

GSSR

GLOBAL SOCIAL SCIENCES REVIEW
HEC-RECOGNIZED CATEGORY-Y

VOL. IX, ISSUE IV, FALL (DECEMBER-2024)

Article Title

Comparative Analysis and Challenges in Data Protection

Global Social Sciences Review

p-ISSN: [2520-0348](#) e-ISSN: [2616-793x](#)

DOI(journal): [10.31703/gssr](#)

Volume: IX (2024)

DOI (volume): [10.31703/gssr.2024\(IX\)](#)

Issue: IV Fall (December 2024)

DOI(Issue): [10.31703/gssr.2024\(IX-IV\)](#)

Home Page

www.gssrjournal.com

Volume: IX (2024)

<https://www.gssrjournal.com/Current-issue>

Issue: IV-Fall (June-2024)

<https://www.gssrjournal.com/Current-issue/9/4/2024>

Scope

<https://www.gssrjournal.com/about-us/scope>

Submission

<https://humaglobe.com/index.php/gssr/submissions>

Google Scholar



Visit Us



Abstract

Pakistani laws have numerous shortcomings, as evidenced by the comparison of their regulations with international standards like GDPR and CCPA. The list comprises the applicability, permissions granted to data subjects, restrictions on its distribution, and enforcing mechanisms. In particular, the GDPR provides extensive data protection rights and enforces rigorous controls on international data transfers, surpassing the level of data security established by Pakistani law in previous years (General Data Protection Regulation, 2018). Similarly, the CCPA's strong emphasis on consumer rights and non-discrimination principles provides a solid framework that Pakistan could use as a model for improving its data protection legislation.

Keywords: Data Protection, Challenges, PECA, CCPA

Authors:

Abida Hassan: (Corresponding Author)

Assistant Professor (Law), Dr. Muhammad Iqbal Law School, Government College University, Lahore, Punjab, Pakistan.

(Email: dr.abidahassan@gcu.edu.pk)

Maryam Hassan: MBA/Mphil (UVAS), Lahore, Punjab, Pakistan.

Pages: 291-298

DOI: [10.31703/gssr.2024\(IX-IV\).26](#)

DOI link: [https://dx.doi.org/10.31703/gssr.2024\(IX-IV\).26](https://dx.doi.org/10.31703/gssr.2024(IX-IV).26)

Article link: <http://www.gssrjournal.com/article/comparative-analysis-and-challenges-in-data-protection>

Full-text Link: <https://gssrjournal.com/farticle/comparative-analysis-and-challenges-in-data-protection>

Pdf link: <https://www.gssrjournal.com/jadmin/Auther/31rv1olA2.pdf>

Citing this Article

26		Comparative Analysis and Challenges in Data Protection					
Author		Abida Hassan Maryam Hassan		DOI	10.31703/gssr.2024(IX-IV).26		
Pages	291-298	Year	2024	Volume	IX	Issue	IV
Referencing & Citing Styles	APA 7 th	Hassan, A., & Hassan, M. (2024). Comparative Analysis and Challenges in Data Protection. <i>Global Social Sciences Review</i> , 9(4), 291-298. https://doi.org/10.31703/gssr.2024(IX-IV).26					
	CHICAGO	Hassan, Abida, and Maryam Hassan. 2024. "Comparative Analysis and Challenges in Data Protection." <i>Global Social Sciences Review</i> 9 (4):291-298. doi: 10.31703/gssr.2024(IX-IV).26.					
	HARVARD	HASSAN, A. & HASSAN, M. 2024. Comparative Analysis and Challenges in Data Protection. <i>Global Social Sciences Review</i> , 9, 291-298.					
	MHRA	Hassan, Abida, and Maryam Hassan. 2024. 'Comparative Analysis and Challenges in Data Protection', <i>Global Social Sciences Review</i> , 9: 291-98.					
	MLA	Hassan, Abida, and Maryam Hassan. "Comparative Analysis and Challenges in Data Protection." <i>Global Social Sciences Review</i> 9.4 (2024): 291-98. Print.					
	OXFORD	Hassan, Abida and Hassan, Maryam (2024), 'Comparative Analysis and Challenges in Data Protection', <i>Global Social Sciences Review</i> , 9 (4), 291-98.					
	TURABIAN	Hassan, Abida and Maryam Hassan. "Comparative Analysis and Challenges in Data Protection." <i>Global Social Sciences Review</i> 9, no. 4 (2024): 291-98. https://dx.doi.org/10.31703/gssr.2024(IX-IV).26 .					



Global Social Sciences Review

www.gssrjournal.comDOI: <http://dx.doi.org/10.31703/gssr>

Cite Us



Title

Comparative Analysis and Challenges in Data Protection

Authors:

Abida Hassan: (Corresponding Author)

Assistant Professor (Law), Dr. Muhammad Iqbal
Law School, Government College University,
Lahore, Punjab, Pakistan.
(Email: dr.abidahassan@gcu.edu.pk)

Maryam Hassan: MBA/Mphil (UVAS), Lahore, Punjab,
Pakistan.

Contents

- [Introduction](#)
- [Literature Review](#)
- [Export Market Orientation](#)
- [Methodology:](#)
- [Data Collection](#)
- [Common Method Bias](#)
- [Measures](#)
- [Endogeneity](#)
- [Analysis](#)
- [Discussion](#)
- [Managerial Implications](#)
- [Limitations and future research directions](#)
- [References](#)

Abstract

Pakistani laws have numerous shortcomings, as evidenced by the comparison of their regulations with international standards like GDPR and CCPA. The list comprises the applicability, permissions granted to data subjects, restrictions on its distribution, and enforcing mechanisms. In particular, the GDPR provides extensive data protection rights and enforces rigorous controls on international data transfers, surpassing the level of data security established by Pakistani law in previous years (General Data Protection Regulation, 2018). Similarly, the CCPA's strong emphasis on consumer rights and non-discrimination principles provides a solid framework that Pakistan could use as a model for improving its data protection legislation.

Keywords: [Data Protection](#), [Challenges](#), [PECA](#), [CCPA](#)

Introduction

This analysis explores the nuances of data privacy regulations, highlighting legal and regulatory frameworks, and enforcement mechanisms within Pakistan, and comparing them with global standards; General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Due to Pakistan's growing reliance on digital systems, which increases the likelihood of

data breaches and cyber incidents, concerns about security breaches have spread around the globe (Ibrar et. al., 2023). This chapter not just pinpoints convergences, divergences and room for improvement in Pakistan's data privacy landscape, but also prescribes problems and gaps in Pakistan's cyber security space, presenting a complex and multifaceted picture of issues and gaps in the country's data protection systems.



Legal Frameworks – Personal Data Protection Bill, 2023 in Pakistan

When examining PDPB, and GDPR, essentials of both rules will be discussed in comparison to one another. Meaning the scope of it, definition, the rights of the data subjects, the responsibilities of controllers/policymakers, the transfer of data and enforcement measures.

When processing the data of Pakistani citizens both inside and outside of Pakistan, the public and commercial sectors are subject to the PDPB. However, its territorial scope is somewhat ambiguous since it does not specify any applicability in regions such as the Gilgit Baltistan and Azad Jammu and Kashmir. On the flip side, all organizations that handle the private data of EU people, no matter where, are subject to GDPR.

The definitions and concepts in PDPB, like the “legitimate interest”, “national interest” and “public interest” are vaguely defined, leading to potential misuse and lack of clarity in the application. Moreover, the “sensitive personal data” and “critical personal data” also lack comprehensive definitions, which eventually undermines the law’s effectiveness. Whereas, GDPR provides clear and comprehensive definitions of the key terms such as “personal data”, “data subject”, “data controller and data processor” as mentioned previously. It also narrowly defines the term “legitimate interest” and ensures that its subjects’ rights and liberty is not compromised, but must be done under specific conditions only.

The Pakistan Bill grants rights to data subjects which includes the access, rectification and even erasure of personal data. However, the provision regarding the data erasure lacks any stringent timelines which allows up to 14 days, which may delay the enforcement of this right. Moreover, rights such as data portability and automated decision making lack quality and robust mechanisms for enforcement. The GDPR, meanwhile, gives data subjects a number of powerful rights, including the ability to view, edit, remove, and transfer personal data as well as the ability to refuse data processing and automated decision-making. It expressly states that the demands of the data subjects must be complied with by the data controllers as soon as possible, usually within a month.

The PDPB requires the data controllers to

obtain consent for dealing with personal data and should notify the subjects within a reasonably possible timeframe. However, the bill has broad exceptions for consent, such as processing for legitimate interest, which is vaguely defined and may lead to misuse. Although it mandates data localization for critical personal data, which may impose significant operational and economic burdens. In contrast, the GDPR mandates that data controllers provide proof of a legitimate and authorized basis for handling personal data, such as permission, contract fulfillment, legal requirements, vital interests, public interest, and legitimate interests. It enforces stern requirements for obtaining consent, including clarity, specificity and the ability to withdraw consent as easily as it was given.

With regards to cross-border data transfer, the PDPB allows the transfer of personal data outside Pakistan under certain condition but states that the critical personal data must be stored and processed within Pakistan. This is a strong data localization requirement which eventually restricts the free flow of data and puts forth challenges for international businesses. The transfers are permitted only if the receiving country has adequate data protection measures in place or if the subject has granted explicit permission for a transfer. However, again definition of the word adequate and the specific criteria for determining it are not clearly outlined in the bill, leading to potential ambiguities in its implementation. Moreover, the PDPB includes broad exemptions for data transfer in cases of national interest and public order, which are not clearly defined and could be used to circumvent the restrictions on data transfer.

On the other hand, only those nations that offer an acceptable degree of data protection are permitted by GDPR to receive personal data transfers from individuals residing outside of the European Economic Area (EEA). These nations are evaluated and recognized by the European Commission. GDPR therefore permits the use of Standard Contractual Clauses (SCC) and obligatory business standards for transfers to nations that are not acknowledged as offering acceptable data protection. as mechanisms to ensure that data protection during the transfers. These mechanisms and delegations are well-defined and strictly regulated in order to prevent any sort of abuse.

As far as the enforcement mechanisms are

concerned, the PDPB aims to establish the National Commission for Personal Data Protection (NCPDP) which is responsible with the enforcing of the provisions of the law. However, the commission is under the administrative control of the federal government which again raises concerns about its independence and potential for government influence over data protection matters.

The bill provides for penalties in the case of noncompliance, including fines for violations, for example, for unauthorized processing of personal data or lack of appropriate personal data protection measures. But here too the enforcement steps taken to apply these penalties and the procedural framework of how to do so is again not entirely spelled out. Although the PDPB allows individuals to lodge their complaints with the Commission regarding any violation of their data protection rights still the process and the timelines for handling these complaints are not well defined, which could affect the efficacy of this enforcement mechanism.

Meanwhile, GDPR introduces independent supervisory authorities in every EU member state that will be tasked with enforcing GDPR. The Data Protection Authority (DPA) have extensive powers of investigation, the ability to give fines and regular demands to comply with principles of Data Protection to Organizations. A violation of the GDPR can result in fines of up to €20 million or 4% of the global yearly revenue of the previous fiscal year, whichever is larger. Such high-level financial penalties serve as a strong deterrent against violations. Moreover, GDPR employs of “one-stop shop” instruments and mechanisms where DPA coordinates investigations and enforcement actions for organizations that are operating in multiple EU countries, to ensure the consistent application of the law across the European Union. GDPR also has strong provisions which allow for seeking redress, such as complaints to DPS and court remedies if a person feels that their right has been breached. The rules require a timely response to complaints and mechanisms must be put in place to enable individuals to obtain an effective remedy.

CCPA Versus PDPB

The PDPB and the CCPA are aimed at protecting individuals’ personal data. But there are differences in both scales and approaches, and in the way they will be implemented, according to the different

political economic and technological spheres in Pakistan and California. This analysis will highlight where the PDPB lacks in comparison to the CCPA and how the CCPA is more effective.

In terms of the PDPB's scope and applicability, data controllers and processors are covered, as was previously stated. The applicability of the legislation to foreign entities or corporations is less apparent and robust than that of the CCPA which regulates businesses that gather personal data from California residents wherever they may be. Therefore, if businesses outside of California are handling the data of Californians, this applies to them as well. This applies to companies outside California that bring in more than \$25 million a year, maintain the data of at least 50,000 customers and households, and make at least half of their revenue from the sale of personal data. PDPB mentions the application to data controllers that do not reside in Pakistan, if they process personal data of Pakistani residents, but it lacks detailed mechanisms for enforcement and compliance as compared to the CCPA's approach.

The effectiveness of the PDPB enforcement commission may be impacted by its lack of autonomy due to administrative oversight by the federal government. In contrast, the CCPA benefits from an independent enforcement authority. Moreover, the CCPA's strong penalties and clear enforcement procedures provide a significant deterrent against non-compliance where is the PDPB's less stringent and politically influence enforcement may not be as effective in ensuring compliance as the enforcement mechanisms are less transparent and potentially subject to political influence.

With regards to data localization and international transfers, CCPA can be seen for adopting a more flexible perspective as compared to the PDPB as there are no specific requirements for data localization under the CCPA and allows cross-border transfers provided that the data subjects rights are protected and transfers comply with the applicable regulations. Whereas PDPB's requirements are highly restrictive and require explicit consent in compliance with the national interest provisions which are ambiguously defined and could be used to limit data flows. Moreover, it requires the critical personal data to be stored and processed within Pakistan which could impact international businesses and local economic growth

negatively due to the lack of infrastructure. Hence, the CCPA's lack of data localization requirements facilitates the international businesses operations and data flows, while the PDPB's strict localization requirements could hinder economic growth and international trade. PDPB's vague provisions on cross-border trader transfers may lead to inconsistent application and create challenges for businesses operating across borders.

California Privacy Protection Agency (CPPA) is an independent organization that has the power to police the CCPA. It is independent of the government, and guarantees the independent application of the data protection provisions. That means the CCPA's enforcement arm is more independent, making it more effective in enforcing data protection. While PDPB's regulatory agency is not independent, which may result in potential conflict of interest and reduced effectiveness; the federal government's power to control of the policy directives, members appointments and the procedures by which the Commission is run, may impair the independence of the Commission. Imagine CCPA's transparency and accountability requirements are greater, it engenders very high levels of trust and compliance. The PDPB on the other hand lacks such details in its provisions that could cause gaps and transparency.

Notable Data Breaches/Incidents in Pakistan

Pakistan has witnessed several events that have resulted in critical data breaches and disruption of cyber security, including government organizations and the private sector (Khan, [2022](#)). By outlining these incidents, it can be seen how the threat landscape has evolved and the importance of robust cybersecurity measures to safeguard sensitive information and systems.

Case Study 1.

Malware Infections: In 2017, the country of Pakistan experienced one of the world's highest malware infections rates at 15-20 malware hosting websites per 1000 hosting websites. (A. Rafiq, [2019](#)). Moreover, country boasts second highest malware detection rate in the world in the first quarter of 2017 (27.48%). In Asia Pacific, Pakistan is the most vulnerable country to Malware infection as revealed by Microsoft's Asia Pacific Malware Index 2016. The

major malware that affected Pakistan was Gamarue, Skeya and Peals which can install more software and steal important information from infected desktops. (Microsoft, 2016).

Case Study 2.

Banking Sector Breaches: There were major banking sector breaches in 2018, causing heavy losses to the financial sector. It has been revealed that the dark web comprised the personal details of over 8,000 Pakistani bank accounts, which is presenting a big privacy concern. (Bukht et al., [2020](#)).

Case Study 3.

Denial of Service (DoS) Attack by Indian Hackers: Denial of service (DoS) attacks are carried out to disrupt the services of targeted organizations by flooding their networks with excessive traffic resulting in service interruptions and malfunctions (Raza et al., [2021](#)). Indian hackers carried out a series of DoS attacks for Pakistani Websites targeting government as well as security agencies. These attacks were based on flooding the target's websites with traffic to make them crash and unavailable.

Recurrent attacks were the manifestation of the ongoing cyber warfare situation between India and Pakistan (Khan et al., [2021](#)). The Incident reveals the necessity of robust defenses to protect critical network infrastructure from DoS malicious activities, and highlights that cyber can never be considered outside of the air of Cyber Warfare and the key role of Cyber Security in the National Defense.

Gaps and Challenges

The Pakistan cybersecurity ecosystem is marred by various issues, such as limitations, threats from cross-border, lack of awareness and need for proper regulatory framework, and a lack of the PDPB (Khan & Anwar, [2020](#)). Acknowledging and managing these issues is crucial in enhancing a nation's cybersecurity and decreasing the risks associated with data breaches and cyber threats.

Enforcement Challenges

Pakistan's legislation on the safeguarding and protection of data, along with cyber security were found to be conflicting with numerous other areas

of enforcement. The National Cybercrime Response Center (NRC3), established under the Electronic Crimes Ordinance in 2007, operates under the Federal Investigation Agency (FIA) rather than as an independent agency, which reduces its effectiveness in combating cyber threats (Adil, [2023](#)). Moreover, there is an ongoing dispute among government officials over which law enforcement agency should handle cybersecurity matters, and there are doubts about the FIA's capability or competence (U.P.Khan & Anwar, [2020](#)). Inadequate oversight and accountability is also a big problem because of the absence of independent oversight bodies and a lack of accountability mechanisms (M.Z.U. Rehman, [2023](#)).

The scope and impact of the law is limited due to its wide discretion granted to state ministries. Issues with the draft's weak legal definitions, particularly the definition of 'data subject' and 'authorities', and the term 'state', make it obscure and difficult to apply for public authorities; it is also difficult to enforce. The effective implementation of data protection in a federally – based system such as Pakistan would require coordinated actions by both federal and regional governments. Additionally, the PECA has broad powers on the access and demanding the decoding of data, which can lead to misuse and questions about the efficacy of security measures (Halim et al., [2022](#)).

Institutional Challenges

The institutional challenges in the context of data protection in Pakistan are complex and have a number of key concerns. In the absence of dedicated Cybersecurity Agencies, Cybersecurity issues remain undermined and suppressed with respect to other priorities related to terrorism, and existing agencies like NRC3 lack the independence and/or the focus they need for effective management (M. F. Khan et al., [2021](#)). There is no Cyber Emergency Response Team (CERT), and no dedicated cybercrime tribunals which impedes the development of efficient cyber security measures (Mishra et al., [2022](#)). The difficulty for the proposed commission (NCPDP) is to achieve independence and proper funding to effectively handle the data practices. Moreover, people consider a lack of coordination between different government bodies and agencies assigned to data protection has a higher risk of cyber threats (Halim et al., [2022](#)).

Lack of know-how and resources to address data protection issues is also a challenge at institutions. While the existing systems of accountability are inadequate and cannot hold institutions accountable for data breaches (Lonzetta & Hayajneh, [2021](#)). In addition to erecting new structures like the NCPDP, there is a need for major improvement in coordination, capacity building and accountability at all levels, to address those institutional challenges.

Technical Challenges

There are many technical challenges with data protection in Pakistan. Strong Cyber security aspects are nonexistent, on the contrary a state of the art anti-intrusion system and enough security officers are not visible. The prevalence of human mistakes resulting in data breaches underscores the insufficiency of staff training across all tiers. While data encryption and pseudonymization are useful tools for protecting personal data, it is still difficult to apply them consistently across all sectors of the system (Zahid, [2024](#)). Furthermore, a lot of IT systems are antiquated and inefficient, and they frequently lack the capacity that is required (Nawaz, [2023](#)). The incorporation of best practices for information security into system-wide policy is also lacking. In addition, the country's cybersecurity infrastructure is underdeveloped, making it difficult to protect sensitive data from data breaches. Data protection techniques and best practices are not well understood by many organizations or individuals, making them a disadvantage. In addition, rapid technological progress is making it more challenging for regulatory systems and enforcement mechanisms to keep pace (Saeed et al., [2023](#)).

Cultural Challenges

Pakistan has a number of cultural issues related to data protection. Data protection is not one thing people are aware of, and there isn't a lot of public awareness regarding the risks with data breaches either (Hayat, [2023](#)). Personal Data protection is too often eclipsed by cultural aspects where this protection is not a priority or a concern. Additionally, the cultural inertia of resistance to change is an obstacle in implementing new technologies and practices that can enhance data protection (Boothe, [2023](#)). Additionally, the role of

civil society in promoting dialogue and engagement, and the influence of the media, which tends to focus on violations of human rights and cyber threats make efforts to promote a strong data protection culture in the country complicated (Sadruddin, [2012](#)).

Socio-economic Challenges

Data protection is also facing the challenges of significant inequality in the status of digital environment in Pakistan. Usability of information and technologies is poor and becomes a risk for marginalised groups who do not have access to these technologies in protecting their personal information (Z. S. Ahmed et al., [2023](#)). Limited financial resources serve to make these issues worse as it means that not all locations can invest in state-of-the-art technologies or infrastructure to protect the current data protection. Limited funding available to implement and regulate data privacy laws can hinder the establishment of effective regulatory bodies and technologies (Manzoor et al., [2021](#)).

SMEs face hurdles in establishing the effectiveness of data protection efforts due to a scarcity of resources and lack of expertise (Rawindaran et al., [2023](#)). Achieving financial gain while implementing information and robust privacy safeguards is a more challenging, contentious matter in terms of policy (Rawindaran et al., [2023](#)) (Merritt, [2021](#)). The hurdles faced reflect the intricate equilibrium involved in safeguarding personal data and fostering digital innovation and growth in Pakistan. The conscientious integration of all these factors points to the holistic importance of policies that deal with the digital divide as well as economic inequalities and ensure equitable protection of privacy in a rapidly changing technological environment of

Pakistan.

Conclusion

The PDPB 2023 is a positive step in the direction of establishing a comprehensive data protection framework in Pakistan, but it still has a number of shortcomings when compared to GDPR and CCPA. The clear and comprehensive, globally recognised and powerful data transfer and enforcement mechanisms within GDPR offer more protection in terms of your data and more transparency in how you operate. The CCPA, with its wide reach and applicability on consumer rights, and independent enforcement model rather than data localization restrictions, is more comprehensive and effective. In comparison, the PDPB involves a narrower scope of more government-operated entities, less obvious rights and extensive data localization, which impact data flows and international business activities abroad. The PDPB must be evolved and improved in order to raise its level of protection and develop it in a way that is more conducive to the protection of personal data and more effectively enforces it, following the spirit of the CCPA and GDPR, which provide greater protection and enforceability for personal data.

On the other hand, the significance of cyber security to Pakistan's digital transformation is apparent and cannot be ignored. The lessons learned from the case studies and challenges featured in this chapter highlight the need to be proactive in responding to cybersecurity threats and making strategic investments in cybersecurity infrastructure, training, and collaboration. Through direct action on these issues, Pakistan can establish a foundation for ensuring the safety of its digital assets and safeguarding both the privacy and national security of individuals in heightened global connectivity.

References

- Adil, K. (2023, March 7). *Legal framework for policing cyberspace in Pakistan: An overview*. Research Society of International Law.
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Baig, A. (2023, August 14). *What is California Consumer Privacy Act (CCPA)*. Securiti. <https://securiti.ai/what-is-ccpa/>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Boothe, K. (2023). *Cultural change on the regulatory topic of data privacy: Preparing all "lines of defence" in an organization for regulatory changes triggered by the General Data Protection Regulation (GDPR)* [Doctoral dissertation, LIGS University]. ResearchGate. <https://doi.org/10.13140/RG.2.2.23904.15363/1>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Bukht, T., Raza, M., Awan, J., & Ahmad, R. (2020). Analyzing cyber-attacks targeted on the banks of Pakistan and their solutions. *IJCSNS International Journal of Computer Science and Network Security*, 20(2), 31–38. <https://www.researchgate.net/publication/342344572>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Christ, B. (2024, April 9). *The impact of security breaches on educational institutions*. Bravura Security. <https://www.bravurasecurity.com/blog/the-impact-of-security-breaches-on-educational-institutions>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Halim, W., Upadhyay, A., & Coflan, C. (2022). *Data access and protection laws in Pakistan: A technical review*. EdTech Hub. <https://doi.org/10.53832/edtechhub.0098>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Hayat, A. (2023, July 13). *Protecting data privacy: The significance of laws in developing countries and the digital age*. Medium. <https://medium.com/@rajaahsanhayat/protecting-data-privacy-the-significance-of-laws-in-developing-countries-and-the-digital-age-217c4023a341>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Khan, M. F., Raza, A., & Naseer, N. (2021). Cybersecurity and challenges faced by Pakistan. *Journal of International Affairs*, 4(4).
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Khan, S. (2022). *Cyber security challenges in Pakistan: An assessment*. ResearchGate. <https://www.researchgate.net/publication/360256123>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Khan, U. P., & Anwar, M. W. (2020). Cyber security in Pakistan: Regulations, gaps and a way forward. *Cyberpolitik Journal*, 5(10).
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Lonzetta, A. M., & Hayajneh, T. (2021). Challenges of complying with data protection and privacy regulations. *EAI Endorsed Transactions on Scalable Information Systems*, 8(30), Article e5. <https://doi.org/10.4108/eai.26-5-2020.166352>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Manzoor, R., Javed, A., Ahmed, V., & Rauf, A. (2021). Digital financial services in Pakistan: Opportunities, challenges and suggestions. *Journal of Finance & Economics Research*, 6(2), 1–16. <https://doi.org/10.20547/jfer2106201>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Merritt, R. (2021, December 29). *Balancing data privacy and growth in the digital economy*. Center for International Private Enterprise. <https://www.cipe.org/blog/2021/12/29/balancing-data-privacy-and-growth-in-the-digital-economy/>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: Evidence from seven nations. *Computers & Security*, 120, Article 102820. <https://doi.org/10.1016/j.cose.2022.102820>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Nawaz, U. (2023, February 24). *The state of cyber security in Pakistan: Challenges and opportunities*. LinkedIn. <https://www.linkedin.com/pulse/state-cyber-security-pakistan-challenges-umer-nawaz/>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Rafiq, A. (2019). *Challenges of securitising cyberspace in Pakistan*. Supreme Court of Pakistan. <http://supremecourt.gov.pk/ijc/articles/10/1.pdf>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in Industry 5.0: A comparative study between Saudi Arabia and the United Kingdom. *Digital*, 3(3), 200–231. <https://doi.org/10.3390/digital3030014>
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)
- Raza, M. A., Bukht, T. F. N., Ali, M., Rehman, A. U., & Idrees, M. (2021). Analyzing the behaviour of DDoS cyber attack. *Journal of Computer Science and Network Security*, 26(4), 46.
- [Google Scholar](#) [Worldcat](#) [Fulltext](#)

Rehman, M. Z. U. (2023). Critical issues of governance in Pakistan: Strategies and solutions. *ISSRA Papers*, 15.

[Google Scholar](#) [Worldcat](#) [Fulltext](#)

Sadruddin, M. M. (2012). Study on the role of media, NGOs and civil society in promoting pluralism in Pakistan. *The Dialogue*, 7(2).

[Google Scholar](#) [Worldcat](#) [Fulltext](#)

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), Article

6666. <https://doi.org/10.3390/s23156666>

[Google Scholar](#) [Worldcat](#) [Fulltext](#)

Zahid, R. (2024, April 26). Cybersecurity challenges: Safeguarding Pakistan's digital infrastructure. Imarat Institute of Policy Studies. <https://iips.com.pk/cybersecurity-challenges-safeguarding-pakistans-digital-infrastructure/>

[Google Scholar](#) [Worldcat](#) [Fulltext](#)