

Reconceptualizing the right to be forgotten: constitutional lacunae in Pakistan and legislative insights from Latvia

Muhammad Imran Ali LL.M*

Quaid-e-Azam Law College, Kasur-Pakistan; ORCID: 0000-0003-1395-229X

Abstract

This article redefines the right to be forgotten (RTBF) as the key element of digital constitutionalism, paying attention to both its strictly legal and normative embodiment in Pakistan. It places the right in the context of the larger development of data subject rights and relies on the original jurisprudence such as the Google Spain judgment and the General Data Protection Regulation (GDPR) in the EU. The article criticizes the constitutional silence of Pakistan through a theoretical approach based on autonomy, human dignity and informational self-determination and then assesses the legislative gap on data deletion. In contrast, Latvia proposes a good example of Article 96 of the Constitution, Personal Data Processing Law, 2018, and the important position of the Data State Inspectorate. Based on the comparative constitutional approach, the article has provided a solid legal roadmap of Pakistan; it has suggested the amendment of the Constitution, the formulation of a data protection law, and the creation of an independent regulatory body. Finally, the article develops the right-based solution to digital privacy, which is vital to maintaining human dignity in the age of the algorithm.

Keywords

Data Protection • Digital Privacy • Latvia • Pakistan • Right to Be Forgotten

INTRODUCTION

Digital era has changed the quality of privacy, autonomy and identity, and poses new challenges to national legal regimes everywhere. One of such challenges has become the right to erasure and its role as a pillar of data subject rights (Eskens, Helberger & Moeller, 2017). It gives people the right to demand expungement of old, out of date, irrelevant or inaccurate or unlawfully processed personal data (Allegri, 2022). Article 17 of the General Data Protection Regulation (GDPR) of the European Union (Hoofnagle, van der Sloot & Borgesius, 2019), and the Court of Justice of the European Union (CJEU) landmark finding in Google Spain SL and Google Inc, v Agencia Esp a nola de Proteccon de Datos (AEPD) and Mario Costeja Gonz lez (Frantziou, 2014), can be deemed as the best manifestations of both the conceptual and legal development of RTBF.

This article reveals a large constitutional and legislative gap in the Pakistan legal system about digital privacy and the RTBF. In spite of the increasing rate of internet penetration and the development of data ecosystems, Pakistan does not have a statutory regime garnering individuals the ability, through the

Constitution, to demand erasure of their data. Under Article 14 of the Constitution of Pakistan, 1973, the right to dignity and privacy is granted, yet it is limited to the physical privacy and dignity only, not to the online identity or informational independence (Ali & Hussain 2024). The extraction of a homogeneous jurisprudence around digital rights has not been established by the courts and Pakistan has not ratified any comparable law to the GDPR. Consequently, people are susceptible to damage to their reputation, loss of personal control of their data, and the ability of outdated or disgraceful information to affect a long-term impression.

This article tries to find out the way in which Pakistan can implement a suitable model that would work and fit in its context in order to recognize and implement the RTBF. This article will draw some comparative lessons learnt on Latvia, which is a post-Soviet country, a democratic country where the process of digital and constitutional transformation has been strong in the European Union. Latvia is selected mainly because of three reasons, because of its relative size, as far as the legal system is concerned, Latvia is much more accessible and replicable model of a system that is structurally similar to its developing juniors in the EU. Second,

* Corresponding author: principal.kasur@qlc.edu.pk

Open Access. © 2025 Muhammad Imran Ali, published by Sciendo

 This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

although Latvia is constitutionally not comparable to Pakistan, yet there are certain historical peaks on which the country seems like Pakistan, i.e. a country that has travelled the path of authoritarianism to constitutional democracy. Third, Latvia has implemented the RTBF into its National legislation, the Personal Data Processing Law, 2018, based on the principles of GDPR (Potaičuks, 2024), and implemented by the Data State Inspectorate (Nikiforova, 2018) and constitutional guarantees, Article 96, which protects the right to privacy.

The choice of selecting Latvia, nevertheless, does not present us with a direct transposition of the legal norms of the European context to the South Asian. Instead, Latvia is presented as a referential framework that, because of its EU commitments and membership of wider rights monitoring groups like the Council of Europe and the United Nations, describes a stratified and rights-based solution to digital privacy. These are not only the rulings of the European Court of Human Rights (ECtHR) and the guidelines of the EU Data Protection Officer, but also reports of bodies like the Fundamental Rights Agency that adds to the experience of Latvia, as well as providing useful lessons of the procedural, legislative and institutional routes to data protection and digital dignity. This comparative perspective enables a normative analysis that is sensitive of scale of the institution, democratic accountability and constitutional adaptation in a particular legal realm in Pakistan.

The article adopted a doctrinal and comparative method of legal approach whereby the attention is given to legal texts, constitutional articles, judgements and legislative dynamics. The modes of interpretation are textual, purposive and teleological interpretation of legal norm and a rights-based interpretation which is focused on values of informational self-determination, human dignity and autonomy. It is suggested that primary legal sources, i.e. the Constitution of Pakistan and the Personal Data Processing Law of Latvia are critically examined in comparison with the judgment of the CJEU, ECtHR, and national courts. Secondary materials can be found in scholarly works, policy documents, and reporting by human rights bodies.

To support the scientific clarity and analytic structure of the article, a series of research questions were developed that reconsidered the general hypothesis of the article as follows; How well is the right to be forgotten recognized and protected by the existing constitutional and legal framework in Pakistan? What are the provisions in Latvia to carry out the RTBF in its domestic law, particularly strict adherence to GDPR and outer European human rights systems and frameworks? How might Pakistan, with the experience of Latvia in mind, use legislative, institutional, and constitutional means to come up with a contextually appropriate and implementable regime of digital data erasure?

These questions inform the analysis because it defines it with the normative inquiry, and it is enhanced with the comparative legal research. Instead of a blanket transfer of legislation, the article promotes legal transfer in contextual parallels and incremental change, including the amendment of the present laws to privacy, enhancing the provisions of legislative bodies such as the Pakistan Telecommunication Authority, and compelling the digital dignity being appreciated in the newsstands of Article 14.

Lastly, the paper intends to bridge an important academic and policy gap. It does this by providing a theoretically informed and rights-based legally actionable roadmap to enshrine the right to be forgotten into the legal system of Pakistan based on the Latvian experience and generally the European project of data protection.

RESEARCH RESULTS AND DISCUSSION

Theoretical and international foundations of the right to be forgotten

Right to be forgotten (RTBF) is one of the contemporary legal phenomena that intersects with aspects of privacy, reputation and digital memory (Stainforth, 2021). Due to the emergence of digital technologies, search engines and social media, personal data have been challenging the individual rights of control and use of their own information and dignity. To rectify these issues, RTBF will endow people with the right of asking to remove or erase their personal data that has become outdated, irrelevant, or damaging.

The theoretical foundations of RTBF have a solid grounding in established sets of philosophical and legal principles; they predominantly involve the privacy rule and esteem. One fundamental human right is privacy, which is guaranteed within an instrument as the International Covenant on Civil and Political Rights (ICCPR) Article 17 that guarantees one against arbitrary interference with his or her privacy (Taylor, 2020). Under the category of privacy, there is reputation that concerns the right to honour and dignity, which is especially topical in the digital sphere because there is always a risk of reputation expansion and the impossibility to erase unwanted data.

Unlike human memory, the digital memory is not lost with time. This indestructibility of internet information jeopardizes the capacity of people to forget the past or the errors. Viktor Mayer-Schönberger maintains that digital permanence inhibits human development, as people are always reminded about themselves repeatedly due to their earlier activities (Smith & Mayer-Schönberger, 2009). RTBF is a balm which helps to bring back into possession of the control of their own story and attain what Mayer-Schönberger refers to as the right to obscurity.

The Court of Justice of the European Union (CJEU) in *Google Spain SL and Google Inc. v AEPD and Mario Costeja Gonzalez*, 2014, declared the doctrine of RTBF by using the legal terms of references in the legislation. In this judgment, the court decided that, people are entitled to direct search engines to remove links that include information that is substandard, of no concern or not relevant anymore (Youm & Park, 2023). The decision came to form Article 17 of the EU General Data Protection Regulation (GDPR) which formulized the right to erasure.

According to Article 17(1) of the GDPR (Regulation (EU), 2016), data subjects have the right to demand the erasure of personal data provided that the data is no longer necessary, the consent has been withdrawn, and so on. Nevertheless, Article 17(3) stipulates exceptions to this right, so that the freedom of expression, the public interest and the requirements of the law should not be harmed (Juliussen, 2023). The RTBF can, therefore, not be absolute, it comes with a context of proportionality where personal privacy can be traded off against those of the society.

RTBF principles as also established by the European Court of Human Rights (ECtHR) through Article 8 in the European Convention on Human Rights involving the right of respect of a private and family life. In *M.L. and W.W. v. Germany*, 2018, the ECtHR affirmed the decision by Germany not to delete the names of convicted persons out of online archives because of the necessity to reconcile privacy rights with the right of freedom of the press (Čtvrtník, 2023).

RTBF is philosophically justified by the principle of autonomy, of dignity, and of informational self-determination. With autonomy, people are free to establish their identity without constant digital consideration. Dignity as understood in the legal constitutions such as the Article 1(1)) Basic Law of Germany (Grundgesetz) obliges to treat people with respect, and the circulating outdated or stigmatizing information cannot be forgotten in time (Shultziner & Carmi, 2014). The so-called informational self-determination, introduced by German Federal Constitutional Court in its 1983 decision concerning the Census Act (BVerfGE), provides the right of individuals to management of their personal data, which has also occurred in the concept of GDPR and the CJEU decisions (Eberle, 2012).

Against the permanence of information on the internet, RTBF serves a critical reaction. The fact that it is theoretically well-grounded, based on privacy, reputation and dignity as well as autonomy and the international recognition of its validity particularly in the European Union makes it a potentially hard model to be adopted elsewhere. In the case of Pakistan, the RTBF offers a chance to reform the constitution and overhaul legislative initiatives influenced by the European patterns such as Latvia to guarantee the security of personal information and human dignity in the age of digitalization.

Constitutional silence in Pakistan on data privacy and erasure

There is a distinctive lack of mentioning the Right to Be Forgotten (RTBF) in the constitutional and legal set up of Pakistan that especially since more countries are making concessions internationally with regard to data privacy and digital erasure rights. Although other countries such as the European Union have implemented a viable legal framework to ensure protection and erasure of personal data, mainly, General Data Protection Regulation (GDPR), Pakistan remains in an old, incomplete legal framework (Jabeen Khan, A., Mushtaq, S. A., Siddique & Wadood, 2025). Such insufficiency is most prominently manifested in the restrictive understanding of the Article 14 of the Constitution, the lack of a comprehensive data protection law, and judicial interest in digital rights, whose repercussions can be drastic to both personal liberties and institutional practices.

Dignity of man and the privacy of home have been enhanced under Article 14 (1) of the Constitution of Pakistan, 1973. Nonetheless, the meaning of this provision has traditionally been used rather narrow, particularly in connection with physically accessible or spatial privacy, and not with the information, or digital privacy (Khan, Gul, Naznin & Khan, 2022). Whereas non-progressive constitutional paradigms are used in countries like Germany or South Africa where dignity is inclusive of the right of the individual to regulate personal data, Pakistani jurisprudence has yet to develop in favour of it. It is important, in terms of jurisprudential implication, to underscore that despite the fact that the Constitution of Pakistan, 1973, declares a right to life, under Article 9 and secures right to human dignity, under Article 14, as fundamental, infallible, and supreme, it is also silent, conspicuously, on the express safety of the data privacy and the new rights of digital deletion. The Supreme Court in the *Monal Group of Companies v. Capital Development Authority*, and *Jawwad S. Khawaja v. Federation of Pakistan* have proudly broadened the interpretive spectrum of dignity to embrace the elements of ecological well-being as well as procedural fairness, thereby meaning a dynamic and evolving constitutional culture. Still, the evolution fails in the digital realm, since the constitutional text has no explicit positive expressions of informational independence, data economy, the right to be forgotten.

Although cases like the *Munir Ahmad Bhati v. Director FIA Cyber Crime Wing, Lahore* and *Bytes for All v. Federation of Pakistan* highlights an infantile understanding of the dignity of cyberspace, they only point in the direction of protection without a normative system. The lack of the development of the legal framework of concepts of dignity in virtual space in the context of modern developments is a gap in the Constitution that hinders the comprehensive manifestation of dignity in cyberspace. The closure of this gap requires a pressing constitutional response (namely a textual amendment or a

judicial reinterpretation), in order to avert the danger of the emerging architecture of digital human rights in Pakistan.

In legislation, Pakistan does not have a general data protection law. The Prevention of Electronic Crimes Act, 2016 (PECA) covers the misuse and unauthorized access to data by referring to it in Section 3, 4 and 20 of the said Act. Nonetheless, it is rather punitive and does not require positive rights to the data subject, including the right to erase, correct, or de-index (Yongmei & Afzal, 2023). As opposed to Article 17 of GDPR, PECA does not impose on data controllers and platforms any proactive obligation to observe erasure requests. The Personal Data Protection Bill, 2023, as it stands in its draft form is still awaiting legislation, so at this point there is no formal law in Pakistan that allows protection of digital identity of citizens or addresses RTBF.

Lack of constitutional and legislative guarantees of basic right to erasure exposes people to risks of reputational harm, identity theft and, ultimately, the lasting effects of outdated digital information or factually misleading digital information. There is nothing that citizens can use to demand that such data be deleted on search engines or social media. Even public institutions lack clear, recognizable data governance aspects, further making it difficult to comply or be held accountable.

This legal black hole does not only undermine individual rights, but also leave Pakistan at odds with the international human rights regime that ensure that individuals are protected against arbitrary interference with his or her privacy under Article 17 of the International Covenant on Civil and Political Rights (ICCPR) (McCrudden, 2008). Unless Article 14 gets expanded in the lens of interpretation and a broad data protection law is adopted, the state of information sovereignty of Pakistan will be further negated.

Constitutional and legislative silence on data privacy and erasure in Pakistan means the change must happen promptly. Based on such comparative models as the Latvia GDPR-adoptive framework of laws, Pakistan should undergo a transformation of its approach to national legislation in order to be able to keep pace with global trends and protect digital dignity, autonomy, and privacy.

A constitutionally anchored approach to digital privacy in Latvia

Latvia introduces a constitutionally-based and thorough system of digital privacy protection and the use of the right to be forgotten (RTBF), which is applicable to countries such as Pakistan, which have limited constitutional and legislative safeguards to data privacy. Chapter 8 of the Constitution of the Republic of Latvia, titled "Fundamental Human Rights," was adopted in 1998, this part is the basic foundation of human rights development in Latvia (Balodis, Kārkliņa & Danovskis, 2023). It has legalized some major civil liberties

such as the right to privacy, expression, and protection of personal information. Article 96 is especially applicable, which does ensure an inviolability of a home, correspondence, and private life, which are interpreted as covering digital privacy as well. Chapter 8 provides constitutional foundation of modern rights like Right to Be Forgotten within more comprehensive level of human rights, as Latvia aligns itself with European Convention on Human Rights and the law of the European Union. (Krūma & Statkus, 2019).

Latvia has adopted the Personal Data Processing Law in 2018 to commit itself to the idea adopted in the constitution and domestically engages in the General Data Protection Regulation (GDPR) established by the European Union (Naef, 2023). This law states the rights of data subjects and the duties of the data controllers and data processors and they are at par with the European standards. The relevant Sections of the Latvian law is; Section 4, which provides people with the right to access, correct and erase their personal data, Section 9 that states data processing must be carried out by journalists with freedom of expression, and privacy rights that is crucial in RTBF cases, Section 15 that imposes obligation on data controllers of safe and lawful processing of data.

Latvia acknowledges the RTBF and enables it through the following provisions, justifying the Article 17 of the GDPR stating that people can demand that personal data be deleted in situations where the data is no longer relevant or where consent has been withdrawn. Simultaneously, the right is conditional and proportional to the law, where it acknowledges valuable exceptions, including the interest of the general public and the freedom of expression (Alessi, 2017).

Violation of data protection regulations in Latvia falls within the management and regulation of the Data State Inspectorate ((Datu valsts inspekcija or DVI),) which is formed under the Personal Data Processing Law, 2018. This autonomous agency makes sure that the law is obeyed, handles complaints, and gives fines. Its jurisdiction consists of; Audits and investigations of illegal data processing under Section 25, issuing binding instructions to cease processing or erase data under Section 26 and cross-border consistency with the European Data Protection Board.

During the past few years, the Inspectorate has indicated an increment in social awareness and RTBF-related complaints. Entering the example, in 2021, the agency solved a number of cases related to the removal of obsolete criminal data records in the results of search engines. In a balancing test that paid attention to the right of the people to know and the right of privacy of the person, the Inspectorate incorporated the principles of GDPR.

This balance has been strengthened by Latvian courts. In the case of Consumer Rights Protection Centre v. Private individual, the court approved the demand of a citizen to delete

false personal information on a state information database. The judgment was made under Article 96 of the Constitution and The GDPR 17th article highlighting the responsibility of the judiciary to the rights of data subjects and state responsibility. Besides, when it comes to applications concerning media archives, the courts have always been sensitive to the sensitivity of information, the lapse of time, and the interest of the society and the present position of the individual society holds. This puts Latvian jurisprudence in line with a development of ECtHR standards and puts forward a sophisticated RTBF implementation that protects individual dignity, at the same time, preserving democratic transparency. Latvia has a constitutionally and legislatively built strategy to the digital privacy incorporating Article 96, the Personal Data Processing Law, 2018, and the Data State Inspectorate that act in a coordinated manner to guarantee the rights of individuals. It is a model that offers a viable and practical framework that Pakistan can use in its endeavor to come up with coherent laws on data protection and the Right to Be Forgotten. Following the experience of Latvia, Pakistan can pave the way to the future where the rules on digital dignity and informational autonomy are considered and safeguarded by its legal and constitutional frameworks.

A comparative analysis between Latvia and Pakistan

The Right to Be Forgotten (RTBF) has become an essential legal thought in the current digital world where online exposure and the storing of information are a considerable threat to individual responsibility and integrity. Latvia provides a constitutionally and legislatively harmonized system which is effectively protecting the digital privacy. Such a model is a stark contrast to the fractured constitutional and legal framework of Pakistan, and it is a critical example that Pakistan can learn to transform a data protection framework of its own.

In the center of Latvian framework is the Article 96 of national Latvian Constitution ensuring the right to personal life, domicile, and any private correspondence (Dupate, 2016). Notably, Latvian courts have interpreted this provision wide to embrace digital privacy and RTBF, which conforms with the modern state of international human rights. These constitutional guarantees are further implemented in the Personal Data Processing Law (2018) in the Republic of Latvia to the extent permitted by the General Data Protection Regulation (GDPR) of the European Union. Important provisions in Section 4, 9 and 15 provide enforceable rights to have an access to, correction, and deletion of the personal data and impose responsibilities on data processors to protect privacy.

Conversely, article 14 of the Constitution of Pakistan, 1973 protects the dignity of man and privacy of home, which have been narrowly defined, and usually restricted to the physical or

spatial privacy. There have been some exceptional decisions like the Monal Group of Companies Islamabad v. Capital Development Authority, Jawwad S. Khawaja v. Federation of Pakistan, Munir Ahmad Bhati v. Director FIA Cyber Crime Wing, Lahore and Bytes for All v. Federation of Pakistan. The courts have since failed to bring this protection into the digital world. Consequently, it leads to the lack of unambiguous constitutional status of informational self-determination in Pakistan.

Latvia has strength in the structural coherence of the constitutional as well legislative framework supplemented with a powerful enforcer of the law, the Data State Inspectorate that will be created pursuant to the Section 24 of the 2018 Law. This is a statutory audit, investigative and enforcement body to guarantee that the right to data by the citizens becomes a reality. A libertarian approach has also been demonstrated by the Latvian courts when they applied a balanced rights-based approach RTBF to the judgment in Consumer Rights Protection Centre v. Private individual and instructed that the right of a citizen to have inaccurate data removed from a state database be upheld under both constitution and the GDPR.

Pakistan is, however, not ready in terms of such institutions. Although the digital regulation is carried out by an agency such as Pakistan Telecommunication Authority (PTA) and Federal Investigation Agency (FIA), they do not have a legal orientation and autonomy to execute the RTBF principles. The Prevention of Electronic Crimes Act, 2016 (PECA), especially, Section 3, 4, and 20, only offer restrictive and penal measures towards the misuse of data, but they do not incorporate a user rights-based approach. Also, the Personal Data Protection Bill, 2023 of Pakistan still does not enjoy legislative success and creates an open gap in data subject protection.

However, there exist some possibilities to fill this gap, Pakistan has opportunities, its courts have been activist in interpreting the constitution rights and can be persuaded to use Article 14 in a new light with the Islamic values, like, *hurmaat-e-insaan* (dignity) and *pardah* (privacy) to include digital privacy (Sarwar, Azhar & Baig, 2024).

Pakistan can learn some strategic lessons, which would help it to bridge its current gaps in constitutional and legislative protections of digital privacy: it should introduce a broad privacy-protective law based on the model of the GDPR and the Personal Data Processing Law, 2018 in Latvia, including the right to be forgotten; create an independent, autonomous body on Data Protection with authority to enforce data protection legislation and modeled after the Latvian Data State Inspectorate; educate the judicial system to integrate comparative jurisprudence in regards to digital rights legislations that would enable the courts to apply their reasoning using All in all, the constitutionally fixed,

institutionally guaranteed interface of digital privacy in Latvia provides a useful guideline to Pakistan. The example of Latvia proposes that RTBF is not a Western invention but the global necessity of law in preserving personal dignity in the era of digitalization. The challenge is not the wholesale copying of the model but its contextual adaptation in the case of Pakistan, where constitutional tenets, lawful procedures and, institutional abilities are to be developed concomitantly to shield citizens in the digital age.

Although Pakistan cannot exactly copy the example of Latvia, the gradual incorporation of the international standards into the national system introduced by Latvia can serve as a valuable guideline towards a more targeted process of legal changes and organizational building.

Towards a constitutional and legislative framework for data erasure in Pakistan

The right to be forgotten (RTBF) whereby a person can require the erasure or de-listing of his or her own information on certain terms, is becoming an indispensable aspect of online privacy and control in the 21st century. The article analysis consists of four major parts: the entrenchment of the Right to Be Forgotten (RTBF) in the Constitution; the adoption of detailed legislation on personal data security; the creation of an effective and independent data protection defense; and the national regulations, and the international practices convergence.

The Constitution of Pakistan does not provide a specific mention of the RTBF, which gives it an exposure to different interpretations. Article 14 of the Constitution guaranteed the right to dignity and the privacy of home, although there is no direct mention of digital privacy, or informational self-determination. The inclusion of the RTBF in the right to privacy should come out clearly in the proposed amendment to the constitution. As an example, one can propose the insertion of a new Article 14A, which will read as follows:

*Article 14A. The right to informational self-determination
"It shall be guaranteed to every individual the information self-determination and have the right to request that his or her personal data be erased or restricted as provided by this law."*

The Constitution of Latvia, although equally silent, has also worked out a data protection jurisprudence based on adherence to the General Data Protection Regulation (GDPR) of the EU, which formally acknowledges RTBF in Article 17. Pakistan may also do the same by pegging such a right on its constitution hence legally clarifying its interpretation to the courts and grounding the right on fundamental rights jurisprudence.

The Personal Data Protection Bill 2023 (PDP) that is yet to become law in Pakistan tries to cover the issue of the Right to be Forgotten (RTBF) in a narrow-minded manner, which is not enforceable and comprehensive. Pakistan must also develop a strong data protection law based on the following main principles: purpose limitation i.e. uses the data to only enable its purpose; data minimization that is retention of only the needed data; the right to erasure must be explicitly stated along with conditions; transparency and consent that is informed consent is required to all processing of personal data. The RTBF must also be expressed in a special section in the proposed Bill 2023 as a revised law and must include the following grounds: withdrawal of consent, data no longer necessary, unlawful processing, or relevant to a legal obligation.

Successful enforcement-mechanism conditions the success of the Right to Be Forgotten (RTBF). The draft Personal Data Protection Bill 2023 provides a Commission, which however is compromised by the government control and politically biased appointments. Pakistan should also seek to form its Data Protection Authority (DPA) as an independent body with quasi-judicial powers over data related matter, power to fine and data erasure, and total independence on appointments and budget to bring fairness and resisting the political influence. The revised section of the proposed Data Protection Bill, 2023 should adequately spell the structure of the DPA which must be autonomous, in terms of operation and cash-related matters.

Pakistan needs to align its national regulation of data protection with the international norms of human rights. The international commitment to digital rights is demonstrated by the Resolution 68/167 on the Right to Privacy in the Digital Age adopted by the United Nations General Assembly and the International Covenant on Civil and Political Rights (ICCPR) to which Pakistan is a signatory (Milanovic, 2015).

In addition to that, having Latvia as an example of harmonizing to GDPR, Pakistan must follow principles of extraterritorial applicability and reciprocity, moreover, allowing cross-border data flow with appropriate protection. Particular section must require international treaties and discourse on rights in the digital setting in line.

Pakistan is in a critical crossroad of defining its digital future. A constitutional entrenchment of the right to be forgotten, the development of a comprehensive personal data regulation with justiciable rights, the creation of an independent Data Protection Authority, and conformity with international standards will make the individual dignity and data sovereignty a reality in the cyber world. Based on the Latvian and general GDPR methods, Pakistan will be able to protect the data of citizens while stimulating transparency, trust, and technological advancement.

CONCLUSION

The digital world has mostly transformed the aspect of the personal autonomy, memory, and reputation within the society. Given that people are getting exposed to more and more algorithmic memory, and this tendency results in a permanent information retention, the legal frameworks should be adjusted accordingly to guarantee a right to informational self-determination. In Pakistan, the protection of constitutional principles against invasion of privacy and dignity, though restricting in physical aspect, provided in Article 14 of the Constitution have a gap in regard to protecting the privacy in the digital aspect. That highlights the necessity of a complete doctrine of digital constitutionalism.

The case of Latvia is an instructive comparative example not because of similar contexts but because it can be used as an example of how a minor EU member can monitor the adjustment of its domestic law to supranational standards, such as the General Data Protection Regulation (GDPR) and supranational bodies (such as the Council of Europe and the European Court of Human Rights). Chapter 8 on Fundamental Rights of Latvia that entered into operation in 1998 and the Personal Data Processing Law, 2018 which is enforced by the Data State Inspectorate evidences the cohesive system that guarantees the right to be forgotten as established under the Art. 17 GDPR.

Pakistan has to use these structural and procedural aspects and incorporate them in their own legal and cultural environment. This also involves institutionalising RTBF within its constitution with a view of incorporating this into either Article 14A, or enactment of a robust independent DPA. Any domestic changes will also be proved to be more legitimate in accordance with the international instruments such as the ICCPR and the UN Resolution on Privacy in the Digital Age. It is finally clear that RTBF is not only a legal obligation but also ethical obligation of regulating human dignity.

REFERENCES

- Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, 32(1), 145–171. <https://scholarlycommons.law.emory.edu/eilr/vol32/iss1/4>
- Allegri, M. R. (2022). The right to be forgotten in the digital age. In F. Comunello, F. Martire, & L. Sabetta (Eds.), *What people leave behind* (Vol. 7, pp. [page range if available]). Springer. https://doi.org/10.1007/978-3-031-11756-5_15
- Ali, M. I., & Hussain, K. A. (2024). Unveiling the tapestry: A comparative investigation into data-protection legislation in India and Pakistan. *Socrates*, 1(28), 1-8.
- Balodis, R., Kārklīņa, A. & Danovskis, E. (2023). The development of constitutional and administrative law in Latvia after the restoration of independence. *Juridiskā Zinātne*, 5, 44–119.
- Bytes for All v. Federation of Pakistan, W.P. No. 958/2013 (Islamabad High Court).
- Consumer Rights Protection Centre v. Private individual, ECLI:LV:AT:2023:0807. A420234319.27.L (Latvia Supreme Court, Department of Administrative Cases, Aug. 7, 2023).
- Čtvrtník, M. (2023). Personality rights, privacy, and post-mortem privacy protection in archives: International comparison, Germany and “protection of legitimate interests.” In *Archives and Records*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-18667-7_2
- Dupate, K. (2016). The constitutional social security rights in Latvia. *Studia z Zakresu Prawa Pracy i Polityki Społecznej*, 23, 125–140.
- Eberle, E. J. (2012). Observations on the development of human dignity and personality in German constitutional law: An overview. *Liverpool Law Review*, 33, 201–233. <https://doi.org/10.1007/s10991-012-9120-x>
- Eskens, S., Helberger, N., & Moeller, J. (2017). Challenged by news personalisation: Five perspectives on the right to receive information. *Journal of Media Law*, 9(2), 259–284. <https://doi.org/10.1080/17577632.2017.1387353>
- Frantziou, E. (2014). Further developments in the right to be forgotten: The European Court of Justice's judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Española de Protección de Datos. *Human Rights Law Review*, 14(4), 761–777. <https://doi.org/10.1093/hrlr/ngu033>
- Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, EU:C:2014:317 (Court of Justice of the European Union).
- Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), 65–98. <https://doi.org/10.1080/13600834.2019.1573501>
- Jabeen Khan, A., Mushtaq, S. A., Siddique, M. A., & Wadood, M. A. (2025). The right to be forgotten in the digital age: A Pakistani perspective on balancing data protection & privacy, freedom of expression, and cyber security. *Journal for Social Science Archives*, 3(1), 387–403. <https://doi.org/10.59075/jssa.v3i1.126>
- Jawwad S. Khawaja v. Federation of Pakistan, PLD 2024 SC 337.
- Juliussen, R. J. (2023). Algorithms that forget: Machine unlearning and the right to erasure. *Computer Law and Security Review*, 51, 105885. <https://doi.org/10.1016/j.clsr.2023.105885>
- Khan, A. S., Gul, R., Naznin, S., & Khan, Y. (2022). The right to privacy, its progress & decline: A critical review. *Journal of Business and Social Review in Emerging Economies*, 8(2), 331–340.
- Krūma, K., & Statkus, S. (2019). The Constitution of Latvia – A bridge between traditions and modernity. In A. Albi & S. Bardutzky (Eds.), *National constitutions in European and global governance: Democracy, rights, the rule of law* (Vol. 2). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-273-6_20

- McCrudden, C. (2008). Human dignity and judicial interpretation of human rights. *European Journal of International Law*, 19(4), 655–724. <https://doi.org/10.1093/ejil/chn043>
- Milanovic, M. (2015). Human rights treaties and foreign surveillance: Privacy in the digital age. *Harvard International Law Journal*, 56(1), 81–146.
- Munir Ahmad Bhati v. Director FIA Cyber Crime Wing, Lahore, PLD 2022 Lahore 664.
- Naef, T. (2023). The global reach of the right to data protection. In *Data protection without data protectionism* (Vol. 28). Springer. https://doi.org/10.1007/978-3-031-19893-9_2
- Nikiforova, A. (2018). Open data quality evaluation: A comparative analysis of open data in Latvia. *Baltic Journal of Modern Computing*, 6(4), 363–386.
- Potaičuks, A. (2024). Data protection under review of Constitutional Court: Administrative databases directly accessible to public authorities. *TalTech Journal of European Studies*, 14(2), 73–87.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- Sarwar, L. G., Azhar, M. M., & Baig, M. S. R. (2024). The role of judicial activism in the enforcement of human rights in Pakistan and its impacts on governance in Pakistan. *Global Legal Studies Review*, IX(III), 1–14. [https://doi.org/10.31703/glsr.2024\(IX-III\).01](https://doi.org/10.31703/glsr.2024(IX-III).01)
- Shulztiner, D., & Carmi, G. E. (2014). Human dignity in national constitutions: Functions, promises and dangers. *The American Journal of Comparative Law*, 62(2), 461–490.
- Smith, M. L., & Mayer-Schönberger, V. (2009). Delete: The virtue of forgetting in the digital age. *IDIS*, 2, 369–373. <https://doi.org/10.1007/s12394-010-0039-x>
- Stainforth, E. (2021). Collective memory or the right to be forgotten? Cultures of digital memory and forgetting in the European Union. *Memory Studies*, 15(2), 257–270. <https://doi.org/10.1177/17506980211044707>
- Taylor, P. M. (2020). Article 17: Privacy, home, correspondence; honour and reputation. In *A commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's monitoring of ICCPR rights* (pp. 458–498). Cambridge University Press.
- The Monal Group of Companies v. Capital Development Authority, PLD 2024 SC 925.
- W.W. v. Germany, Apps. No. 60798/10 and 65599/10 (European Court of Human Rights, 2018).
- Youm, K. H., & Park, A. (2023). The right to be forgotten: Google Spain as a benchmark for free speech versus privacy? *Chicago Journal of International Law*, 24(1), 167–186. <https://chicagounbound.uchicago.edu/cjil/vol24/iss1/9>
- Yongmei, C., & Afzal, J. (2023). Impact of enactment of 'The Prevention of Electronic Crimes Act, 2016' as legal support in Pakistan. *Academy of Education and Social Sciences Review*, 3(2), 203–212. <https://doi.org/10.48112/aessr.v3i2.500>