Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2024)

Data Protection in Pakistan: Need for a Comprehensive Legal Framework

Naveed Hussain
Assistant Professor, School of Law, University of Gujrat
Email: naveed.hussain@uog.edu.pk

Rao Qasim Idrees
Associate Professor, School of Law, University of Gujrat Email: qasim.rao@uog.edu.pk

Yasir Arfat
Lecturer, School of Law, University of Gujrat Email: yasir.arfat@uog.edu.pk

ABSTRACT
Digital technologies, e-commerce, e-governance, biometric identification systems, and data-driven decision-making have grown exponentially and changed the process of collecting, processing, storing, and sharing personal data in Pakistan. There is a growing dependence on personal data by both the public authorities and the private companies in service delivery, security, financial transaction and oversight of these entities. Although this datafication of society occurs at a rate, Pakistan still does not have an extensive and enforceable legal framework of data protection, which would allow protecting the privacy of individuals, providing accountability, and controlling the data practices of the state and non-state actors. This article discusses why a general data protection regime is necessary in Pakistan by looking into the current rules of the law, practices of institutions and the risks that are coming on board in face of unregulated processing of data. It claims that the existing safeguards are piecemeal, industry-oriented, and mostly insufficient to tackle modern issues like mass data gathering, internet monitoring, intercontinental data flows and the abuse of private data. The lack of a comprehensive law on data protection undermines the constitutional privacy protection, negative impacts on the trust of people in digital systems, and puts individuals at a significant risk, such as identity theft, profiling, and unauthorized surveillance. Using the constitutional provisions and the global standards of data protection, this article will argue that Pakistan is in dire need of an overhaul data protection framework, clearly defining the rights, duties, enforcement, and control frameworks. It concludes that in the absence of such a framework, the digitalization of Pakistan can become a system of systemic privacy infringement and a threat to democratic governance in the digital era.

Keywords: Data Protection; Privacy; Personal Data; Digital Governance; Constitution Of Pakistan; Information Privacy; Surveillance; Data Regulation; International Data Protection Standards; Pakistan.

Introduction

The boom of the digital technology in Pakistan has essentially changed the manner in which personal information is produced, gathered, and used in both the government and non-government sectors. The biometric identification system and the database of digital identity has turned into the main resource of the governance, economic activity, and daily life; online banking, e-commerce platforms, mobile applications, and social media

ISSN Online: 3007-3154
ISSN Print: 3007-3146

services. Government programs to digitalize its services, enhance security and make the administration more efficient are becoming increasingly pegged on extreme data collection and amalgamation, and private sector actors are relying on personal data to develop targeted advertising, finance and consumer analytics. This ubiquitous data-driven nature has generated more opportunities than ever before in the field of innovation and service delivery, although, it has led to individuals being susceptible to privacy risks, abuse, and additional harm.[1]

However, as much as this has been based on extensive use of personal data, Pakistan lacks a unified and uniform data protection legal framework that can govern the current data practice. The current legal provisions safeguarding personal data are distributed in various parts of the Constitution, industry-specific legislations and regulations, most of which were created in a pre-digital era or had only a narrowly-focused regulatory need. Although the Constitution of Pakistan acknowledges the dignity of the individual and the sanctity of the privacy, the two have not been translated into specific laws and duties in processed data in any systematic manner. Consequently, the collection, storage, distribution and analysis of personal data in Pakistan tends to be carried out without any pronounced legal criteria concerning the consent, limitation of purpose, protection of information and responsibility.[2]

It is quite worrying as no comprehensive data protection laws are in place considering the magnitude and sensitivity of the data under processing. State authorities and third-party organizations are becoming bigger users of biometric information, financial data, metadata of communication and locational data and in most cases, there is little or no transparency and accountability in the handling of this information. Breach of data, unauthorized access, and misuse of personal data are dangerous not only to individual privacy but also to the interests of the wider society, such as the trust towards digital systems and democratic governance. The scarcity of data governance regulations in the public sector increases the surveillance, profiling, and creep of functions, in which data gathered under one purpose is reused without significant rationale or protections.[3]

The practice of data protection regimes shows that it is a key element of current digital governance, which can be seen in different countries. Countries worldwide have embraced legislations on extensive data protection, which stipulate the rights of individuals, govern the behavior of data controllers and data processors, create external control agencies, and offer redress in breaches. These frameworks are now also viewed as privacy protection mechanisms, as well as, enabling digital trust, transnational data flows, and economic integration. By contrast, the disjointed stance of Pakistan on its data control puts the country at a disadvantage, both to protect its citizens and to enable them to take part in the global digital economy.

The convergence of the data protection system with the constitutional rights and the international norms further motivates the necessity of the overall data protection system in Pakistan. Privacy is becoming an underlying right that lays the foundation of freedom of expression, association, and autonomy in digital age. In the absence of legislative means to bring this right to reality, constitutional guarantees are abstract and hard to implement. Furthermore, its international human rights obligations place the country

[1] Ali, M. I., & Hussain, K. A. (2024). Unveiling the tapestry: a comparative investigation into data-protection legislation in India and Pakistan. *Socrates Rīga Stradiņš Univ Fac Law Electron Sci J Law*, *1*, 1-8.

[2] Masudi, J. A., & Mustafa, N. (2023). Cyber security and data privacy law in Pakistan: Protecting information and privacy in the digital age. *Pakistan Journal of International Affairs*, *6*(3), 356-366.

[3] Noorani, G. M. (2025). DATA PROTECTION LAWS IN PAKISTAN: CHALLENGES AND OPPORTUNITIES. *Journal of Media Horizons*, *6*(1), 364-374.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

(Pakistan) with a duty to guard people against the unfair or unlawful encroachment on their privacy, which cannot be effectively achieved without explicitly and legally enforceable principles of data protection.[4]

This paper will be exploring the reasons why there should be overall data protection laws in Pakistan, first by discussing the legal frameworks that already defend this data, then finding vulnerabilities in the legislation, and finally evaluating the threats of the unchecked data usage behaviors. It aims at proving that data protection is not just a technical or administrative or rather a fundamental matter of constitutional governance and democratic responsibility. By placing the issue of data protection in Pakistan in comparative and international context, the article seeks to present the principles and structural factors that are required to have a successful legal framework. The subsequent sections examine the existing literature on the topic of data protection and privacy, the methodology that will be used in the research, the weaknesses of the existing legal system in Pakistan, and the directions of the development of a comprehensive data protection system that can be adapted to the digital future of the nation.

Literature Review

The existing literature on data protection and privacy in Pakistan demonstrates that more and more people are beginning to understand that the legal and institutional frameworks of the country did not keep up with the fast growth of data-driven technologies. The initial legal research on privacy in Pakistan was mainly centered on constitutional interpretation especially on Article 14 of the Constitution that guarantees the dignity of man and privacy of the home. The analyses highlighted privacy as an individual and spatial right, which was primarily related to physical intrusion and illegal searches. This body of literature is foundational in nature and much of it is older than the emergence of mass processing of digital data, and thus offers little in the way of guidance on modern day challenges in the form of informational privacy, data profiling, and automated decision-making.[5]

With the further penetration of digital technologies into governance and business, researchers started pointing out the weakness of the current legal safeguards concerning the information about individuals. Legal pundits noted that the statutory environment in Pakistan is composed of fragmented and industry-specific legislation that is dispersed throughout telecommunications legislation, banking regulations, cybercrime laws, and administrative regulations. This fragmentation, as the literature claims, leads to unequal protection and inconsistent standards, which leave large sectors of personal data largely unregulated. According to the researchers, the absence of a common framework on the definition of rights and obligations makes data protection discretionary and reactive, and not guided by legal norms.[6]

The connection between data protection and surveillance is also considered in a considerable amount of literature. According to scholars, without a thorough data protection laws, surveillance activities have little restrictions on the data retention, sharing and secondary use. This loophole facilitates the creep of functions, in which information gathered in good faith in either administration or protection is used other

[4] Jhokio, A., & Rehman, T. U. (2025). Data privacy laws in Pakistan: A comparative analysis with the EU's General Data Protection Regulation. *Journal of Political Stability Archive*, *3*(2), 870-882.

[5] Bint Sohrab, L., Shah, K., & Nawaz, B. (2024). BRIDGING THE GAP: CROSS-BORDER DATA FLOWS & DATA PROTECTION HARMONIZATION IN PAKISTAN. *JOURNAL OF SOCIAL SCIENCES DEVELOPMENT*, *3*(3), 232-247.

[6] Ahmad, J. B., Hussain, M. A., & Mir, H. A. (2024). Developing a Legal Framework for Digital Policy: A Roadmap for AI Regulations in Pakistan. *Law and Policy Review*, *3*(1), 162-188.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

functions without disclosure or agreement. The literature reiterates the fact that the data protection legislations are critical complements to the regulation of surveillance, since they offer life-cycle controls on personal data and establish accountability mechanisms that go beyond the time of data capture. In the absence of such controls, the constitutional privacy protection is compromised by the ubiquitous and obscurity practices of data.[7]

In Pakistan, comparative and international scholarship has been mostly central in influencing the debate on the reform on data protection. Often, in studies, researchers cite entire regimes, like the General Data Protection Regulation of the European Union, to show the main points of the current legislation on data protection, which are the legal justifications to process such data and personal rights, as well as the presence of independent data protection authorities and protection of cross-border data transfer. Although it is true that this model cannot be sold in supermarket, the scholars believe that the principles that support them, i.e. legality, transparency, limit their purpose, and accountability are universal. According to the literature, a deficiency in Pakistan to conform to the principles prevents cooperation between countries in the international data environment and undermines the confidence of consumers and investors in the country digital environment.[8]

Another literature that concerns the economic and governance impact of weak data protection is also present. Analysts believe that strong data protection systems have become pre-requisites into the global digital markets, cross border outsourcing and trade, and international trade in services. Lack of proper protection of data will be reputational risk to Pakistan and could restrict the integration opportunities with jurisdictions where they have adequate requirements of protection of data transfers. Regarding the aspect of governance, the scholars note that explicit data protection regulations contribute positively to confidence in online public services, minimise corruption and abuse, and promote evidence-based policymaking by guaranteeing data completeness and responsibility.[9]

There are also social impacts of unregulated data practices that are brought to the fore by civil society and literature that is policy oriented. Reports record issues of data breach, identity theft and profiling which is discriminatory especially against vulnerable groups. These harms are worsened by the absence of available remedies as well as independent checks since victims have very little resources to fight misuse or even demand redress. As highlighted in this literature, data protection is not just a technical compliance concern but also a social justice and democratic responsibility since the data practices will determine power relationships between state, corporations, and individuals.[10]

In general, the literature leads to the same conclusion that Pakistan is currently using an inappropriate method of data protection in the context of the digital era. Researchers always suggest that constitutionalization of privacy, though significant should be put into practice with a set of extensive legislation on defining of rights, data handling and development of effective supervision. The literature has a solid normative and comparative basis to evaluate the existing gaps in the legislation of Pakistan and to

[7] Halim, W., Upadhyay, A., & Coflan, C. (2022). Data Access and Protection Laws in Pakistan: A technical review.

[8] Ibid.

[9] Asghar, M. S., Saqib, K. M., Mukhtar, H., & Naz, H. (2022). AN ANALYSIS OF DATA PRIVACY AND PROTECTION LAWS IN PAKISTAN. *Russian Law Journal*, *10*(4), 142-147.

[10] Baig, K., Fazail, A., & Shahzadi, A. I. (2025). Protection of Digital Privacy under the Constitution: A Comparative Analysis of the EU, US and Pakistan. *Journal for Current Sign*, *3*(4), 1519-1536.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

explain why a logical framework of data protection is required. This literature shapes the methodological/analytical tool to be used in the following parts of this paper where the data protection situation in Pakistan is discussed in more detail and offers the ways in which such a situation can be improved.

Methodology

The present article is a qualitative, doctrinal, and comparative research study that aims at evaluating the necessity of an extensive data protection legal framework in Pakistan. The approach of methodology lies in the fact that data protection is essentially a legal and governance problem and not a technical one, demanding consideration of constitutional concepts, legislative architecture, institutional structure, and normative standards. In this respect, the paper integrates legal assessment with the governance-oriented assessment to discuss the current regulation of personal data in Pakistan, regulatory gaps, and the way in which the latter can be closed by means of coherent changes in legislation.

The initial part of the methodology is the doctrinal examination of the current legal context in Pakistan that pertains to data protection and privacy. This would involve review of Article 14 of the Constitution and statutory instruments such as telecommunications legislation, banking and financial legislation, cybercrime legislation, and administrative legislation that, though incidental to the subject matter of data handling and confidentiality, address the subject matter. The discussion is aimed at determining the extent and boundaries of these provisions, rights they grant to individuals and liability to data-handling entities. Of special interest is how these laws can express fundamental data protection standards like lawful processing, consent, data limit, minimization, security, and accountability, or protection is still implicit and scattered.

The second methodological aspect looks into institutions practices and governance regimes in the area of processing data in terms of public and non-government actors. This part of the research will rely on the secondary sources such as the official policy documents, regulatory guidelines, audit reports, and authoritative civil society examination to evaluate the extent to which personal data are collected, stored, shared, and used in practice. Instead of individual cases, the methodology aims at defining the general trends, including the growth of biometric databases, growing into dependence on the data-driven decision-making, and a lack of transparency concerning the practices of data-sharing. This governance based analysis is critical to comprehending that legal loopholes are converted to practical privacy dangers and lack of accountability.

Based on my agreed enhancement framework used in this series of articles, the methodology will include the use of analytical instruments, which are structured to enhance clarity and rigor. The data protection landscape in Pakistan is placed in relation to the international standards and best practices in relation to comparative tables and conceptual figures. As an illustration, Table 1 can be subsequently presented to contrast the principle components of an all-encompassing data protection regimes, including individual rights, legal grounds of processing, and supervision systems, with the currently scattered ones in Pakistan. In a similar manner, Figure 1 can conceptually demonstrate the data lifecycle, pointing out areas where legal protection is either lacking or insufficient. These instruments help systematically evaluate loopholes and priorities of reforms.

At the third part of the methodology, a comparative approach and an international law approach are taken. It entails the analysis of generally established principles of data protection embodied in international instruments and comparative laws, which are not

ISSN Online: 3007-3154
ISSN Print: 3007-3146

intended to be directly applied in transplantation, but to create the normational standards. The analysis takes into account the ways in which these principles have been modified in various juridical and socio-economic settings and how they can be applied in the case of Pakistan. This comparative prism assists in finding the minimum standards required to safeguard privacy and to enable global information transfers, whilst making room to make context-specific design decisions.

Lastly, the framework of evaluation that was used in this research determines the sufficiency of data security as being legally understandable, enforceable, independent of institutions, and even able to safeguard the rights of individuals. The notion of a comprehensive data protection framework, in this context of analysis, is the form which grants individuals clear rights, places binding duties on data processors and controllers, creates an independent oversight body, and provides remedies that are readily available in case of infractions. Using these criteria, the methodology allows critically evaluating the current situation in the field of data protection in Pakistan and justifying the identification of specific legal and institutional changes. The conclusions that are produced by the means of this practice are the foundation of the next part that evaluates the flaws of the current data protection mechanisms of Pakistan and what they mean in terms of privacy, power, and digital trust.

Research Findings

According to the research results, the existing data protection strategy used in Pakistan is disjointed, reactive, and not structurally able to tackle the magnitude and complexity of the modern-day data processing habits. Among the most important conclusions, it should be mentioned the lack of any one, large-scale law, which could define the personal data, govern its processing, and create the rights and obligations to be enforced. Rather, the data protection in Pakistan is spread over constitutional principles, sector-specific confidentiality rules, and incidental mentions in the laws (telecommunications, banking, and cybercrime). This disjointed legal environment leads to inconsistency, absence of regulations, and unpredictability of individuals and organizations, as personal data is prone to misuse and abuse.[11]

One of the major discoveries is how constitutional privacy guarantees are scarcely operationalized. Although Article 14 of the Constitution is aware of the dignity of the individual and inviolability of privacy, these provisions are not reflected in concrete statutory rights concerning the processing of data, including the right to know, the right to authorize, the right to access, and the right to amend personal data. In a sense, the citizenry is not very aware of the way their information is gathered and utilized and there are even fewer means of objecting to illegal processing or redressing. This disjunction in constitutional acknowledgment and statutory application makes privacy as a fundamental right in the digital setting weakly enforceable in practice.[12]

It also shows that there are great risks involved in the practices of data in the public sector. Government agencies are increasingly placing trust in mass data gathering as well as biometric databases, digital identity systems, and integrated information platforms, and typically they lack any explicit legal obligations of data sharing, information retention or secondary utilization. The absence of uniform data governance policies

[11] Aftab, S. (2024). Recommendations: A privacy law for Pakistan. In *Comparative perspectives on the right to privacy: Pakistani and European experiences* (pp. 257-291). Cham: Springer Nature Switzerland.

[12] Yaseen, M. (2024). Cross-Border Data Flows in Pakistan: Legal Challenges and Technological Solutions for Digital Trade. *Journal of Engineering, Science and Technological Trends*, *1*(1).

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2024)

allows the occurrence of a phenomenon of function creep in which data intended to serve a particular administrative purpose is re-used by others without visibility or agreement. This poses major issues relating to surveillance, profiling and discriminating decision making especially where there are no independent check and balances or proper accountability.[13]

Table 1: Core Data Protection Elements and Pakistan's Legal Framework

Core Element	Comprehensive Framework	Pakistan's Current Position
Definition of personal data	Clearly defined	Absent or inconsistent
Lawful bases for processing	Explicit and limited	Largely undefined
Individual data rights	Clearly articulated	Minimal or implicit
Independent oversight authority	Established	Absent
Remedies and penalties	Clear and enforceable	Fragmented and weak

The other significant discovery is associated with the data practices in the private sector. E-commerce websites, banks, mobile network operators, and technology firms are actively gathering and processing huge amounts of personal information on a regular basis, in many cases with consent systems that are unnegotiable or non-transparent. Without mandatory data protection requirements, businesses do not have many legal reasons to enforce strong data protection or reduce data gathering. Hacker intrusions and informal dissemination of information are thus recurring threats, and little transparency or responsibility is shown to take place in the event of damage. Victims of such cases have limited viable solutions, in that, the current legislation lacks avenues through which they can be compensated or regulations enforced against perpetrators.[14]

Another area of concern that is found in the findings is the cross-border data flows. The absence of a detailed data protection regime by Pakistan makes international data transfer complex, especially when using jurisdictions that base their protection on the requirement of adequate protection standards. Not only does this exposes personal data to lesser protection when sent to other countries, but it also restricts Pakistan to be involved in the global digital markets and outsourcing systems in their full scope. The results indicate that poor data protection does not just raise an issue of rights, but is an economic and strategic drawback as well.[15]

Lastly, the lack of institutional oversight is an important weakness of the findings. Pakistan lacks a dedicated data protection body or authority charged with the role of overseeing the adherence to the same, investigating any breach, and sensitizing stakeholders. Regulation of data practices is rather decentralized among sectoral regulators with little concern on privacy or data protection. This lack of accountability in institutions helps decrease citizens trust in digital systems, as there is no specific

[13] Amin, M. H., & Hassan, M. (2024). Digital privacy in Pakistan: Ending the era of self-regulation. *LUMS LJ*, *10*, 22.

[14] Butt, M. F., Saleem, H. A. R., Hashmi, M. A. I., & Bano, N. (2024). THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN. *ASSAJ*, *2*(4), 1449-1458.

[15] Mushtaq, A. A. (2025). Data Protection Challenges in Pakistan: Lessons from the EU GDPR. *Available at SSRN 5799442*.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2024)

institution which would hold innovation, governance and individual rights in balance.[16] Combined with the fact that no individual country worldwide has the legal and institutional framework to guarantee the protection of personal data in a data society, these findings indicate that the current legal and institutional provisions that exist in Pakistan are not adequate in ensuring the protection of personal data in a data society. Absence of a overarching law, rights that are enforceable, explicit duties, and independent controls causes structural weaknesses that impact individuals, organizations, and the overall digital ecosystem. These results form the analytical background within the further discussion, involving the interaction of these structural gaps with the principles of the constitution, governance, and international standards to support the severity of the necessity of an all-encompassing data protection framework in Pakistan.

Discussion

Results of this research show that the challenges of data protection in Pakistan are not caused by a single failure of the legislative system but are indicative of structural lack of correlation between the fast digitalization and the slow change in legislation and governance. It can be seen in the discussion that the protection of data in Pakistan is still a conceptually immature issue that is considered a peripheral factor instead of a fundamental part of constitutional governance and internet policy. Although personal data has taken center-stage to the administration of states, security operations, and business operations, the legal system remains unable to adjust to control data as a source of power that needs to be clearly limited, accountable and has rights-based protections. This asymmetry enables the growth of data-driven practices with the least legal resistance and legitimizes intrusion and undermines individual autonomy.[17]

One of the key aspects that arise out of the discussion is the discrepancy between constitutionalization of privacy and its being applied in statutory law. Article 14 of the Constitution offers a valuable normative point of reference, because privacy and dignity have been put at the center of the document, still, that is only an abstract definition of how such personal data might be collected, processed, and shared without the detailed legislation. On an online platform, the privacy breach is usually achieved not by an explicit intrusion, but by ordinary types of data practices that are not evident to the individuals. In the absence of the statutory articulation of the informational privacy and the enforceable data rights, the constitutional guarantees are hard to invoke and more so, to enforce. This detachment makes privacy an empty ideology and not a viable protection.

The risks of governance of uncontrolled practices of public sector data are also brought to the fore in the discussion. The growth of biometric systems, central databases, and data-sharing agreements between government agencies has taken place to a large degree without clear legally prescribed models or external regulation. This preconditions the situation of the creep of functions, surveillance, and discriminatory profiling especially when the data is reutilized beyond its original rationale. Constitutionally, these practices weaken the concept of limited government since it allows constant surveillance and profiling of people without any noticeable responsibility. This lack of a full-fledged data

[16] Ullah, S. (2025). The Right to Privacy under the Constitution of Pakistan. *The Right To Privacy Under The Constitution of Pakistan*.

[17] Mushtaque, K., Ahsan, K., Nadeem, A., & Umer, A. (2014). Critical Analysis for Data Privacy Protection in Context of Cyber Laws in Pakistan. *Journal of Basic and Applied Scientific Research*, *4*(10), 1-4.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

protection system implies that these risks are resolved, at best, by informal administrative actions, but not by legally binding norms.

The scope of data protection is also complicated by the data practices of private sector. The discussion highlights that a market incentive is not enough in the absence of legal binding forces to provide responsible data handling. Mechanisms of consent tend to be formalistic, opaque, or enclosed within take-it-or-leave-it terms of service, and provide users with only limited real choices. Unless there are legal minimum of data requirements in the form of data minimization, data security, and accountability, the companies might obtain the data and sell it to the highest bidder, without considering the rights of the individual. Such data imbalance between data subjects and data controllers underpins social and economic injustice and distrust of the digital services.

The urgency of reform is supported by international and comparative points of view. The discussion highlights that data protection has become one of the main conditions of being involved in the global digital economy, as well as cross-border data flows. This is the situation in jurisdictions that do not have sufficient protection structures, which are becoming obstacles to data exchange, outsourcing, and digital trade. The disunited nature of the approach used by Pakistan not only undermines the protection of rights, but also makes this country strategically disadvantaged, which restricts the possibility of economic integration and innovation. In the global law perspective, poor data protection also compromises on the capability of Pakistan to address its human rights concerns concerning privacy and personal information.[18]

In general, the discussion highlights the fact that data protection is a governance necessity and not a technical luxury. On the one hand, a lack of a legal framework facilitates the systematic privacy threat, transfers the information authority to unaccountable institutions, and undermines the democratic control. To resolve such issues, there is a need to change the legal and policy mindsets towards viewing personal data as a constitutional concern, economic and social consideration. This preconditions the further recommendations in the direction of the creation of a coherent and rights-respecting system of data protection in Pakistan.

Recommendations

An overall data protection infrastructure in Pakistan must start by the introduction of specific law on data protection which will explicitly state what personal data, sensitive data, and what forms of processing data are regulated. This legislation must express lawful grounds of data processing, consent, legal obligation, and public interest and at the same time such grounds are limited and liable to protection. It would help to bring a sense of legal predictability to both individuals and institutions and decrease the dependency on discretional or ad hoc data practices, which would be defined by clear statutory terms.

The second important suggestion is the identification and legalisation of the rights to individual data protection. They should consist of the right to know the information about the collection and usage of these data, the right to access and rectify personal data, the right to refuse unlawful processing, and the right to claim redress and compensate the damage. Incorporating these rights into the law would make constitutional privacy entitlement concrete and provide people with the meaningful power to control their personal data. Sensitive data like biometrics, health information and financial records

[18] Asif, M., Javed, Y., & Hussain, M. (2021, December). Automated analysis of Pakistani websites' compliance with GDPR and Pakistan data protection act. In *2021 International Conference on Frontiers of Information Technology (FIT)* (pp. 234-239). IEEE.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

should be provided with special protection owing to the probability of abuse.

The effective control and enforcement can only be achieved by creating an independent data protection authority. This organ must be required to oversee adherence, probe complaints, give guidance and punish breaches. The system should also not be dependent on the executive power as this would lack credibility and the trust of the population, especially when it comes to state agencies. The resources, technical skills, and enforcement capabilities would be sufficient to empower the authority to be a key image of data management and responsibility.

There is a need to pay specific attention to the practices of the public sector data. The legislation must bring evident responsibilities on government agencies in terms of data minimization, restriction of purpose, existence of data and protection. The legal authorization of data-sharing between agencies must be transparent and controlled. Routine audits and impact analyses of large-scale or high-risk data processing projects would assist in the prevention of the function creep and adherence to the constitutional principles.

A sensible regulatory framework that leads to a balance between innovation and the rights protection should be extended to the private sector as well. Data security, data breach notification and accountability obligations must be uniform and must have flexibility to meet various organizational capabilities. Strict policies to regulate the use of cross-border data transfer would enhance international collaboration and the protection of personal data would be ensured when used overseas.

Lastly, data protection reform must be supported by the public awareness, institutional capacity building and stakeholder participation. The principle and responsibility of data protection need to be taught to citizens, businesses, and public officials in order to achieve success in their application. Consultation with civil society, industry and technical specialists in an inclusive manner would assist in ensuring that the framework is rights-respecting and contextually appropriate. All of these recommendations offer a way to create a comprehensive data protection regime that will facilitate privacy, trust, and sustainable digital development in Pakistan.

Conclusion

This paper has discussed why a holistic legal framework should be enacted in Pakistan regarding data protection given the fast rate at which the country is undergoing digital transformation and increasing dependency on personal information. The discussion shows that the current legal regulations are disjointed, insufficient, and ill-equipped to deal with modern data practices of extensive data collection, processing and information sharing of personal data. Although constitutional acknowledgment of privacy provides a significant normative baseline, it has not been restated into enforceable statutory rights or institutional protections, which can help people in a society of data to be safeguarded.

The overall finding of this paper is that the lack of data protection in Pakistan is systematic and institutional. Lack of deeper legislations and independent monitoring of this process, as well as the explicit form of accountability, leaves people vulnerable to severe privacy threats and creates distrust toward online governing. Not only do these weaknesses have an impact on the individual rights, but also on the overall results of governance, such as transparency, democratic accountability, or economic competitiveness. Unless reformed, data-driven practices are likely to enshrine surveillance, inequality, and informational power abuse.

The article also notes that data protection is not a hindrance to the digital development but a compulsory aspect to its sustainability and legitimacy. Well-developed legal

ISSN Online: 3007-3154
ISSN Print: 3007-3146

systems that establish rights and duties allow the process of innovation to occur as it creates a trustworthy environment, supports cooperation among countries, and promotes responsible information handling. As it has been evidenced on the international experience, effective data protection regimes enhance the protection of rights as well as economic integration.

To sum up, a holistic data protection system is no longer an option to Pakistan instead of a mandatory requirement of its constitutional, governance, and developmental imperatives. Pakistan can also balance its digital future with constitutional principles and international norms by implementing transparent laws, building independent control, and instilling principles of data protection in both the public and the private sector. This kind of reform would mark a very decisive move towards individual autonomy protection, advancement of democratic governance, and the realization of the benefits of the digital transformation without undermining the core rights.

References:

Aftab, S. (2024). Recommendations: A privacy law for Pakistan. In Comparative perspectives on the right to privacy: Pakistani and European experiences (pp. 257-291). Cham: Springer Nature Switzerland.

Aftab, S. (2024). Right to Privacy and Freedom of Expression in the Constitution of Pakistan. In Comparative perspectives on the right to privacy: Pakistani and European experiences (pp. 99-126). Cham: Springer Nature Switzerland.

Afzal, J. (2025). Comparative Review on Acceptance of Digital Evidence within the Legal Frameworks of Pakistan and China. International Journal of Law and Legal Advancement, 1(1).

Ahmad, I., Bakhsh, F., Faisal, M., & Sultan, S. (2024). Regulatory Framework for Artificial Intelligence in the Legal System of Pakistan. The Critical Review of Social Sciences Studies, 2(2), 1068-1076.

Ahmad, J. B., Hussain, M. A., & Mir, H. A. (2024). Developing a Legal Framework for Digital Policy: A Roadmap for AI Regulations in Pakistan. Law and Policy Review, 3(1), 162-188.

Ali, M. I., & Hussain, K. A. (2024). Unveiling the tapestry: a comparative investigation into data-protection legislation in India and Pakistan. Socrates Rīga Stradiņš Univ Fac Law Electron Sci J Law, 1, 1-8.

Amin, M. H., & Hassan, M. (2024). Digital privacy in Pakistan: Ending the era of self-regulation. LUMS LJ, 10, 22.

Asghar, M. S., Saqib, K. M., Mukhtar, H., & Naz, H. (2022). AN ANALYSIS OF DATA PRIVACY AND PROTECTION LAWS IN PAKISTAN. Russian Law Journal, 10(4), 142-147.

Ashraf, M. (2025). Legal Framework of Artifical Intelligence in Pakistan and Its Regularisation: A Comperative Anaylsis and Its Development with Cognitive Suggestions: https://doi. org/10.5281/zenodo. 17494761. ASSAJ, 4(01), 4562-4595.

Asif, M., Javed, Y., & Hussain, M. (2021, December). Automated analysis of Pakistani websites' compliance with GDPR and Pakistan data protection act. In 2021 International Conference on Frontiers of Information Technology (FIT) (pp. 234-239). IEEE.

Baig, K., Fazail, A., & Shahzadi, A. I. (2025). Protection of Digital Privacy under the Constitution: A Comparative Analysis of the EU, US and Pakistan. Journal for Current Sign, 3(4), 1519-1536.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2024)

Bint Sohrab, L., Shah, K., & Nawaz, B. (2024). BRIDGING THE GAP: CROSS-BORDER DATA FLOWS & DATA PROTECTION HARMONIZATION IN PAKISTAN. JOURNAL OF SOCIAL SCIENCES DEVELOPMENT, 3(3), 232-247.

Butt, M. F., Saleem, H. A. R., Hashmi, M. A. I., & Bano, N. (2024). THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN. ASSAJ, 2(4), 1449-1458.

Halim, W., Upadhyay, A., & Coflan, C. (2022). Data Access and Protection Laws in Pakistan: A technical review.

Jhokio, A., & Rehman, T. U. (2025). Data privacy laws in Pakistan: A comparative analysis with the EU's General Data Protection Regulation. Journal of Political Stability Archive, 3(2), 870-882.

Masudi, J. A., & Mustafa, N. (2023). Cyber security and data privacy law in Pakistan: Protecting information and privacy in the digital age. Pakistan Journal of International Affairs, 6(3), 356-366.

Mushtaq, A. A. (2025). Data Protection Challenges in Pakistan: Lessons from the EU GDPR. Available at SSRN 5799442.

Mushtaque, K., Ahsan, K., Nadeem, A., & Umer, A. (2014). Critical Analysis for Data Privacy Protection in Context of Cyber Laws in Pakistan. Journal of Basic and Applied Scientific Research, 4(10), 1-4.

Noorani, G. M. (2025). DATA PROTECTION LAWS IN PAKISTAN: CHALLENGES AND OPPORTUNITIES. Journal of Media Horizons, 6(1), 364-374.

Ullah, S. (2025). The Right to Privacy under the Constitution of Pakistan. The Right To Privacy Under The Constitution of Pakistan.

Watto, O. M., Islam, M., Hussain, S. A., & Shahab, M. (2024). Cyber law and cyber security policies in pakistan: a comparative study with USA, canada and australia. Pakistan J Humanit Soc Sci, 12(1), 271-277.

Yaseen, M. (2024). Cross-Border Data Flows in Pakistan: Legal Challenges and Technological Solutions for Digital Trade. Journal of Engineering, Science and Technological Trends, 1(1).

Zeb, M. A., & Rahim, W. (2025). Cybersecurity in Pakistan: Legal Gaps, Institutional Challenges, and the Need for a Comprehensive National Strategy. Research Consortium Archive, 3(4), 1454-1465.