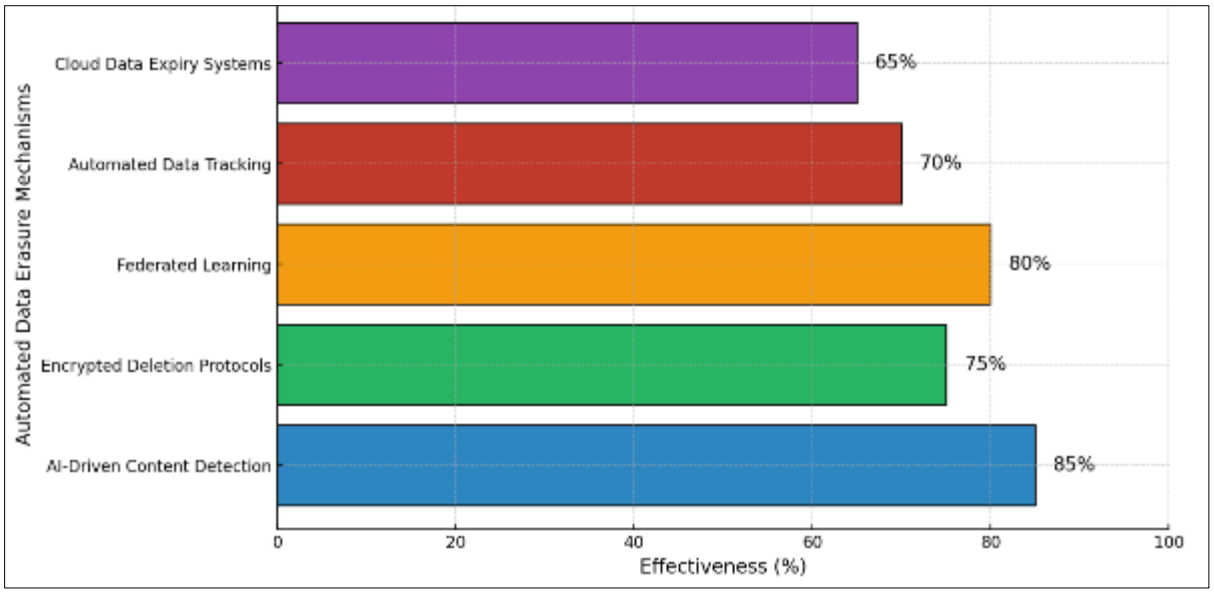

Figure 2 Mechanisms for Automated Data Erasure in RTBF Implementation

Figure 2 outlines key technological mechanisms for automated data erasure, illustrating AI-driven content detection, encrypted deletion protocols, and federated learning techniques. These solutions highlight how automation can enhance RTBF compliance while addressing challenges related to data persistence, cloud storage, and AI-driven tracking systems [29].

5. Ethical and societal implications of the right to be forgotten

5.1. Individual Privacy vs. Public Interest

The Right to Be Forgotten (RTBF) raises an ongoing debate between individual privacy rights and the public's right to access information. Advocates argue that individuals should have control over their digital footprint, particularly when outdated or misleading information negatively impacts their personal or professional lives. Privacy laws, such as the General Data Protection Regulation (GDPR), reinforce the notion that individuals should have the ability to request the removal of personal data when it is no longer relevant or serves no legitimate public interest [16].

Conversely, opponents argue that unrestricted RTBF enforcement risks undermining freedom of information, particularly in cases involving public figures, legal records, or historical events. Journalistic organizations have voiced concerns that granting individuals the ability to erase digital records may lead to censorship or revisionist history. News archives and investigative reports often serve as critical references for understanding past events, and removing information upon request could compromise transparency and accountability [17].

A notable challenge lies in distinguishing between private and public-interest information. While personal financial data or medical history may be justifiably erased, legal records or corporate misconduct reports serve broader societal functions. Courts have attempted to balance these rights by evaluating RTBF requests based on public relevance, legal obligations, and the nature of the information involved. For instance, judicial decisions often consider whether the information pertains to a criminal conviction, political activity, or other matters of significant public concern before granting an erasure request [18].

Additionally, the extraterritorial application of RTBF remains a contested issue. While the European Union enforces RTBF strictly, countries such as the United States prioritize free speech and press freedoms, limiting the extent to which search engines and content providers must comply. The *Google v. CNIL* ruling clarified that RTBF obligations apply only within EU domains, illustrating the challenges of enforcing privacy rights in a globally interconnected digital environment [19].

Ultimately, striking a balance between personal privacy and public interest remains a core challenge for RTBF implementation. While privacy protections are essential in safeguarding individual rights, excessive restrictions on

information access could have unintended consequences, including eroding journalistic integrity and limiting historical record preservation [20].

5.2. Social and Psychological Impacts

Digital identity has become an integral part of personal and professional life, influencing reputation, career prospects, and psychological well-being. The permanence of online information means that individuals often struggle to escape past mistakes or misinformation that may no longer reflect their current circumstances. For many, RTBF serves as a mechanism for regaining control over their digital identity, offering a sense of closure and allowing them to move forward without the burden of outdated or harmful content [21].

Psychological research suggests that online reputation management plays a crucial role in mental health. Studies indicate that negative digital exposure can lead to stress, anxiety, and even depression, particularly when individuals feel powerless to remove damaging content. Cases involving cyberbullying, revenge pornography, or defamatory statements highlight the importance of granting individuals the ability to erase content that affects their emotional well-being [22].

Furthermore, the psychological need for erasure extends beyond personal reputation to broader societal attitudes toward redemption and second chances. Criminal rehabilitation efforts, for example, emphasize the need for reintegration into society, yet digital records of past offenses often remain accessible indefinitely, limiting employment opportunities and social acceptance. While legal systems recognize the principle of expungement for certain offenses, digital records persist, making RTBF a valuable tool for ensuring that individuals are not permanently defined by their past [23].

Despite its psychological benefits, RTBF also raises concerns about selective memory and accountability. Erasing digital records may allow individuals or organizations to avoid responsibility for past actions, leading to ethical dilemmas about the limits of digital forgiveness. As RTBF evolves, policymakers must consider how to balance psychological well-being with broader ethical and societal implications [24].

5.3. Corporate Responsibility and Compliance

Corporations play a critical role in enforcing data privacy and ensuring compliance with RTBF requests. Search engines, social media platforms, and data aggregators serve as gatekeepers of online information, making them responsible for processing and evaluating data removal requests. Under GDPR, companies must respond to RTBF claims in a timely manner, removing personal data unless a legitimate exemption applies. However, compliance remains a complex and resource-intensive task, as organizations must balance legal obligations with technological challenges in tracking and deleting data across multiple platforms [25].

Ethically, businesses have a responsibility to ensure transparency in data management. Many companies collect and store vast amounts of user data without clear disclosure on how it is used or shared. Implementing privacy-by-design principles—such as minimizing data collection, enabling user control over personal information, and providing clear opt-out mechanisms—can enhance corporate accountability and foster consumer trust [26].

Despite regulatory frameworks, some corporations resist RTBF enforcement, citing concerns about operational costs, legal uncertainties, or conflicts with other data retention policies. Critics argue that businesses prioritize commercial interests over privacy rights, delaying compliance or exploiting legal loopholes to avoid deleting user data. High-profile cases of data breaches and privacy violations have highlighted the need for stricter enforcement and penalties for non-compliant organizations [27].

Moving forward, corporations must integrate robust data governance strategies, ensuring that RTBF is implemented fairly and efficiently. By prioritizing ethical data management, businesses can navigate the complexities of digital privacy while upholding consumer rights and maintaining transparency in an increasingly data-driven world [28].

6. Economic and business implications of RTBF

6.1. Cost of Compliance and Implementation

The enforcement of the Right to Be Forgotten (RTBF) has imposed significant financial and operational burdens on businesses, particularly those handling large volumes of personal data. Compliance costs vary depending on the size of the organization, industry regulations, and the complexity of data management systems. Large multinational

corporations, such as Google and Facebook, invest millions annually in legal teams, automated request-handling systems, and AI-driven content moderation to manage RTBF claims efficiently [19].

For small and medium-sized enterprises (SMEs), the financial burden of RTBF compliance can be disproportionately high. Unlike tech giants with dedicated legal departments, SMEs often lack the resources to establish sophisticated data governance frameworks. Costs associated with hiring data protection officers, implementing secure data storage systems, and ensuring regulatory compliance can be overwhelming. A 2021 study estimated that GDPR compliance costs for SMEs range from €10,000 to €50,000 per year, depending on the volume of data processed and the complexity of legal requirements [20].

The rise of privacy-focused legal consulting and compliance industries reflects the increasing demand for professional expertise in navigating RTBF obligations. Law firms and consultancy services specializing in data protection have expanded significantly, offering businesses guidance on RTBF compliance, risk assessments, and data protection impact evaluations. Additionally, privacy tech startups are developing automated solutions to streamline RTBF request processing, reducing administrative burdens for businesses while ensuring compliance with evolving legal standards [21].

Despite the high costs, non-compliance with RTBF regulations can result in severe financial penalties. Under GDPR, organizations that fail to process data erasure requests appropriately face fines of up to €20 million or 4% of their annual global revenue. These strict penalties have prompted businesses to prioritize RTBF compliance as part of their broader data protection strategies [22].

Ultimately, while RTBF enforcement presents financial challenges, the long-term benefits of investing in data privacy infrastructure—such as enhanced brand reputation and reduced legal risks—can outweigh the initial costs. As privacy laws continue to evolve, businesses must adopt proactive strategies to manage RTBF obligations efficiently and cost-effectively [23].

6.2. Economic Benefits of RTBF

Beyond compliance costs, RTBF offers economic advantages for businesses that prioritize consumer privacy. In an era where data breaches and privacy violations frequently make headlines, companies that implement strong data protection measures can differentiate themselves in the market. Consumers are increasingly choosing brands that demonstrate transparency and accountability in data management, making privacy a key factor in brand trust and reputation [24].

A 2022 survey found that 72% of consumers are more likely to do business with companies that provide clear data privacy policies and allow them to control their personal information. RTBF compliance, therefore, serves as a competitive advantage, reinforcing customer loyalty and mitigating reputational risks associated with privacy scandals. Companies that proactively address data privacy concerns can attract privacy-conscious consumers and build long-term brand equity [25].

Market differentiation through data privacy standards is particularly relevant in industries such as finance, healthcare, and e-commerce, where personal data security is a major consumer concern. Businesses that exceed regulatory requirements by offering enhanced privacy controls, encrypted transactions, and transparent data policies gain a competitive edge. Additionally, compliance with RTBF and broader privacy regulations can facilitate international business expansion, as many jurisdictions now require strict data protection measures for market entry [26].

As digital privacy continues to shape consumer behavior, businesses that integrate RTBF into their corporate strategies stand to gain not only compliance benefits but also financial advantages. The ability to leverage data protection as a brand differentiator underscores the broader economic value of privacy-focused business models [27].

6.3. Impact on Digital Platforms and Online Services

The implementation of RTBF has had significant implications for digital platforms, including social media networks, search engines, and online data repositories. As primary data controllers, these platforms face the challenge of balancing RTBF compliance with operational efficiency and free speech concerns. Companies such as Google, Twitter, and Facebook process millions of RTBF requests annually, requiring automated systems and legal teams to evaluate each case based on regulatory criteria [28].

One of the most contentious issues is the role of search engines in RTBF enforcement. While GDPR requires search engines to remove specific links upon valid requests, the underlying content often remains accessible on third-party websites. This raises concerns about the effectiveness of RTBF in fully erasing unwanted digital traces, as information can still be retrieved through alternative search engines or archived copies. Additionally, platforms must assess whether removing links violates public interest or journalistic freedom, leading to legal disputes and inconsistencies in enforcement [29].

Social media platforms also face conflicts between RTBF requirements and their own content policies. Many platforms allow users to request content removal from their own profiles, but issues arise when third-party users share personal data without consent. Platforms must navigate the legal complexities of balancing user privacy rights with freedom of expression, particularly in cases involving public figures, legal records, or controversial online discussions [30].

The rise of decentralized and blockchain-based platforms further complicates RTBF enforcement. Unlike traditional centralized platforms, blockchain transactions are immutable, meaning that once data is recorded, it cannot be altered or deleted. This poses fundamental challenges to RTBF implementation, as individuals cannot remove personal information stored on blockchain networks without disrupting the entire ledger [31].

Overall, RTBF has reshaped the way digital platforms manage user data, driving companies to develop new policies, automated tools, and legal frameworks to comply with evolving privacy regulations. While the enforcement of RTBF remains complex, digital platforms must continue adapting to regulatory requirements while balancing the interests of users, businesses, and legal systems [32].

Table 1 Estimated Compliance Costs of Right to Be Forgotten (RTBF) Across Industries

Industry	**Average Compliance Cost per Request (USD)**	**Annual Requests (Estimated)**	**Total Annual Compliance Cost (USD)**
Healthcare	$500	12,000	$6,000,000
Financial Services	$750	8,500	$6,375,000
E-Commerce	$300	20,000	$6,000,000
Social Media Platforms	$900	35,000	$31,500,000
Cloud Service Providers	$600	15,000	$9,000,000
Telecommunications	$400	10,000	$4,000,000
Education	$250	5,000	$1,250,000

Table 1 provides an overview of the estimated compliance costs associated with RTBF implementation across different industries, highlighting variations based on data processing complexity, regulatory requirements, and operational scale. As privacy regulations continue to evolve, businesses must evaluate the financial implications of RTBF while leveraging data protection as a strategic advantage [33].

7. Future perspectives and policy recommendations

7.1. Strengthening Legal Frameworks

As digital privacy concerns become increasingly complex, the need for global harmonization of privacy laws is more pressing than ever. While the General Data Protection Regulation (GDPR) has set a strong legal precedent for the Right to Be Forgotten (RTBF) in the European Union, significant disparities remain in how different jurisdictions approach data privacy and information access. The fragmented nature of global data protection laws creates enforcement challenges, as multinational companies must navigate varying legal obligations across different regions [22].

A key issue is the lack of a standardized approach to RTBF outside the EU. The United States, for example, prioritizes free speech protections over data removal rights, limiting RTBF applicability. In contrast, countries such as Brazil and Japan have adopted GDPR-inspired laws but differ in enforcement mechanisms. To address these inconsistencies,

policymakers must work towards international agreements that provide clear RTBF guidelines while balancing privacy rights with free expression concerns [23].

Suggested improvements to RTBF policies include clearer criteria for evaluating data erasure requests, more transparent decision-making processes, and better mechanisms for dispute resolution. Currently, search engines and online platforms play a central role in assessing RTBF claims, raising concerns about corporate influence over privacy rights. Independent regulatory bodies or privacy ombudsmen could be established to oversee RTBF implementation, ensuring fairness and accountability in handling data removal requests [24].

Furthermore, RTBF laws should be adapted to account for evolving digital technologies. Cloud computing, decentralized networks, and AI-driven analytics present new challenges for data erasure. Legislators must consider whether data erasure should extend to AI training datasets, preventing personal information from being used to refine machine learning models even after deletion requests are granted. Strengthening enforcement mechanisms through automated compliance tools and stricter penalties for non-compliance can further enhance RTBF effectiveness [25].

A globally coordinated approach to privacy regulation would provide greater legal clarity for businesses and individuals while ensuring that RTBF remains enforceable in an increasingly interconnected digital landscape. International privacy frameworks modeled after GDPR could serve as the foundation for a more unified approach to data protection, ensuring consistent privacy rights worldwide [26].

7.2. Innovations in Privacy Technologies

Emerging privacy technologies are playing a crucial role in enhancing RTBF enforcement and addressing technical challenges associated with digital data erasure. As data storage and processing become more complex, advanced tools are needed to ensure compliance while maintaining security and efficiency. One promising development is the use of AI-driven content detection and automated data removal systems. These technologies help identify personal information across multiple online platforms and streamline the processing of RTBF requests, reducing reliance on manual interventions [27].

Blockchain technology presents both challenges and solutions for RTBF. While blockchain's immutability conflicts with traditional data deletion practices, researchers are developing privacy-focused blockchain frameworks that allow for controlled data expiration. Concepts such as zero-knowledge proofs and cryptographic hashing can enable selective data concealment without compromising the integrity of the distributed ledger. These innovations offer potential pathways for reconciling RTBF with decentralized data systems [28].

Next-generation encryption methods are also advancing privacy protections. Homomorphic encryption, for instance, allows computations on encrypted data without exposing its contents, reducing the need for permanent data storage. Similarly, differential privacy techniques introduce statistical noise into datasets, ensuring that personal information cannot be reconstructed while maintaining data utility for research and analytics. By incorporating these technologies into RTBF frameworks, companies and regulators can enhance data privacy without compromising functionality [29].

Looking ahead, continuous innovation in privacy-enhancing technologies will be essential to ensuring that RTBF remains enforceable in an evolving digital landscape. Governments and businesses must invest in privacy research and encourage collaboration between technology experts and policymakers to develop effective solutions that uphold individual rights while maintaining transparency and accountability [30].

7.3. Balancing Rights and Responsibilities

RTBF must be carefully balanced with freedom of expression, digital governance, and broader societal interests. While data privacy is a fundamental right, excessive restrictions on information access could hinder journalistic transparency, academic research, and public accountability. Governments must ensure that RTBF is applied proportionally, considering factors such as public interest, historical significance, and legal requirements before granting data removal requests [31].

Digital platforms, businesses, and regulators also share the responsibility of upholding privacy rights without enabling censorship or manipulation of historical records. Establishing clear boundaries between personal privacy and public access to information is critical in preventing the misuse of RTBF for suppressing legitimate discourse. Effective oversight mechanisms, including independent review bodies, can help resolve disputes and ensure that RTBF is applied fairly across different cases [32].

Figure 3 outlines key steps for improving global RTBF implementation, including legal harmonization, technological advancements, and ethical guidelines for balancing privacy with freedom of information. By integrating these strategies, policymakers can ensure that RTBF evolves to meet future privacy challenges while safeguarding transparency and digital rights [33].

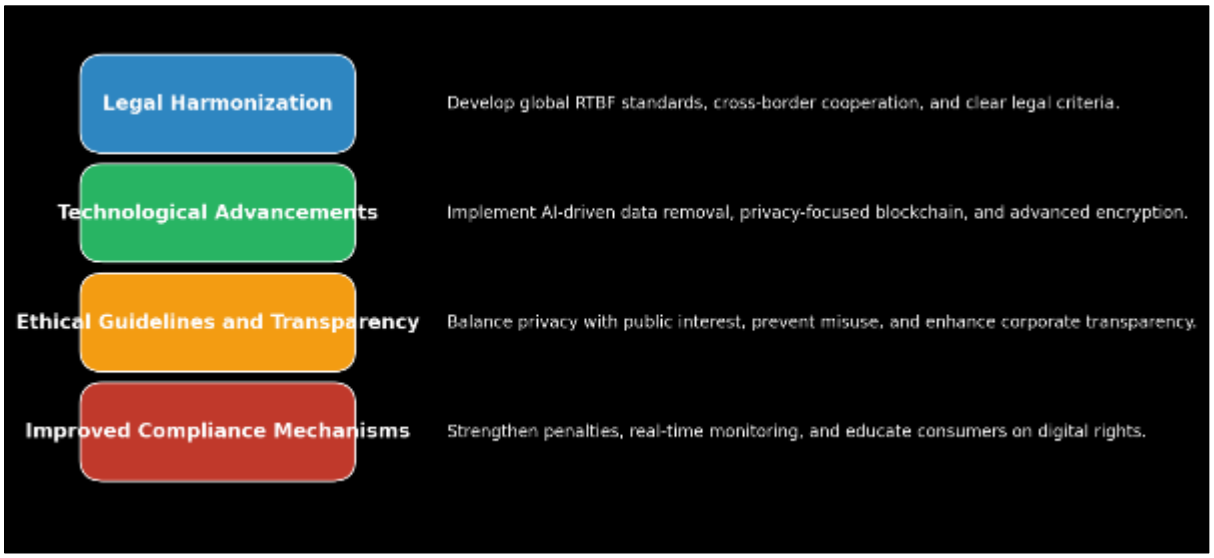

Figure 3 Roadmap for Strengthening Global RTBF Policies

8. Conclusion

8.1. Summary of Key Insights

The Right to Be Forgotten (RTBF) has emerged as a crucial legal and ethical framework in the digital era, aiming to provide individuals with control over their online personal data. Across legal, technological, and ethical perspectives, RTBF presents both significant advancements and complex challenges.

From a legal standpoint, RTBF is primarily rooted in the General Data Protection Regulation (GDPR), which grants individuals the right to request the removal of personal data under specific conditions. This has had a profound impact on data protection policies worldwide, influencing legislation in regions such as Latin America and Asia. However, differences in legal interpretations, especially in jurisdictions such as the United States, where free speech laws take precedence, have led to inconsistent enforcement of RTBF across global digital platforms. The need for international harmonization of privacy laws remains a critical challenge.

Technologically, RTBF enforcement faces substantial hurdles. Digital data is often replicated across multiple servers, stored in cloud-based infrastructures, and backed up in ways that make complete erasure difficult. Search engines can delist information from search results, but the original content often remains on third-party websites. Advances in privacy technologies, such as AI-driven automated data detection and cryptographic tools, are being explored to enhance RTBF compliance, but the implementation of these solutions is still in its early stages. Blockchain technology further complicates the situation, as its decentralized and immutable nature conflicts with data deletion requirements.

Ethically, RTBF raises debates about the balance between privacy rights and the public's right to access information. While individuals may have valid concerns over outdated or damaging information, excessive data removal could hinder transparency, historical record-keeping, and journalistic freedom. RTBF must be carefully applied to ensure that it does not become a tool for censorship or revisionist history.

Despite these complexities, RTBF has undeniably shifted global attitudes toward digital privacy, reinforcing the importance of individual autonomy over personal information. As digital ecosystems continue to evolve, the effectiveness of RTBF will depend on a combination of legal reforms, technological innovations, and ethical considerations.

8.2. Future Challenges and Open Issues

RTBF remains at the center of an ongoing debate between privacy rights and transparency. While data protection regulations such as GDPR have provided a legal foundation, unresolved questions persist regarding how to balance individual privacy with public access to information. Journalists, historians, and digital rights activists argue that excessive enforcement of RTBF could erase critical records, making it more difficult to hold institutions accountable. Governments and policymakers must continue refining RTBF guidelines to prevent potential misuse while safeguarding personal privacy.

Additionally, the evolving nature of digital privacy threats presents new challenges. With the rise of AI-driven data collection, big data analytics, and biometric tracking, individuals' digital footprints are expanding beyond traditional text-based records. Emerging technologies, such as facial recognition and behavioral profiling, make it increasingly difficult for individuals to control their online presence. This raises the question of whether RTBF should extend beyond traditional data erasure and include mechanisms for preventing personal data from being continuously re-collected and analyzed.

Another unresolved issue is the extraterritorial application of RTBF. Since digital data is stored across multiple jurisdictions, enforcing a removal request within one country does not necessarily guarantee data deletion worldwide. The *Google v. CNIL* ruling reinforced the challenge of enforcing RTBF across different legal systems, highlighting the need for international cooperation in privacy regulation. As digital interactions continue to transcend borders, achieving a globally consistent approach to RTBF remains a major challenge.

Ultimately, RTBF is still evolving, and its future effectiveness will depend on how well legal frameworks, technological advancements, and societal expectations adapt to emerging digital realities.

8.3. Final Thoughts

The digital landscape is constantly changing, and with it, the complexities surrounding data privacy and RTBF. As individuals continue to generate vast amounts of personal data through online interactions, social media activity, and digital transactions, the importance of having mechanisms to control and manage digital identities will only increase.

Ongoing research and policy adaptation are essential for ensuring that RTBF remains relevant and effective in addressing emerging privacy challenges. Legal frameworks must be continuously reviewed and refined to ensure they provide adequate protections without infringing on freedom of expression. Similarly, technological advancements must be leveraged to develop automated and scalable solutions for enforcing RTBF while ensuring compliance with regulatory requirements. Governments, businesses, and civil society organizations all play a role in shaping the future of digital privacy, and collaboration among these stakeholders will be critical in addressing unresolved issues.

Beyond legal and technological considerations, individuals also have a role to play in managing their digital identities. Digital literacy and awareness of privacy rights are crucial for ensuring that people understand how their data is collected, stored, and shared. Users should take proactive measures such as adjusting privacy settings, using encrypted communication tools, and being cautious about the personal information they share online. While RTBF provides a legal pathway for requesting data removal, prevention remains the most effective strategy for maintaining digital privacy.

As the internet continues to evolve, the conversation surrounding RTBF will remain dynamic, requiring constant vigilance, innovation, and ethical reflection. By balancing privacy rights with public interest, RTBF can serve as a valuable tool for empowering individuals while maintaining the integrity of digital information ecosystems.

References

[1] Goodman B, Flaxman S. European Union regulations on algorithmic decision-making and a "right to explanation". AI magazine. 2017 Oct 2;38(3):50-7.

[2] Gascón Marcén A. The extraterritorial application of European Union data protection law. Spanish yearbook of international law Nº23. 2019:213-25.

[3] Valiela I, Bowen JL, York JK. Mangrove Forests: One of the World's Threatened Major Tropical Environments: At least 35% of the area of mangrove forests has been lost in the past two decades, losses that exceed those for tropical rain forests and coral reefs, two other well-known threatened environments. Bioscience. 2001 Oct 1;51(10):807-15.

[4] Yussuf MF, Oladokun P, Williams M. Enhancing cybersecurity risk assessment in digital finance through advanced machine learning algorithms. Int J Comput Appl Technol Res. 2020;9(6):217-35.

[5] Adegbesan Bukunola Oluyemisi, Ogunlabi Olugbenga Owolabi, Olawale Olatunbosun Oladipupo, Edema Adeleye Adegboyega, Onasanya Oladayo Olaoluwa. Oral Cellgevity® improves antioxidant parameters and stalls damages in STZ-diabetic rat pancreas. Fountain Journal of Natural and Applied Sciences. 2021; Accepted February 19. Available from: http://www.ftstjournal.com/uploads/docs/61%20Article%2021.pdf

[6] Mayer-Schönberger V. Delete: The virtue of forgetting in the digital age. Princeton University Press; 2011 Dec 31.

[7] MacLean CE. It Depends: Recasting Internet Clickwrap, Browsewrap, I Agree, and Click-through Privacy Clauses as Waivers of Adhesion. Clev. St. L. Rev.. 2016;65:45.

[8] Bloustein EJ. Privacy as an aspect of human dignity: An answer to Dean Prosser. NYUL rev.. 1964;39:962.

[9] Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal. 2001;40(3):614-34.

[10] Denning DE. A lattice model of secure information flow. Communications of the ACM. 1976 May 1;19(5):236-43.

[11] Kitchin R. The data revolution: Big data, open data, data infrastructures and their consequences. Sage; 2014 Sep 16.

[12] Wachter S, Mittelstadt B, Russell C. Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harv. JL & Tech.. 2017;31:841.

[13] Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MIS quarterly. 2011 Dec 1:989-1015.

[14] Gavison R. Privacy and the Limits of Law. The Yale law journal. 1980 Jan 1;89(3):421-71.

[15] Solove DJ. Understanding privacy. Harvard university press; 2010 Mar 30.

[16] Fung BC, Wang K, Chen R, Yu PS. Privacy-preserving data publishing: A survey of recent developments. ACM Computing Surveys (Csur). 2010 Jun 23;42(4):1-53.

[17] Mcleod E, Chmura GL, Bouillon S, Salm R, Björk M, Duarte CM, Lovelock CE, Schlesinger WH, Silliman BR. A blueprint for blue carbon: toward an improved understanding of the role of vegetated coastal habitats in sequestering CO2. Frontiers in Ecology and the Environment. 2011 Dec;9(10):552-60.

[18] Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems. 2018 Nov 1;88:173-90.

[19] Solove DJ. A taxonomy of privacy. U. Pa. l. Rev.. 2005;154:477.

[20] Weis SA, Sarma SE, Rivest RL, Engels DW. Security and privacy aspects of low-cost radio frequency identification systems. InSecurity in Pervasive Computing: First International Conference, Boppard, Germany, March 12-14, 2003. Revised Papers 2004 (pp. 201-212). Springer Berlin Heidelberg.

[21] Barnes SB. A privacy paradox: Social networking in the United States. First Monday. 2006 Sep 4.

[22] Rabin MO. Efficient dispersal of information for security, load balancing, and fault tolerance. Journal of the ACM (JACM). 1989 Apr 1;36(2):335-48.

[23] Mbah GO. Enhancing IP protection in Nigeria: revising the 2004 Copyright Act. Int J Eng Technol Res Manag. 2019;3(8):63. doi: 10.5281/zenodo.15062203.

[24] Yang Q, Liu Y, Chen T, Tong Y. Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST). 2019 Jan 28;10(2):1-9.

[25] Laudon KC, Traver CG. E-commerce 2019: Business, technology, society. Pearson; 2020.

[26] Von Schomberg R. A vision of responsible research and innovation. Responsible innovation: Managing the responsible emergence of science and innovation in society. 2013 Apr 26:51-74.

[27] Harvey D. The right to the city. InThe city reader 2015 Jul 16 (pp. 314-322). Routledge.

[28] Wang C, Chow SS, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for secure cloud storage. IEEE transactions on computers. 2011 Dec 20;62(2):362-75.

[29] Hoekstra JM, Boucher TM, Ricketts TH, Roberts C. Confronting a biome crisis: global disparities of habitat loss and protection. Ecology letters. 2005 Jan;8(1):23-9.

[30] Juels A. RFID security and privacy: A research survey. IEEE journal on selected areas in communications. 2006 Feb 6;24(2):381-94.

[31] Harvey D. The right to the city. InCitizenship rights 2017 May 15 (pp. 465-482). Routledge.

[32] Mittelstadt BD, Allo P, Taddeo M, Wachter S, Floridi L. The ethics of algorithms: Mapping the debate. Big Data & Society. 2016 Nov;3(2):2053951716679679.

[33] Vågsholm I, Arzoomand NS, Boqvist S. Food security, safety, and sustainability—getting the trade-offs right. Frontiers in sustainable food systems. 2020 Feb 21;4:487217.