

GDPR Standards and Pakistan's Digital Economy: Analysing the Gap Between Compliance Requirements and Enforcement Capacity

*Hassan Iqbal**

Abstract

The digital economy of Pakistan is facing a major issue in aligning with General Data Protection Regulation requirements, and the gaps in compliance requirements and enforcement capabilities are critical in this case. Such issues as the lack of proper legislation to protect data, insufficient equipment, lack of regulatory control, and ignorance among companies about international data protection standards are amongst the main challenges. The lack of an extensive data protection system in line with the GDPR poses obstacles to business operations in Pakistan that want to transact with the European Union markets. Also, limited resources of regulatory agencies, inadequate enforcement mechanisms, and a lack of understanding of data privacy law only worsen such issues. Small and medium businesses are the ones that are more impacted by the difference between compliance capacities, as they are not in a position to comply with the GDPR requirements financially and technically. Although Pakistan is taking the right steps in data protection by passing the Personal Data Protection Bill, there is still a significant gap in the realisation of the law, the ability to implement it, and the compatibility with international standards, which is an essential issue for the competitiveness of the digital economy and the protection of citizen data in the country.

Keywords: Data Protection Compliance, Digital Economy Pakistan, Enforcement Mechanisms, GDPR Alignment, Regulatory Framework Gaps

Introduction

The consideration of data protection standards has become one of the foundations of the digital governance system, given that it governs how personal data is collected, processed, and secured in a world economy that is becoming more interconnected (Bentotahewa et al., 2022). The digital economy of Pakistan is rapidly expanding, as e-commerce, fintech, and other digital services sectors are growing, and they need effective data protection models (Shami et al., 2025). Nevertheless, there are still major issues related to harmonising the domestic laws with the international ones, including the General Data Protection Regulation (GDPR) of the European Union, which has become the universal standard of data protection (Ali & Ahmad Hussain, 2024).

The disparity between the requirements and the enforcement level of compliance is one of the issues that is a dire concern to the digital economy of Pakistan. As the country has tried to come up with data protection laws, factors like the lack of institutional capacity, minimal technical infrastructure, and lack of legal frameworks are major problems that prevent its successful implementation (Jhokio et al., 2025). Such issues are further exacerbated by weak enforcement frameworks, the absence of regulatory expertise, and limited awareness of the population regarding data privacy rights (Nabeel & Iqbal, 2025). Lack of holistic laws on data protection poses a hindrance to cross-border data flows and digital trade, which may restrict the incorporation of Pakistan into the world digital economy (Sohrab et al., 2024).

Deficiency in the enforcement capacity should be considered among the most pressing issues in the regulatory bodies in Pakistan. Although Pakistan has acknowledged the significance of data protection, there are no specialised regulatory bodies that could oversee adherence to the regulations because they do not have sufficient resources and technical expertise to handle them (B. Saleem et al., 2024). This will provide a platform in which data breaches and privacy breaches are possible with little accountability, which will reduce consumer trust in online services (Asif et al., 2025). The actual implementation of data protection in Pakistan

does not meet the international standards in many aspects (Rauf et al., 2025).

Pakistan is developing at a fast pace, and the involvement of international businesses is on the rise. Since the IT exports of Pakistan exceed 3.2 billion annually and the e-commerce market is growing exponentially, the observation of international data protection policies has become an important issue for the economy, among matters of competitiveness. Absence of efficient data protection systems would present immense barriers to Pakistani businesses that aspire to join the EU markets, where GDPR is mandatory.

Moreover, the technological peculiarities of Pakistan, the level of mobile penetration is high, the sphere of fintech is evolving, and the number of digital payment systems is growing, which argues that holistic systems of data protection are needed. The hinged comparison between the demands of GDPR and the currently available regulatory ability in Pakistan can lead to a preview of the realities of the process of accommodating internationally relevant demands in a developing economy.

The biggest hurdle for Pakistan is to manage the demands of data protection and adapt to the swift transition towards a digital health environment, where few regulations exist, and the legal landscape is developing (Mehmood, 2025). The literature review will include a brief description of the challenges of cross-border data transfers, flaws in organisations and challenges of compliance with the GDPR in the Pakistani Digital economy.

The literature reveals that a key gap in Pakistan's digital economy lies in the disparity between Pakistan's existing legal framework and the standards established under the GDPR. The existing data protection law in Pakistan does not include the principles of data subjects' rights, consent, and accountability (A. B. Haque et al., 2021). Lack of legal clarity on the identity of the data controllers and processors, and the requirements as to public awareness regarding data breaches, creates great challenges to businesses operating in Pakistan (Mangi et al., 2025). Citizens are neither aware of the right to privacy nor of the collection, processing

and transfer of personal data, which is another problem in the enforcement of citizens' rights (Malik et al., 2025).

This also relates to the institutionalisation of the norms. A review of the regulatory framework in Pakistan shows that the data protection principles are mentioned in various places; however, there is no authority that has the capacity and skills to enforce such laws (Mushtaq et al., 2024). The lack of special bodies, technical facilities and human resources is one of the more dangerous issues that the effective enforcement faces (Faisal et al., 2024). This has led to some doubts around the monitoring and implementation of compliance with international requirements for safeguarding information, including cross-national flows in information, which are essential in digital trade (Kaya & Shahid, 2025; Yaseen, 2024).

The recent changes in Pakistan, including the draft Personal Data Protection Bill and the establishment of the Personal Data Protection Office, provide the basis for this research. This research attempts to identify the gaps between the demands of GDPR compliance and the enforcement potential in Pakistan in terms of its regulatory and technical requirements. It will contribute to the understanding of how the data protection reforms can be considered as a part of the digital economy strategy in Pakistan that will stimulate consumer confidence, business competitiveness, and adherence to international standards, without disregarding the local economic realities and institutional capacity.

Research Methodology

This research is conducted using a systematic review technique. The rationale behind this method is the establishment of the research goals (Kraus et al., 2022; Paul et al., 2021; Snyder, 2019) and the comprehensive literature review of the issue (Booth et al., 2016; Komba & Lwoga, 2020). By using this method, the study's outcomes are classified by topic content (Hiver et al., 2024; Paré et al., 2015; Petticrew & Roberts, 2006). The information presented in the study is organised into headings (Howell, 2013; Pawson et al., 2005; Xiao & Watson, 2019). The analysis of the information so classified and titled produces a flow of the study (Page et al., 2021; Rahi, 2017). In this respect, the integrity of the

study is preserved by situating the research subject within its appropriate context. (Egger et al., 2022; Victor, 2008). Therefore, the relevant approach was selected, and the corresponding processes were observed. The relevant literature was interpreted to facilitate the synthesis and coding of information and data in accordance with the study's objectives. The coded data were analysed by grouping them into categories. This involved classifying and consolidating the data before organising it according to the level of association. The criteria of selection are listed.

Relevance: The research which directly related to the questions of this study is included.

Quality: The study included a specific quality of research data. The articles are mostly published in indexed and credible Scopus-based and Clarivate Analytics journals.

Recency: This is the aspect that takes into account the date of a review, so that the information that is contained in the review is up to date. The larger portion of the research is published within the last three years.

Sufficiency of Information: The past research should have had adequate information about the findings of interest to extrapolate the information into practical use in the research; this is what will happen in the present research as well.

Emerging Legal Framework of GDPR and its Enforcement in Pakistan

Concerns relating to data protection are relatively recent in Pakistan. However, the issues of privacy are not entirely unknown to the system. In the absence of a comprehensive framework on data protection and digital privacy, Pakistan primarily relied on the traditional criminal law system. Since these laws were not designed to address the issues relating to data processing, digital privacy and cybersecurity, this results in regulatory gaps in the country's digital framework (Afzal, 2024).

Prevention of Electronic Crimes Act (PECA) 2016 was introduced as the first step towards Cyber Legislation, as it dealt with a far larger number of cases of cybercrime as compared to general data protection. The prime intent of Pakistan to take control of the digital space was its first attempt to do so, but it was not the country's plan to protect its part in the digital space regarding privacy rights; it rather had an agenda of criminalisation (H. A. R. Saleem et al., 2025). The efforts to come up with more extensive frameworks (E. U. Haque et al., 2023) are being made due to the digitisation of the Pakistani economy and the growing demand for data protection by most countries.

So far, Pakistan has not been successful in achieving the protection of data. In the absence of a comprehensive legal framework, data lacks adequate protection regarding ownership, control, and associated rights, creating significant challenges for both businesses and citizens (Isazade et al., 2025). The principles of GDPR have also been incorporated into the recent draft data protection laws, but once enacted, the laws will face implementation challenges due to deficient institutional capacity and political instability (Yaseen & Phattanasin, 2025).

To understand and resolve these challenges, required to examine the theoretical foundations of GDPR through which Pakistan's GDPR framework can be assessed. The theoretical background of GDPR standards has strong roots in the premises about privacy, data protection, and the freedom of a person that were formed in European legislation (Bentotahewa et al., 2022). Theoretical frameworks which are taken to be the core of data protection are privacy as a right of a human being, informational self-determination, and the principle of minimum data. The main theme of GDPR is that individuals have a right to manage their personal information and rights, such as access, correction, deletion, and data portability (A. B. Haque et al., 2021).

The regulations are formulated based on seven principles, namely: lawfulness, fairness and transparency; limitation on purpose; limitation on data; accuracy; storage limitation; integrity, confidentiality, and accountability. These principles stipulate that the data controllers shall process personal data in a way that

complies with the law, the purpose for which they were collected, and appropriate security measures (Yaseen, 2024). The principle of accountability encourages organisations to demonstrate compliance through meeting the requirements of documentation, data protection impact assessment, and data protection officers (A. B. Haque et al., 2021).

The concepts of privacy by design and privacy by default are also included in the theoretical basis, as the protection of the data should be ensured by the organisations in the creation of their systems in the first place. The risk-based approach acknowledges that the degree of risk assumed when conducting data processing activities will not be equal and, therefore, will need equal protection (Bentotahewa et al., 2022). Such speculative opinions guide the enforcement mechanisms, including imposing heavy fines and mandatory notice of breach. Lastly, the theoretical base of GDPR introduces the required balance between the right to innovation and the right to individual privacy, and data protection is considered to be one of the primary rights and the regulatory adherence (A. B. Haque et al., 2021).

These principles provide a benchmark from which Pakistan's existing legal instruments can be evaluated. The legal framework of data protection in Pakistan continues to develop, and different regulations are currently being debated to address the problem of digital privacy and data security, yet none of the wide-ranging laws comparable to the GDPR has been adopted (Jhokio et al., 2025). The dignity of an individual, as well as the privacy of the home, is guaranteed under Article 14 of the Constitution of Pakistan, which provides a constitutional foundation for the right to data protection, though it does not explicitly mention digital data. The Electronic Transactions Ordinance, 2002, is transforming electronically signed and electronically recorded documents, which are creating the electronic business and information protection provisions for the service providers (Rauf et al., 2025).

The Personal Data Protection Bill is proposed legislation which stipulates complicated data protection provisions similar to GDPR (Jhokio et al., 2025). It offers the norms of data processing according to the legislation and the rights of individuals. The law

proposes the Personal Data Protection Office as the regulatory body. Moreover, the Prevention of Electronic Crimes Act, 2016, is concerned with cybercrimes, unauthorised access to information systems, and electronic fraud. Though the details of criminal cases receive precedence, it comprises provisions on unauthorised data leak and privacy invasion (H. A. R. Saleem et al., 2025). Similarly, the Telegraph Act of 1885 and the Pakistan Telecommunication (Re-organisation) Act of 1996 regulate telecommunication and provide a provision on confidentiality of subscriber information and legal interception.

Barriers to GDPR Alignment and its Enforcement in Pakistan's Digital Economy

There is an insufficient adequacy determination by the EU Commission in the EU jurisdiction for Pakistani companies to transfer data, and the standard contractual terms, due to the complexities and high compliance costs, are required for businesses involved in international operations.

Another challenge is that the Gaps in Awareness and Training of the requirements of the GDPR and best practices in the data protection field are not universal among businesses, and because of this, it is hard to secure data. It is hard to implement data protection officers or employees who have training on international privacy standards, since there are only a few organisations with such training.

Similarly, the Lack of technical infrastructure is another concern. The majority of Pakistani firms, and particularly the SMEs (small and medium enterprises), lack the technical infrastructure to meet the requirements of the GDPR, including data encryption services, secure data storage services, and data breach detection services. This poses a problem for privacy.

Moreover, Pakistan lacks a similar legislative data protection framework to the GDPR, and the absence of a law leaves businesses under the uncertainty of what rules they should comply with to meet international standards, and citizens without the protection of their privacy.

Another major challenge is the lack of resources, technical skills, and qualified staff members to apply the data protection standards to the regulatory authorities. The Office of Personal Data Protection has not been operationalised, and there is no particular organ that oversees such issues.

Pathway to GDPR Compliance in Pakistan's Digital Economy

The Personal Data Protection Bill under consideration provides the opportunity to establish a comprehensive system of data protection based on the principles of the GDPR. The enactment of effective legislation would empower Pakistan in the international digital economy and facilitate the flow of data across borders.

Local capacity may be built regarding data protection through investment in training regulators, lawyers, and businesses. Technical assistance and knowledge transfer may also be sought from international bodies and EU institutions.

Moreover, the growing IT industry and state-level digitalisation, including the Digital Pakistan policy, show an opportunity in Pakistan to use privacy-enhancing designs and information security as the new models are being developed.

Similarly, Pakistani IT firms may be a dependable partner to European firms in the export of IT, as well as their direct foreign investment, through their capability to adhere to GDPR. The certification schemes and compliance schemes can be used to differentiate Pakistani firms in the global markets.

Public-Private Cooperation can also prove to be a significant step. The consensus on the data protection standard can be established by creating multi-stakeholder forums between the government, the industry associations, the civil societies, and the technology companies to establish collaborative enforcement mechanisms to support the international standards and the local situation.

Discussion

A significant disparity exists between the requirements of the GDPR and Pakistan's capacity to meet them, highlighting the broader challenges faced by developing economies in adapting to international data protection frameworks. Regulatory uncertainty exists because no legislation exists, in particular, the pending Personal Data Protection Bill, and this has had a disproportionate impact on SMEs, who have no resources to fund compliance infrastructure. This institutional loophole is further enhanced by the lack of technical capacity in the proposed regulatory agencies, like the Personal Data Protection Office, which is not functioning according to the legislative will.

Compliance gaps not only concern legal frameworks but also structural issues, including insufficient cybersecurity infrastructure, privacy unawareness among businesses and citizens, and the absence of mechanisms for cross-border data transfer. The successful GDPR alignment process requires implementation strategies that emphasise phasing, massive investments in capacity building, and government-business partnerships. The instance of Pakistan will be a good example of how the drive of global standardisation may lead to a clash with the reality of local institutions, and that the solutions that are country-specific rather than wholesale regulatory transplantation are required. The following recommendations are made:

- It is recommended that industry-specific compliance be developed in banking, medical, e-commerce, and telecommunications, with regard to industry-specific issues of data processing.
- Dissemination of awareness about data ownership and corporate duty for creating a privacy mindset culture in the digital ecosystem in general is also an important requirement.
- Explore leveraging EU data protection authorities and global privacy lobby groups to exchange information, offer technical guidance, and do capacity building.

- Introduce voluntary certification schemes, with the assistance of which companies will be able to demonstrate that they implement the GDPR-compliant practices that will make them competitive in the market, and their consumers will trust businesses that use their information.
- Invest in national cybersecurity infrastructure, including, but not limited to, data breach response and capabilities, secure cloud services, and encryption technologies of any size. It is imperative to make sure that the Personal Data Protection Instructions follow the Personal Data Protection Bill that is heavily geared towards the GDPR requirements, along with all the provisions that discuss in detail the subject data rights, the controller's responsibilities, and the provision of liability.
- Mainstream training on data protection officers and privacy specialists must be introduced. Offer data protection courses in law schools and information technology courses to produce expertise on a long-term basis. The office is operational at maximum capacity by making sure that it has the necessary finances, highly qualified staff, and power to ensure conformity and punish non-conformity.
- There are technical support plans that can be prepared to provide technical and financial support to the SMEs to implement the data protection initiatives, including free or subsidised compliance software and expert advice. Work together with the European Commission to request the determination of adequacy to make data flows smoother with no issues, and become an even more attractive partner in the digital economy.

Conclusion

The digital economy in Pakistan has significant issues with pursuing GDPR compliance, relying on crucial gaps between the global demands and the locally available capacities to enforce the rules. Lack of approved comprehensive data protection laws, inadequate regulatory capacity, and technical competencies pose a lot of hurdles to business and provide insufficient protection to the

citizens. Although the draft Personal Data Protection Bill is a step in the right direction, the resources available to enforce it and the delays in its implementation are some of the challenges that prevent success. The inadequacy of technical infrastructure, especially amongst the SMEs, is another compliance challenge. Such loopholes not only limit Pakistan's access to lucrative markets in the EU but also expose citizens to data privacy risks, which makes legislative intervention, capacity building, and strategic investment in the digital governance infrastructure urgent.

These findings contain significant implications for policy regulation and the institutional development of GDPR in Pakistan. The research on GDPR standards and the digital economy of Pakistan has the following implications:

Building a regulatory body which shows the areas requiring investment in regulatory infrastructure, expertise, and institutional structures to make it workable in enforcement. GDPR awareness will allow businesses to develop strategic approaches to comply with competition, which, in turn, will contribute to ontological accessibility to international markets and foreign investments.

The findings can be utilised to revise the legislation on the Personal Data Protection Bill to ensure that the legislative provisions are based on realistic compliance challenges and enforcement abilities. The insight into the weaknesses in the technology can be applied to guide their investments in privacy-enhancing technologies and safe data management systems by the public and the private sector.

The outcomes of the study can be employed to initiate a dialogue with the EU institutions regarding the matter of adequacy establishment and the technical assistance programmes, and put Pakistan into an advantageous position in terms of cooperation with other nations in creating the digital economy.

The studies of the modern standards, such as GDPR, and the digital economy of Pakistan have a number of limitations. Firstly, the dynamism of the law of data protection in Pakistan, where the Personal Data Protection Bill is yet to be adopted, is what causes a certain sense of ambiguity in analysing the legislation and the requirements of the law.

Secondly, no empirical research has been carried out on the actual practice of business compliance because not a great number of organisations publish their data protection standards and GDPR compliance initiatives. Third, the results of the research will be less transferable in the near future, and they should be continuously updated due to the speed of technological changes and the new nature of the types of businesses that may emerge. Furthermore, as the regulatory authority does not operate, there is virtually no information on the enforcement and case studies to practice. The digital economy in Pakistan is heterogeneous due to the fact that it is situated between the high-tech IT-based exporters and small informal e-businesses, and so it is hard to generalise findings across various industries.

Finally, the credibility provided by the government in terms of regulation by imposing resources and their availability is not readily available in credible information due to limitations of transparency. Such limitations demand strict orientation of the results and that an individual realises that the regulatory landscape will transform radically the moment the legislation is implemented.

Future Research Directions

The additional development of the GDPR standards and the digital economy in Pakistan may be considered in relation to several main spheres, which should be addressed to resolve the current problems and improve compliance:

- A close analysis of the data protection with other related developing economies that managed to tailor themselves to the GDPR guidelines, and what could be applied or learned.

- The economic analysis of the impact of GDPR compliance on Pakistani businesses, including the investment requirements, the cost of doing business, and the possible advantages of entering the market.
- Assessment of the alternative types of enforcement models that may be engaged in the case of Pakistan, such as co-regulatory, self-regulation, or industry and public-private partnerships, which can be employed to increase compliance with the outlined resource limits.
- The investigation of the implementation issues and excellence in various industries, such as fintech, healthcare, e-commerce, and telecommunications, to come up with the industry-specific compliance models.
- Comparison of how the privacy-enhancing technology is used in Pakistani business and the obstacles to the use of technical controls that the GDPR demands.

References

- Afzal, J. (2024). Digital Law Enforcement Challenges and Improvement. In J. Afzal, *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (pp. 47–78). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-7106-6_3
- Ali, M. I., & Ahmad Hussain, K. (2024). Unveiling the tapestry: A comparative investigation into data-protection legislation in India and Pakistan. *SOCRATES. Rīgas Stradiņa Universitātes Juridiskās Fakultātes Elektroniskais Juridisko Zinātnisko Rakstu Žurnāls / SOCRATES. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law*, 1(28), 1–8. <https://doi.org/10.25143/socr.28.2024.1.01-08>
- Asif, M., Shah, H., & Asim, H. A. H. (2025). Cybersecurity and Audit Resilience in Digital Finance: Global Insights and the

- Pakistani Context. *Journal of Asian Development Studies*, 14(3), 560–573. <https://doi.org/10.62345/jads.2025.14.3.47>
- Bentotahewa, V., Hewage, C., & Williams, J. (2022). The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *SN Computer Science*, 3(3), 183. <https://doi.org/10.1007/s42979-022-01079-z>
- Booth, A., Anthea, S., & Diana, P. (2016). *Systematic Approaches to a Successful Literature Review* (2nd ed). https://www.researchgate.net/publication/235930866_Systematic_Approaches_to_a_Successful_Literature_Review (Original work published SAGE Publications)
- Egger, M., Higgins, J. P. T., & Davey Smith, G. (Eds.). (2022). *Systematic Reviews in Health Research: Meta-Analysis in Context* (1st ed.). Wiley. <https://doi.org/10.1002/9781119099369>
- Faisal, S. M., Khan, N. T., & Ahmad, I. (2024). Challenges in Combating Cybercrime: A Comparative Study of Pakistani and International Legal Frameworks. *The Journal of Research Review*, 01, 228–242. <https://thejrr.com/index.php/39/article/view/43>
- Haque, A. B., Islam, A. K. M. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR Compliant Blockchains—A Systematic Literature Review. *IEEE Access*, 9, 50593–50606. <https://doi.org/10.1109/ACCESS.2021.3069877>
- Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber Forensic Investigation Infrastructure of Pakistan: An Analysis of the Cyber Threat Landscape and Readiness. *IEEE Access*, 11, 40049–40063. <https://doi.org/10.1109/ACCESS.2023.3268529>
- Hiver, P., Al-Hoorie, A. H., Vitta, J. P., & Wu, J. (2024). Engagement in language learning: A systematic review of 20 years of research methods and definitions. *Language Teaching Research*, 28(1), 201–230. <https://doi.org/10.1177/13621688211001289>

- Howell, K. (2013). *An Introduction to the Philosophy of Methodology*. SAGE Publications Ltd. <https://doi.org/10.4135/9781473957633>
- Isazade, A., Malik, A., & Alshawki, M. B. (2025). Blockchain-Enabled GDPR Compliance Enforcement for IIoT Data Access. *Journal of Cybersecurity and Privacy*, 5(4), 84. <https://doi.org/10.3390/jcp5040084>
- Jhokio, A., Rehman, T. U., & Kaleemullah. (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. <https://doi.org/10.63468/jpsa.3.2.48>
- Kaya, M., & Shahid, H. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. *Interdisciplinary Studies in Society, Law, and Politics*, 4(2), 219–233. <https://doi.org/10.61838/kman.isslp.4.2.20>
- Komba, M. M., & Lwoga, E. T. (2020). Systematic Review as a Research Method in Library and Information Science: In P. Ngulube (Ed.), *Advances in Library and Information Science* (pp. 80–94). IGI Global. <https://doi.org/10.4018/978-1-7998-1471-9.ch005>
- Kraus, S., Breier, M., Lim, W. M., Dabić, M., Kumar, S., Kanbach, D., Mukherjee, D., Corvello, V., Piñeiro-Chousa, J., Liguori, E., Palacios-Marqués, D., Schiavone, F., Ferraris, A., Fernandes, C., & Ferreira, J. J. (2022). Literature reviews as independent studies: Guidelines for academic practice. *Review of Managerial Science*, 16(8), 2577–2595. <https://doi.org/10.1007/s11846-022-00588-8>
- Malik, W., Gul, S., & Qureshi, G. M. (2025). Regulating Artificial Intelligence: Challenges for Data Protection and Privacy in Developing Nations. *Journal of Social Signs Review*, 03(05), 95–108. <https://socialsignsreivew.com/index.php/12/article/view/249>

- Mangi, Dr. D. B., Butro, I., & Shaikh, A. (2025). The Impact of Artificial Intelligence on Data Protection Laws in Pakistan. A Critical Analysis. *ACADEMIA International Journal for Social Sciences*, 4(2), 1653–1663. <https://doi.org/10.63056/ACAD.004.02.0279>
- Mehmood, M. (2025). The Role of Cyber Security in Promoting Digital Inclusion: A Case Study of Pakistan. *Annals of Human and Social Sciences*, 6(1), 35–44. <https://ojs.ahss.org.pk/journal/article/view/894>
- Mushtaq, S. A., Baig, K., Hassan, S., & Ahmad, W. (2024). The Importance of China's Competition Law in the Management of Data in the Country's Rapidly Developing Digital Economy: Policy Recommendations for Pakistan. *Current Trends in Law and Society*, 4(1), 27–51. <https://doi.org/10.52131/ctls.2024.0401.0030>
- Nabeel, F., & Iqbal, K. (2025). Privacy, Data Protection and Cyber Crimes: Mapping Perceptions of Pakistani Users. *Journal of Applied Security Research*, 20(2), 293–319. <https://doi.org/10.1080/19361610.2024.2372989>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., & Moher, D. (2021). Updating guidance for reporting systematic reviews: Development of the PRISMA 2020 statement. *Journal of Clinical Epidemiology*, 134, 103–112. <https://doi.org/10.1016/j.jclinepi.2021.02.003>
- Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, 52(2), 183–199. <https://doi.org/10.1016/j.im.2014.08.008>
- Paul, J., Lim, W. M., O'Cass, A., Hao, A. W., & Bresciani, S. (2021). Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). *International Journal of Consumer Studies*, 45(4). <https://doi.org/10.1111/ijcs.12695>
- Pawson, R., Greenhalgh, T., Harvey, G., & Walshe, K. (2005). Realist review—A new method of systematic review

- designed for complex policy interventions. *Journal of Health Services Research & Policy*, 10(1_suppl), 21–34. <https://doi.org/10.1258/1355819054308530>
- Petticrew, M., & Roberts, H. (2006). *Systematic Reviews in the Social Sciences: A Practical Guide* (1st ed.). Wiley. <https://doi.org/10.1002/9780470754887>
- Rahi, S. (2017). Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development. *International Journal of Economics & Management Sciences*, 06(02). <https://doi.org/10.4172/2162-6359.1000403>
- Rauf, S., Sifarish, S., & Ahmed, S. S. (2025). From Drafts To Doctrine: Building A Coherent Legal Framework For Data Protection In Pakistan. *Competitive Research Journal Archive*, 03(02), 512–520. <https://thecrja.com/index.php/Journal/article/view/175>
- Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, 5(4), 533–561. <https://doi.org/10.1365/s43439-024-00128-y>
- Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges Faced by the Judiciary in Implementing Cybersecurity Laws in Pakistan. *The Critical Review of Social Sciences Studies*, 3(1), 1052–1066. <https://doi.org/10.59075/1wyx0v30>
- Shami, A. Z. A., Asghar, U., & Ashraf, C. (2025). Data Protection and Cyber Security Laws in Pakistan: Addressing Digital Privacy in E-Commerce and Consumer Data. *Dialogue Social Science Review*, 03(03), 524–536. <https://dialoguessr.com/index.php/2/article/view/395>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>

- Sohrab, L. B., Shah, K., & Nawaz, B. (2024). Bridging the Gap: Cross-Border Data Flows & Data Protection Harmonization in Pakistan. *Journal of Social Sciences Development*, 3(03), 232–247. <https://doi.org/10.53664/JSSD/03-03-2024-19-232-247>
- Victor, L. (2008). Systematic reviewing in the social sciences: Outcomes and explanation. *Enquire*, 1(1), 32–46. <https://www.nottingham.ac.uk/sociology/documents/enquire/volume-1-issue-1-victor.pdf>
- Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, 39(1), 93–112. <https://doi.org/10.1177/0739456X17723971>
- 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). <https://doi.org/10.48112/jestt.v1i1c.1>
- Yaseen, M., & Phattanasin, Dr. K. (2025). The Tension between Data Flows and Digital Sovereignty A Comparative Analysis of Global Regulatory Approaches. *Dialogue Social Science Review (DSSR)*, 3(4), 866–872. <https://dialoguessr.com/index.php/2/article/view/516>