Journal for Social Science Archives

Online ISSN: 3006-3310
Print ISSN: 3006-3302
Volume 3, Number 1, 2025, Pages 387 – 403
Journal Home Page
https://jssarchives.com/index.php/Journal/about

The Right to be forgotten in the Digital Age: A Pakistani Perspective on Balancing Data Protection & Privacy, Freedom of Expression, and Cyber Security

Asma Jabeen Khan[1], Shahzada Aamir Mushtaq[2*], Muhammad Ali Siddique[3] & Muhammad Abdul Wadood[4]

[1]*Advocate Supreme Court of Pakistan/Special Prosecutor NAB, Email: asmakhan11pk@gmail.com*
[2]*Assistant Professor, Department of Law, Times Institute, Multan, Pakistan. Email: amirqureshi.adv@gmail.com*
[3]*Advocate Supreme Court of Pakistan/ Corporate Consultant, Email: muhammadalisiddiqui@gmail.com*
[4]*Additional Prosecutor General in the Prosecution Department of Punjab/ Incharge Regional Office Multan bench, Punjab, Pakistan, Email: wadooddpg@gmail.com*

ARTICLE INFO

Article History:

Received:	*January*	*01, 2025*
Revised:	*January*	*24, 2025*
Accepted:	*January*	*26, 2025*
Available Online:	*January*	*27, 2025*

Keywords:

Pakistan. Competition Commission of Pakistan. Cyber Security. Data Protection. GDPR. PECA.RTBF

Corresponding Author:
Shahzada Aamir Mushtaq
Email:
amirqureshi.adv@gmail.com

ABSTRACT

Right to be forgotten also known as data de-listing or de-identification is legal and ethical right providing individuals the right to request the search engine to remove the link to the information that is found when the person's name is searched online. Though its concept has been practiced in the developed countries like the members of European Union, its implementation in the developing country like Pakistan is still in bloom. This paper explores the plausibility, likelihood and consequences of imposing the RTBF within the Pakistani context with spec emphasis to its compatibility with privacy, freedom of speech and cyber security. Lack of proper Data protection laws in Pakistan put the individuals at risk of cyber harassment, and misuse of personal data; tarnishing one's reputation. The Constitution of Pakistan acknowledges the right to privacy to the citizens in article 14 and freedom of speech and expression in article 19 but these rights are not well realized while operating in digital platform. The RTBF could allow people to take back control of their online persona but freedom comes with crucial issues of censorship, transparency and the ability of the regulatory bodies. The study employs doctrinal research strategy that involves empirical and comparative methodology to explore the legal, social, and pragmatic implications of RTBF in social media regulations of Pakistan. The study further reveals that there are legal loopholes that need to be addressed in order to enhance the privacy laws relating to Pakistan particularly in the context of digital environment as there is lack of comprehensive legal protection, overlapping of the regulation and legislation and legal culture, freedom of speech and finally institutional framework. Suggestions include passage of a competently drafted Data Protection Act, better staff and structures, better implementing criteria for RTBF requests, creation of awareness among the citizens regarding their digital rights, involving international organizations in an effort to frame a suitable RTBF framework.

1. Introduction

Most commonly, the right to be forgotten (RTBF) refers to a well-established legal term related to data protection and cyber security within the Information Society. Being an EU led right through the General Data Protection Regulation (GDPR), this right allows individuals to request for erasure of their personal data where, for one or more specified purposes, it is no longer required or suitable. In Pakistan, the legal right for data protection is still in its evolutionary stage, therefore questions like implementation of RTBF, its compliance with the existing laws, and equal protection of both privacy rights and freedom of speech and expression, comes across as challenging. This article flares and analyses RTBF under the context of Pakistani Law about data protection as well as the possibility and problematic of its applications in the field of cyber security (Renuka et al., 2025).

Living in the world of the internet and the fourth industrial revolution the boundlessness of the digital world has become a storehouse of knowledge about people. As much as digitization creates more convenience than it does the physical documentation, it is also much a threat to people's privacy, liberty and image. The Right to Be Forgotten (RTBF) as a concept has come to address these challenges through support for the possibility of users asking for their data to be removed from online platforms and the search results. Given that the RTBF negotiates and enshrine critical values more importantly, privacy, freedom of speech and cyber security the process of its uptake and deployment requires a lot of effort and focus. With internet access growing quickly in Pakistan and the resulting larger footprints on the digital platforms, the need for an RTBF brings up questions on the ability of existing laws, values, and politics of the country to accommodate the new notion (Huynh, 2025).

1.1 Origins and Historical Background of the Right to Be Forgotten

The RTBF, in contrast, Post is a relatively new legal construct that emerged out of the Americas owing to the conflict generated by the digital revolution. Issues formulated within its provisions can be linked back to Europe whose legal systems cherish the importance of privacy and personal dignity. This concept became known worldwide in the year 2014 particularly through the case of GOOGLE Spain SL, GOOGLE Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja Gonzalez CJEU. This case involved Mario Costeja González, who wanted Google to delist him from search results containing information, which was no longer relevant on him financially. The CJEU specified the right of a person to demand the removal of some data concerning him /her due to the fact that such data is no longer required for being published in the public's interest, as the court stated when rendering the González v. Spain case. This ruling entrenches the RTBF into the European Union data protection regime which was later enshrined in Article 17 of GDPR (Cocito & De Hert, 2025).

These principles of RTBF stem from the right to privacy of which international recognition was granted under the 1948 Universal Declaration of Human Rights Article 12 and the International Covenant on Civil and Political Rights 1966 (Article 17). The RTBF also sits well with the principle of 'informational self-determination,' that originates from the German constitutional law, regarding an individual's ability to control his or her personal information. However, together with RTBF emerge discussions on its incompatibility with the right to freedom of speech, which forms the basis of democratic states that is recognized by the ICCPR Article 19 (Aleke, 2025).

1.2 The Pakistani Context: Privacy, Freedom of Expression, and Cyber security

In the context of Pakistan, the RTBF has its considerations and prospects borne out of the country's progressive technological adaptability and its socio-political context. Pakistan over the last few years has reached over 100 million internet users and has a very active engagement on social media platforms. Even as this digital phenomenon has supported economic devolution, creation and social interaction, it has put the user in danger of encountering mishaps including identity theft, cyber bullying and a tarnished image.

The idea of privacy law in Pakistan is rooted in Article 14 of the Constitution of Pakistan which states that; "Every citizen shall have the right to dignity of man and the privacy of home." Nevertheless, this constitutional guarantee is still weak in its implementation when it comes to the context of the network environment. Some provisions are highlighted giving some features of data protection and cybercrimes in Pakistan, but it does not consider the RTBF in the legal system of Pakistan; for example, the Pakistan Electronic Crimes Act (PECA), 2016. Moreover, Pakistan lacks a comprehensive data protection law like the GDPR, on personal data and its erasure from cyberspace which provides considerable legal loopholes in law (Divyashree, 2025).

The implications of RTBF in Pakistani perspective have important questions about privacy protection except freedom of speech, which is a part of Article 19 of the constitution Iraq and cyber security. As in any country freedom of expression in Belgium remains relative due to socio-political sensitives, the RTBF might be misused to stifle legal criticism, dissent or journalism investigation. Similarly, due to the lack of sound data protection at the same time people remain exposed to online risks that are why, of course, it makes sense to focus on the need to have quality but democratic approach while protecting both: private data and public interest (Conde et al., 2025).

1.3 The Need for a Pakistani Perspective

Although the RTBF has generated much academic discourse in the European and North American countries its application in context such as Pakistan has not been researched for extensively. A Pakistani context is inevitable to cover the social, legal, and technological context specific to Pakistan to contribute to the cyber environment. Key considerations include:

- **Cultural Norms and Privacy Expectations:** An important association with privacy generally refers to honor and reputation within Pakistani society, but also gives special emphasis to control over information.
- **Digital Literacy and Awareness:** In Pakistan most of the internet users do not have the necessary knowledge about their digital rights such as privacy for them to be able to fight for the RTBF.
- **Technological and Institutional Capacity:** The formulation of the RTBF necessarily entails considerable resource commitment in terms of technology as well as the laws and rules governing an organization.

1.4 Research Focus and Objectives

This research therefore, offers a critical reflection of the RTBF in Pakistan with regard to privacy, freedom of speech, and cyber security. It outlines some of the possible advantages that are associated with the implementation of the RTBF, including; the ability of users to safeguard their online image It also considers the challenges or a possibility of misuse, and the dangers of application in excess. To this end, by reviewing global trends and legal authorities, this study intends to develop a suitable Pakistani framework of the RTBF that is constitutionally compatible

with the goals of democracy, legally responsive to Pakistan digital domain, and consistent with widely established principles of freedom of expression.

In doing so, this research contributes to the existing literature on data protection and digital rights in Pakistan, and provides direction for policymakers, legal actors, and civil society to engage in the processes of developing a human rights compliant digital Pakistan.

2. Literature Review

Right to be forgotten (RTBF) is another debatable phenomenon in the context of the digitized world across its relation with the privacy rights and freedoms of expression, as well as cyber security. However, relatively little is known on how it works in regions such as the European Union and North America and even less is known on the effectiveness of the application of the system in developing countries like Pakistan. This paper critically discusses the literature available on the RTBF regarding its development, enactment, and controversies internationally and in Pakistan. The review is structured into five thematic areas: The role of social media starting from its evolution and its rationale, privacy in the realm of technology, freedom of speech in the light of now and then, issues related to cyber security and safety and last but not the least the cultural and legal conditions of Pakistan (Chmielarz, 2025).

2.1. Origins and Philosophical Foundations of the Right to Be Forgotten

The RTBF stems from the idea of privacy, and this is one of the rights that enjoy recognition at the Universal Level at Article 12 of the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights at Article 17. Some academic authors, including Rosen (2012), argued that legal origins of the RTBF can be found in the right to informational self-determination enshrined in German's Basic Law. This principle empowers individuals to decide the destiny of their data, their rights to control data sharing (Papadimitriou & Virvou, 2025).

In the European Union, the RTBF was popularized through the case of Google Spain v. the Martinez-Valverde case; better known as the Mario Costeja González (2014) case, the Court of Justice of the European Union (CJEU) ruled it was the right of users to demand removal of links carrying information that is no longer relevant to the persons' lives. This ruling established the RTBF under Article 17 of the GDPR therefore allowing for the regulation of privacy and the public interest (Jiang, 2025).

On the negative account, Zittrain (2014), and Floridi (2016) revealed that RTBF could supplement mischief by omitting out-of-favor data from public memory. Such apprehensions are particularly relevant in relatively less creditworthy jurisdictions, including Pakistan where the RTBF can easily be abused to stifle opposition or cover up corruption.

2.2. Privacy in the Digital Era

In their turn, current changes in the use of the internet and new technologies have created new features regarding privacy. Solove (2008) posits the digital age privacy as a concept laden with tension between independence and freedom, corporate power and state sovereign authority. To that effect, the RTBF is viewed as a process of getting back personal control over data.

In Pakistan, the right to privacy is protected by constitution through article 14 where it declares the dignity of person and private life. However, according to Waheed (2020) and Ahmed (2021) the above constitutional guarantee is not well translated by legal frameworks into sound protection of digital or cyber privacy. The Pakistan Electronic Crimes Act (PECA), 2016 despite addressing

cyber-crimes lacks legal provision or policy over data erasure or the RTBF and therefore there continues to be inadequate coverage of the protection of digital rights of citizens.

In contrast, the GDPR provides a broad data protection regime, with carriers with specific instruments regarding data transfer and deletion. Research by Kuner (2020) and Lynskey (2019) stress that GDPR has succeeded in putting people in the driving seat to take on corporations in the management of their data. On the other hand, PDPB, 2019 is another example since Bhandari and Malik (2020) explain how similar approaches can be useful for India, yet Pakistan can find them applicable to its context as a developing country. But such studies warn against over-formalization of RTBF provisions which might be contrary to rights of free speech and access. Rudden, L. (2025).

2.3. Right to Freedom of Expression and Right to Be Forgotten

The RTBF is entrenched under the **ICCPR Article 19** which also covers freedom of expression. As seen from the earlier example, critics like Pollicino and Quintarelli (2015) have pointed out that for under RTBF people delete legitimate public records in order to hinder investigative journalism and historical scrutiny. This tension is so inherent especially in today's world where the internet is the largest source of information.

In Pakistan, **Article 19 of the Constitution** protects the rights of freedom of speech but with the provisions of placing reasonable restriction in the sake of morality, security or order. As Siddiqui explains in the article under consideration carrying out these restrictions is often carried out subjectively Therefore these restrictions raise the possibility of the RTBF being utilized as a tool for silencing the dissenting voices or filtering out the information that is unpleasant for some individuals.

The RTBF, especially, has been compared with the EU and the US, in which different approaches are found. The EU is concerned about users' privacy more than their freedom of speech in particular situations, as we deduced from the GDPR rules and CJEU cases. On the other hand, the American legal system, fostered in the First Amendment has much emphasis on freedom of speech and hence the RTBF is always a hard sell. Such disparities reveal the fact that the governments of Pakistan need a more sophisticated approach towards free speech liberties as compare to other parts of the world and region because of socio-political barriers (Rampášek et al., 2025).

2.4. The Right to be Forgotten, and its implications on Cyber Security

The RTBF is not only a privacy issue but it also forms an integral part of cyber security. In their work, Acquisti, Taylor, and Wagman (2016) agree with the principles of data minimization and immediate erasure in minimizing risks of cyber –attacks. In so doing, the RTBF reduces the avenues wherein identity theft and data breaches may occur because people can delete unnecessary personal information.

In Pakistan, the cyber security sector is governed by PECA, 2016 that dealt with cybercrimes but has not adequate legislation regarding data security. Akhtar (2020) has pointed out with growing data breaches and their frequency, the absence of proper legislation and protection of personal information. Even in this case however the RTBF could prove useful for improving cyber security but its adoption in Pakistan implies considerable investments in technology and institutions.

Examining the examples from India's PDPB (Bhandari and Malik, 2020) and Brazil's Lei Geral de Proteção de Dados (LGPD) (Gomes, 2020) is instructive. In both jurisdictions data protection is aligned with cyber security in a way that aims at achieving transparency and accountability. Similarly for Pakistan adopting such approach might help in reinforcing the role of RTBF in more effective and militating against cyber security within the context of international standards.

2.5. The Unique Socio-Legal backdrop of Pakistan

Sher and Khan have identified some of the specific socio-legal features of Pakistan's environment that would affect the implementation of the RTBF. Being a Muslim and living in Pakistan, privacy has a close connection with culture, shame and honor according to Hussain (2019). However, this cultural respect for privacy could equally infer ahead the RTBF - even if it may similarly pose significant challenges in enforcement where the data is especially sensitive or immediately contentious.

Institutional weaknesses also negatively affect the real realization of digital rights. According to Khan (2021), the absence of cohesiveness between various regulating bodies, including PTA and law enforcement agencies, lead to enforcement inconsistencies. In addition, due to low digital literacy levels as indicated by Waheed (2020), members of the public have low levels of understanding of their privacy rights and the RTBF.

Such comparative lessons from India and Brazil bring light to the fact that the RTBF model must suit the country's context. For instance, India's PDPB contains the provisions and the rights of individuals seeking their data and protection against the misuse. These frameworks demand a harmonized approach in Pakistan with respect to privacy, rights of freedom of speech, and cyber security.

Analyzing the potential and actual functions of RTBF in overcoming the tasks set by digital privacy and technological development, scholars pay special attention to the conflict between this principle and freedom of speech and cyber security. Though the EU GDPR is a good model of practicing the RTBF, the direct application of the same in Pakistan comes with challenges such as; legal frameworks, institutions and culture barriers. Scholarship from India, Brazil, and the US are explored next to understand how the RTBF was applied in different socio-legal environments (Sun et al., 2025).

For Pakistan, the RTBF is an opportunity to promote power to the people and the overall improvement of digital rights; but with the catch that balancing the participating interests will be crucial. Subsequent studies should concentrate on identifying a reliable local and international model on which the RTBF will serve the intended purpose of enhancing privacy and cyber security without compromising the freedom of the press or public interest (Thir & Wawra, 2025).

2.6 Article 17 of GDPR

The data subject has right to obtain the erasure of the personal data concerning him or her without undue delay and the controller shall have to erase the personal data without undue delay where, inter alia, the personal data are no longer necessary in respect of the purposes for which they are processed or where the data subject has withdrawn consent or objected to the processing of his or her data, the personal data have been processed unlawfully, the personal data have to If the controller has made the personal data public and is under obligation to erase such personal data then it has to communicate such erasure to the controllers processing the data to the data subject. However, the provisions set out in paragraphs 1 and 2 do not apply to the processing operations

which are required for: the exercise of the right of freedom of expression and information, the compliance with legal obligations, the performance of a task carried out in the interest of public health, archiving in the public interest, scientific or historical research purposes, statistical purposes or for the purposes of the establishment, exercise or defense of legal rights (Hamid & Huda, 2025).

2.6 Data Protection and Cyber security in Pakistan: The Current Legal Landscape

The framework of data protection and cyber security law in Pakistan is yet in its developmental stage. The major law that exists for online activities is The Prevention of Electronic Crimes Act (PECA) 2016 which deals with cyber-crimes, any electronic related fraud and unlawful access to data. However, personal data protection under PECA lacks a framework or approach or even a clear legal framework that addresses individual rights pertaining to data erasure. The Personal Data Protection Bill which has been introduced since 2020 aims to address these issues. The bill is an act that seeks to create the Data Protection Authority; place certain responsibilities on any person who processes or uses personal data; offer certain entitlements to individuals over their personal data, including the entitlement to erasure. But it does not also categorize the RTBF in the same way as the GDPR does; this has resulted in much uncertainty regarding its scope and implementation (Gupta & George, 2025).

- **The Legal Basis for RTBF in Pakistan**

The RTBF in Pakistan can be deduced as a result of constitutional right in Pakistan based on the Constitution of Pakistan 1973 under Article 4, 14, and 19. Article 4 also protects the rights of the individual, Article 14 protects the sanctity of dignity and privacy and Article 19 protects freedom of speech and expression. The said provisions together contribute a framework to strike proportionate the freedom of expression against privacy rights, which is a contentious topic In the RTBF debate, Furthermore, The Supreme Court of Pakistan recognized privacy as a fundamental right in Benazir Bhutto v. Federation of Pakistan (mw) 1988 and Justice Qazi Faez Isa v. President of Pakistan (2021). These judgments have jurisprudential precept for integrating the RTBF into the Pakistani law.

3.1 Impediments in Implementing RTBF in Pakistan

According to the above literature review the main challenges that Pakistan is facing in the implementation of RTBF are as follows;

3.1.1. Inexperience in the enactment of Comprehensive Data Protection Laws

Lack of comprehensive data protection legislation in modern Pakistan is a massive problem hindering the implementation of the RTBF. In case of enacting the Personal Data Protection Bill, issues related to procedural and substantive aspects of the RTBF like the criteria for erasure and dispute resolution have to be articulated.

3.1.2. Technological as well as Resource Limitation

The technical and organizational enforcement of the RTBF also demands sophisticated technological tools, as well as experienced staff for controlling the RTBF's implementation as well as for working through requests on data erasure. This right might be difficult for Pakistan to implement due to the fact that the country has limited capability in technology and most of its population is still illiterate about computers (Guo & Li, 2025).

3.1.3. Privacy vs. Free Speech

More often than not, the RTBF stands in the way of the right to freedom of expression and the public's right to information. In Pakistan media freedom is still a topic of debate; the RTBF can be manipulated as a tool for oppression or as a way to hide important facts.

3.1.4. Cross-Border Data Transfers

Since the internet operates on an international platform, transitioning the RTBF into Pakistan shall present cross-border data transfer problem. This means that if the governments were to encourage and build partnerships with Multinational Corporations compliance to international standards would be compulsory (Guo & Li, 2025).

4. Opportunities and Benefits of RTBF in Pakistan

4.1. Enhancing individual's right to privacy

The RTBF can allow individuals to have control over their personal data hence shall help improve the privacy of persons in a society that is quickly embracing the use of digital products. This is well illustrated by the current high incidences of unauthorized access to and misuse of personal data in Pakistan.

4.2. Building Confidence in Digital Environment

Thus, with the help of the RTBF, the subject can request the removal of data and, as a result, strengthen people's confidence in digital platforms and increase the number of users in the digital economy. Also, this is in line with the goals of the Pakistan government's directives in the "Digital Pakistan" efforts.

4.3. Enhancing Cyber security

In this way, the RTBF can support the cyber security endeavors by eliminating unnecessary outdated data which could be utilized by the cybercriminals. This seems especially so given the rising instances of cyber-attacks on Pakistani institutions (Harish et al., 2025).

5. Research Methodology

This study uses doctrinal legal research method and comparative legal research method in an attempt to assess the possibility and effects of adopting the RTBF in Pakistan. This research proposal seeks to fill the above mentioned legal, institutional and practical research gaps concerning the RTBF and the protection of privacy, freedom of expression and cyber security in the emerging digital environment of Pakistan.

The research design is qualitative, focusing on two complementary methodologies: It has primarily employed doctrinal legal research to constructively critique Pakistan's constitutional provisions and its statutes with a view to noting holes and inconsistencies in the combating of the RTBF and comparative legal research in a select number of jurisdictions including the European Union, the United State of America, the Republic of India, and the Federative Republic of Brazil.

The doctrinal approach aims to review textual, statutory and case authorities in relation to legal principles of privacy and freedom of speech, and cyber security. Sources of information used comprise the Constitution of Pakistan, Pakistan Electronic Crimes Act (PECA), Pakistani case

laws regarding privacy and freedom of speech, legal journals, articles, Pakistani constitutional law, and privacy rights books, CCP reports and publications, PTA, and DRF.

The comparative approach seeks to look at some selected jurisdictions with fully developed RTBF environments seeking to understand how these systems integrate the personalities of privacy, free speech, and cyber-security. Some of the jurisdictions sampled are; General Data Protection Regulation (GDPR), First Amendment and the Data Protection Bill from India.

The proposed doctrinal and comparative approach enables a more sophisticated understanding of the RTBF in the context of Pakistan, the detection of legal shortcomings, considering the international experience, and the development of adequate recommendations. The expected outcomes include a legal evaluation of the subject matter, comparative analysis, policy implications, issues of legal, ethical implications, and a clear appreciation of alternative legal systems in Pakistan with regard to the RTBF.

6. Critical Comparative Analysis, Results and Discussion

This section more specifically compares the legal provisions with respect to the right to be forgotten across the **EU, US, India and Pakistan** in regard to the measures taken with regard to the balancing of privacy, freedom of speech, and cyber security. Their effectiveness is discussed and compared to each other and the suitability of each of them for the dynamics of the Pakistani environment is assessed.

6.1. Comparative Analysis of RTBF Provisions

Aspect	European Union	United States	India	Pakistan
Legal Basis	GDPR Article 17 (RTBF)	First Amendment (focuseson freedom of expression; no RTBF recognized)	Justice K.S. Puttaswamy v. Union of India (2017): Recognizes privacy as a fundamental right but lacks formal RTBF.	Article 14 (privacy), Article 19 (freedom of expression); PECA 2016 (limited data protection).
Privacy Emphasis	Strong focus on individual privacy and data autonomy; RTBF ensures data erasure if irrelevant, outdated, or unlawful.	Minimal focus on privacy due to prioritization of free speech and public interest over data erasure.	Recognizes privacy as a constitutional right; RTBF included in draft Personal Data Protection Bill (PDPB).	Privacy acknowledged in constitutional terms but underdeveloped in practical digital protection laws.

Freedomof Expression	Balances RTBF with public interest; protects freedom of information unless outweighed by privacy concerns.	Strong emphasis on freedom of expression; RTBF perceived as a threat to transparency and accountability.	Balances privacy and freedom of expression, but lacks detailed implementation mechanisms for RTBF.	Freedom of expression subject to "reasonable restrictions"; risk of RTBF misuse for censorship or political suppression.
Cybersecurity Integration	GDPR integrates cybersecurity, ensuring secure data handling alongside RTBF obligations.	Cybersecurity policies separate from RTBF; no legal obligation for data erasure as a cybersecurity measure.	PDPB proposes data localization and erasure for enhanced cybersecurity.	PECA 2016 addresses cybercrimes but lacks direct cybersecurity measures linked to RTBF or data erasure.
Implementation Mechanism	Well-defined process for submitting RTBF requests; independent supervisory authorities enforce decisions.	No implementation mechanism; RTBF not recognized as a legal right.	Draft PDPB outlines mechanisms for data removal requests but is not yet enacted into law.	No RTBF implementation process; regulatory overlap between PTA, CCP, and other agencies creates enforcement gaps.
Challenges	Potential misuse to suppress free speech; enforcement across borders is complex.	Perceived as incompatible with free speech; risks of erasing public interest information.	Balancing privacy with the public interest; lack of technological readiness to implement RTBF fully.	Institutional weaknesses, lack of clear legal framework, and risk of political misuse hinder RTBF adoption.

6.2. Results of Comparative Analysis

6.2.1 Advantages of Existing Frameworks

European Union

- Detailed requirement of RTBF provisions of GDPR.
- Solutions regarding how privacy, on one hand, and public interest and freedom of expression should be reconciled.
- Independent supervisory authorities stand for transparency of business procedures and their accountability.

United States

- High degree of freedom of speech, which threatens censorship the least.

- Adopting sound cyber security principles (but unrelated to RTBF).

India

- Judiciary's affirmation of privacy as a stored up right.
- Draft PDPB presents the conceptual foundation for aligning RTBF with cyber security and the public interest at its early stage.

Pakistan

- Privacy is enshrined in the constitution through Article 14 and freedom of expression is enshrined through Article 19 which forms a basis for development of RTBF.
- Increasing concerns for digital rights through PECA 2016 as well as the performance of advocacy group.

6.2.2 Weaknesses and Gaps

European Union

- Lacks comprehensive oversight of potential risks in data erasure, and possible undermining of public responsibility.
- Cross border enforcement is still an issue especially in operation of large international social media companies.

United States

- Failure to recognize RTBF erodes privacy rights.
- Freedom of speech can be extended to the level where dangerous posts are allowed to remain up for months.

India

- Lack of local RTBF legislation halts its enactment.
- There is limited investment in technology protection mechanisms.

Pakistan

- Currently laws, there are no provision that specifically addresses RTBF.
- Courts' authority to regulate privacy is weak due to the inadequacy of enforcement mechanisms as well as duplication of authorities.
- Danger to RTBF from political misuse or abuse resulting from overly broad provisions limiting freedom of speech's accountability.

6.2.3 Applicability to Pakistan

- Pakistan can adopt EU GDPR model while modifying the procedural protection that is the spirit of the law.
- Indian approach where central argument involves the constitutional right to privacy will be compatible with the Pakistan legal system and the developments made therein could be used as reference point for drafting out the RTBF legislation.
- Such experience in America proves that freedom of information should not be violated during the practice of Right to Be Forgotten to prevent individuals from abusing this right.

- Utilization of RTBF along with cyber security model as observed in Brazil and India is needed to solve Pakistan' digital security issue.

However, as the comparative analysis shows, the present legislation of Pakistan lacks sufficient detail and there are no grounds for a complicated and well-developed mechanism of the RTBF. The GDPR efficiency has many procedural safeguards that Pakistan should adopt, with India emphasizing privacy in judiciary and Brazil integrating cyber security successfully. It must be a transparent approach; there must be ways to protect freedom of speech, but at the same time, safeguard the privacy of the users; finally, there has to be institutional capability to deter abuse of such a mechanism. The following flowchart gives a clear path on how RTBF could be implemented in order to be fair and accountable in the Pakistani digital scenario.

7. Recommendations for Pakistan

Referring to a crucial comparative study of legal rules and regulations including EU, US, India, and Brazil, much-needed actions for the implementation of the RTBF in Pakistan have been observed to require a proper contextual approach. The following are detailed recommendations to facilitate the establishment of a sound RTBF framework in the framework of Pakistan constitution and legal regime, as well as the societal requirements of Pakistan without overemphasizing privacy while neglecting free speech and cyber security at the same time.

7.1. Legislative Reforms

7.1.1 Pass Comprehensive Data Protection Laws

- Develop and pass a Data Protection Act that provides the RTBF as one of the legal rights without alteration.
- Integrate the provisions of the legislation to conformity with the international best practices for instance GDPR while adopting other provisions to the socio-legal environment in the country.
- The hope of the Act should be to reconcile commercial gains and privacy protection with no ambiguity by defining the terms "personal data," "public interest," "data processor", and "data controller". a statutory right.

7.1.2 Reforms of the Pakistan Electronic Crimes Act (PECA), 2016

- Ramp up legislative additions to PECA to make provision for data erasure and RTBF request.
- Make sure that these amendments relate to issues of overlap between PECA and other legal and regulatory initiatives such as those of the PTA.

7.1.3 Digital privacy: Constitutional reforms

- Amend the constitution to enhance protection and to include effects of digital privacy rights under Article 14.
- Specify the scope of direct limitations under Article 19 selecting the possible degree of interference with freedom of expression while avoiding its transformation into censorship while asserting the compatibility of the RTBF.

7.2. Institutional Strengthening

7.2.1 Set up a Specialized Data Protection Authority

- Formation of an autonomous Data Protection Authority that will be responsible for overseeing the compliance of the RTBF, accepting and addressing requests and complaints.
- Provide judiciary power and abilities to the DPA, funding that will be sufficient and sufficient managerial freedom to serve as an independent body.

7.2.2 Improve Inter Agency Cooperation among the Regulatory Authorities

- PTA, CCP, regulatory agencies and other government departments should work with clearly defined responsibilities so that there should not be any overlapping.
- Develop multi-agency working to adequately meet the complex areas of privacy, protection of data and cyber security.

7.2.3:1 Capacity Building to support the enforcement of laws

- Conduct the investigation in aspects such as establishing technological support structures for the police and regulatory agencies to meet RTBF requests.
- Give means for tracking the degree of compliance by digital platforms and search engines. Competition Commission of Pakistan (CCP), and other regulatory agencies to avoid jurisdictional conflicts.

7.3. Procedural Safeguards for RTBF Implementation

7.3.1 Visible and Normative RTBF Request Procedure

- Establish an easy-to-complete method so that people can easily submit RTBF requests.
- Add that the users should provide proof that the data is bad and they are worse off due to the accuracy of data. Submit RTBF requests.

7.3.2 Public Interest Test

- Introduce a mandatory public interest test for all RTBF requests so as to defend rights to privacy against either undue restriction or erosion while at the same time fostering freedom of expression and/or information.
- Establish guidelines or yardsticks for identifying when information is in the public interest for example – whether exposing public official’s misdeeds, critical to public safety, or of historical importance.

7.3.3 Appeals Mechanism

- Free and enable direct appeals by the affected individual or the third party involved (e.g., journalists or social media) for independent reconsideration of the RTBF decision made.
- Make sure all appeals are addressed ad hoc and fairly journalists or digital platforms) to appeal RTBF decisions through an independent review process.

7.4. Integration with Cyber security Frameworks

7.4.1 Measures on Data Minimization and Erasure

- Provide legal findings that allow businesses and digital platforms to limit the processing of personal data to the minimum.

- Incorporate the provisions of RTBF, into other policies for cyberspace security to lower chances of identity theft and data losses ensuring that only necessary personal data is collected and retained.

7.4.2 Penalties for Non-Compliance

Increase liability for digital platforms and data processors that do not cooperate with RTBF requests or that noncompliant process.

7.5. Awareness and Public Engagement

7.5.1 Public Awareness Campaigns

- Organize intensive promotional campaigns in the form of specifically targeted information regarding the rights of the citizens in the digital age and the RTBF in particular as well as the procedure that needs to be followed in order to exercise those rights.
- Engage civil society agents and digital rights advocacy group to boost up publicity rights, including the RTBF, and how to exercise these rights.

7.5.2 Stakeholder Consultations

- Refine and enhance the RTBF framework by consulting legal advisers and journalists, social media websites, and consumer organisation is inclusive and equitable.

7.5.3 Promote Digital Literacy

• Incorporate education in the about privacy and data protection in order to allow them acquire knowledge in dealing with matters related to computers.

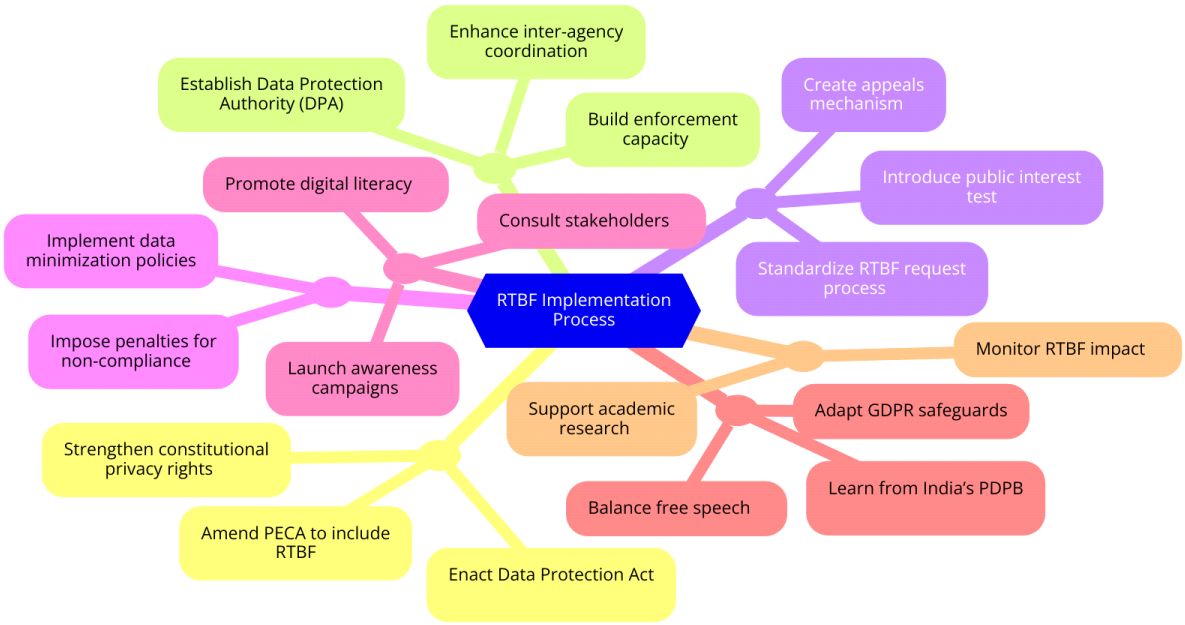

Figure 1: flow chart of Recommendations

7.6. Learning from Global Best Practices

7.6.1 Implement Some Components of the GDPR Model

Provide procedural protections as outlined of the GDPR; the involvement of supervisory authorities; and notification provisions.

7.6.2 Get Inspired with India's PDPB

Reinforce the constitutional privacy rights in the Indian context in order to suit the Pakistani law and etiquette by stressing on the RTBF.

7.6.3 Meeting US's Concern on Freedom of Expression

Calm down RTBF with appropriate fundamentals of free speech since their experience from the United States' First Amendment is omnipresent over-emphasized.

7.7. Research and Monitoring

7.7.1 Improving the assessment of the impact of RTBF.

- Set up ways of measuring compliance with the RTBF as well as its effect on privacy, Free Speech and cyber security.

Engage in impact assessments, which would help to put light on the areas that such services can be misused or where enforcement is lacking.

7.7.2 Encourage Academic Research

- Contribute of the academic and policy-related works in the digital privacy/ data protection & RTBF research to justify the policy making.

To domesticate RTBF in Pakistan, Pakistan should incorporate detailed laws, include Data Protection Authority, launch awareness programs, improve technologies and adhere to the international standards. The framework of the Personal Data Protection Bill should clearly address the RTBF proposing measures for its enforcement and defining the circumstances under which it cannot be applied. Capacity development and establishing an IT identification program may achieve the implementation of the RTBF.

8. Conclusion

The Right to Be Forgotten as a new type of legal and ethical concept in the framework of the information society is an opportunity to regain control over data on oneself. In Pakistan context particularly where public internet usage and digital identity are dramatically growing, the adoption of the RTBF provide huge importance for overseeing essential issues of privacy, misuse of data and cyber security concerns at large. But when it comes to its actual putting into practice, there are numerous issues that can be touched upon starting from the problems with Portal privacy and free speech all the way to the problems of Portal cyber security.

This research has also presented that unlike other jurisdictions Pakistan does not have a specific provision of RTBF at the present legal regime, so privacy of a person in the cyber world remains insecure. There are still laws like PECA, 2016 that offer somewhat privacy protection but do not offer robust protection against data erasure or provide the right to individuals to delete inconvenient, irrelevant, detrimental information. However, the constitutional rights of privacy (Article 14) and freedom of speech (Article 19) remain under developed especially in the aspect of Digital Rights and therefore the question arises whether the RTBF became a tool for Censorship of dissent.

Conclusions made here for Pakistan yield insights from comparative experiences worth learning from, including the European Union, United States, India, and Brazil. The EU GDPR provides a strong procedural context for the realization of the RTBF while maintaining due regard for privacy, public interest, free speech. On the other hand, the United States of America cherishes

abovementioned freedom of expression and precautionary measures pulled off in this domain are considered to be invasive and oppressive. Due to changing legal landscape of the India especially with recent pronounced right to privacy repeatedly the Indian context offers a model for embedding the RTBF in a constitutional and cultural context akin to Pakistan. Such global practices only serve to reinforce principles of much-needed legal sensitivity in Pakistan that may encompass socio-legal, cultural and technological structure of the country.

Hence, for Pakistan, the RTBF has become not only about privacy but also about a necessity to defend the country's cyber space and engage the public in trusting more in digital environment. Nevertheless, its proper functioning is predicted to encounter considerable institutional and procedural barriers. Key challenges include the lack of an all-embracing Data Protection Act, conflicting competencies and the public's poor awareness of digital rights. Besides, careful solution of the political misuse of the RTBF and lack of sufficient guarantees for the public interest must be addressed.

In order to transverse these gaps, the following recommendations are made in this study. These are the current measures that need to be taken including passing of stringent data protection laws, amending constitution to provide enhanced privacy assurance to users and the formation of a specialized Data Protection Authority for the RTBF. Other formal protections in the form of clear RTBF request processes, public interest override tests, and actually seeking appeals also need to be provided. Additionally, linking of RTBF to the cyber security policies and conducting of awareness can improve the practical application of this right in addition to creating of digital responsibility.

All in all, it may be assumed that by using the RTBF Pakistani citizens may regain more control over the provided personal data, as well as increase individual dignity and cyber protection. That is why, nevertheless, its effectiveness is achieved primarily by experimenting with freedom of speech, privacy, and public interests. It is now clear that any country that adopts RTBF without fully understanding the implications of the approach risks creating an illiberal dystopia that has marred the evolution of digital rights across the world including freedom of expression and access to information. This therefore would be a big stride in preventing invasion of privacy in the digital space, encouraging use of the social media platforms through assurance of privacy and sorting out Pakistan's legislation system to fit global standards in the modern society.

References

1. Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data Privacy and Protection: Legal and Ethical Challenges. *Emerging Threats and Countermeasures in Cybersecurity*, 433-465.
2. Huynh, T. T. (2025). Everyone Is Safe Now: Constructing the Meaning of Data Privacy Regulation in Vietnam. *Asian Journal of Law and Society*, 1-29.
3. Cocito, C., & De Hert, P. (2025). Relying on digital principles to complement existing rights: a human rights assessment of the 2022 European Declaration on Digital Rights and Principles. In *Research Handbook on Human Rights and Digital Technology* (pp. 167-191). Edward Elgar Publishing.
4. Aleke, N. T. (2025). The Role of Cybersecurity Legislation in Promoting Data Privacy. In *Integrating Artificial Intelligence in Cybersecurity and Forensic Practices* (pp. 205-244). IGI Global Scientific Publishing.
5. Divyashree, K. S. (2025). Safeguarding the future through the prevention of cybercrime in the quantum computing era. In *Next Generation Mechanisms for Data Encryption* (pp. 258-276). CRC Press.

6. Conde, I., Li, Y., & Vyas, R. P. (2025). Global Companies and China's Data Privacy Laws: Analysing DIDI'S Case and Regulatory Compliance Implications. *Chinese Journal of Transnational Law*, 2753412X241288770.
7. Chmielarz, G. (2025). Data Privacy and Entrepreneurial Responsibility. In *Digital Sustainability* (pp. 36-48). CRC Press.
8. Papadimitriou, S., & Virvou, M. (2025). General Data Protection Regulation and Adaptive Educational Games. In *Artificial Intelligence—Based Games as Novel Holistic Educational Environments to Teach 21st Century Skills* (pp. 253-275). Cham: Springer Nature Switzerland.
9. Jiang, M. (2025). Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa. *Policy & Internet*.
10. Rudden, L. (2025, January). Fragmented Data Privacy Laws: Time for Federal Legislation. In *Boston College Intellectual Property and Technology Forum* (Vol. 2025, pp. 1-18).
11. Rampášek, M., Mesarčík, M., & Andraško, J. (2025). Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification?. *Computer Law & Security Review*, *56*, 106093.
12. Sun, P., Wan, Y., Wu, Z., Fang, Z., & Li, Q. (2025). A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. *Computers & Security*, *148*, 104097.
13. Thir, V., & Wawra, D. (2025). Data Protection and Information Privacy. *Data Protection and Information Privacy*.
14. Hamid, S., & Huda, M. N. (2025). Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023. *Social Sciences & Humanities Open*, *11*, 101234.
15. Gupta, N., & George, A. (2025). Digital Personal Data Protection Act, 2023: Charting the Future of India's Data Regulation. In *Data Governance and the Digital Economy in Asia* (pp. 34-53). Routledge.
16. Guo, S., & Li, X. (2025). Cross-border data flow in China: Shifting from restriction to relaxation?. *Computer Law & Security Review*, *56*, 106079.
17. Harish, V. S. K. V., Gupta, S., Bhatt, J. G., & Bansal, M. (2025). International standards, regulations, and best practices for cyber security of smart grid. In *Cyber Security Solutions for Protecting and Building the Future Smart Grid* (pp. 321-348). Elsevier.