Journal of Media Horizons
Volume 5 Issue 4, 2024 **ISSN(: 2710-4060 | 2710-4052**

LEGAL CONTEXT OF E-PRIVACY IN PAKISTAN

Fizza Pervez[*1], Dr. Tansif Ur Rehman[2], Riaz Ali[3], Adnan Zawar[4], Engineer Muhammad Faizan Khan[5]

[*1,2,3]*Department of Law, Dadabhoy Institute of Higher Education, Pakistan*
[4]*M.Phil. Research Scholar, Institute of Social & Cultural Studies, University of the Punjab*
[5]*Welfare Officer, Lucky Textile Mills*

[*1]fpn2112@gmail.com, [2]tansif@live.com, [3]riazali307307@gmail.com, [4]adnan.zawar@gmail.com, [5]desires_instincts@hotmail.com

Corresponding Author: *

Received: October 24, 2024 **Revised:** November 24, 2024 **Accepted:** December 07, 2024 **Published:** December 14, 2024

ABSTRACT

E-privacy has become a pressing concern in the digital age, where protecting personal data and communications is increasingly vital due to the proliferation of online activities. This research examines the legal context of e-privacy in Pakistan, focusing on the effectiveness of existing legal frameworks and identifying key challenges. Central to this analysis is the Prevention of Electronic Crimes Act (PECA) 2016, which serves as the primary legislation addressing cybercrimes and data protection in Pakistan. The research reveals that while PECA 2016 provides a foundation for addressing e-privacy issues, it faces significant limitations. These include inadequate enforcement mechanisms, limited public awareness, and a lack of coverage for emerging privacy concerns. The study highlights that PECA does not fully align with international privacy standards, such as the General Data Protection Regulation (GDPR), and that Pakistan's e-privacy measures are less advanced than those in neighboring countries.

Keywords: *cybercrimes, digital rights, digital privacy, personal data protection, public awareness*

INTRODUCTION

In the contemporary digital era, where technology increasingly intertwines with daily life, the issue of electronic privacy, often referred to as e-privacy, has gained unprecedented significance (Jahankhani et al., 2021; Walters, 2023). E-privacy protects personal data (Jenkinson, 2022; Page et al., 2022). and digital communications from unauthorized access, misuse, and breaches (Rehman, 2021a). As Pakistan navigates its rapid digital transformation, the importance of e-privacy becomes ever more apparent, highlighting both the progress and the challenges faced in safeguarding personal information in an increasingly connected world

Pakistan's digital landscape has evolved considerably over recent years. The country has seen a remarkable increase in internet usage, mobile phone penetration, and the adoption of digital services. This growth has led to greater connectivity and access to information, facilitating advancements in communication, commerce, and education (Naim et al., 2023).

While these developments have brought numerous benefits, such as enhanced convenience and opportunities for economic growth, they have also introduced new privacy risks. Individuals in Pakistan now share vast amounts of personal data online, from social media interactions to financial transactions, creating significant vulnerabilities. Cybercriminals can exploit these vulnerabilities for various malicious activities, including identity theft, fraud, and unauthorized surveillance (Burri, 2021).

Pakistan has introduced several legislative measures to protect e-privacy in response to these

emerging challenges. The Prevention of Electronic Crimes Act (PECA) 2016 is a cornerstone of Pakistan's approach to addressing cybercrimes and data protection. PECA represents a substantial step toward establishing a legal framework for digital privacy. It addresses various issues, including unauthorized access to data, cyberstalking, and data breaches. By criminalizing various forms of cyber misconduct, PECA aims to create a legal environment that deters cybercrimes and enhances personal data protection.

Despite the foundational role of PECA, its effectiveness in addressing contemporary privacy challenges have been subject to scrutiny. One of the primary criticisms of PECA is its implementation and enforcement. The Act has faced challenges related to inadequate enforcement mechanisms, limited resources, and a lack of technical expertise among law enforcement agencies. These issues have hindered the ability of the legal framework to combat emerging cyber threats and ensure robust e-privacy protections effectively. Additionally, the rapid pace of technological advancements often outstrips the legislative framework, leaving gaps that current laws struggle to address comprehensively (Zahoor & Razi, 2021).

The scope of PECA also raises concerns about its ability to cover new privacy challenges. For instance, the Act does not fully address issues related to big data analytics, artificial intelligence, and the complexities of cross-border data transfers. As digital technologies evolve, the nature of privacy threats changes, necessitating updates and refinements to existing legal frameworks. The challenge lies in ensuring that legislation remains relevant and effective in a landscape where technological innovation occurs at a breakneck pace (Masood, 2023).

Complementing PECA, the Digital Pakistan Policy outlines the government’s vision for advancing digital infrastructure and promoting economic growth through technology. The policy aims to foster a digitally empowered economy and improve technological capabilities across various sectors. While the policy supports the broader goal of digital transformation, it primarily focuses on economic and infrastructural aspects rather than providing a comprehensive approach to e-privacy. This focus means that while the policy contributes to the growth of digital technologies, it does not fully address the multifaceted privacy issues that arise from increased digital activity (Zaman et al., 2022).

Given these circumstances, the primary research problem this study addresses is the inadequacy of current e-privacy measures in Pakistan. Despite the legislative efforts embodied in PECA and the Digital Pakistan Policy, significant gaps exist in effectively protecting personal data and addressing emerging privacy concerns (Akhtar, 2023). This research aims to provide a comprehensive assessment of the current legal context of e-privacy in Pakistan, focusing on the effectiveness of existing legal frameworks, identifying key challenges related to enforcement and implementation, and proposing actionable recommendations for improvement.

Understanding and improving e-privacy in Pakistan is crucial for several reasons. Effective e-privacy protections are essential for safeguarding individual rights in the digital age. As personal data becomes increasingly vulnerable to misuse, ensuring that individuals have control over their information and that it is securely protected is vital for maintaining trust in digital systems (Rehman, 2021a).

Additionally, aligning Pakistan's privacy practices with international standards can enhance the country's global digital standing and facilitate international digital interactions. In a globalized digital environment, adherence to international privacy norms is a matter of compliance and a competitive advantage that can influence Pakistan's position in the international digital economy.

Research Justification

The need for research on legal context of e-privacy in Pakistan is critical due to the country's rapid digital transformation. As internet usage and digital services expand, safeguarding personal data has become increasingly important. Pakistan's legislative framework, notably the Prevention of Electronic Crimes Act (PECA) 2016, represents a significant step towards addressing cybercrimes and data protection.

However, issues such as inadequate enforcement and its inability to fully address emerging privacy threats have challenged PECA's effectiveness. Evaluating the current legal framework and identifying necessary improvements is crucial for ensuring comprehensive e-privacy protections.

Socially, as digital technologies become more integrated into daily life, individuals in Pakistan face increased risks such as data breaches and identity theft. Research in this area is essential to raising public awareness about these risks and developing strategies for better personal data management. Enhancing public understanding of e-privacy can lead to more informed and proactive data protection behaviors.

Economically, aligning Pakistan's e-privacy practices with international standards is vital for fostering trust in digital transactions and attracting foreign investment. By improving e-privacy measures, Pakistan can strengthen its position in the global digital economy and enhance its appeal as a destination for international business and technological innovation.

Research Objectives

1. To explore the historical background of e-privacy in Pakistan.
2. To discuss the provincial laws of e-privacy in Pakistan.
3. To discuss the international laws on e-privacy.
4. To highlight the objectives of e-privacy in Pakistan.

Research Methodology

This study employed a systematic review methodology, with research objectives established accordingly. A comprehensive literature review was conducted (Komba & Lwoga, 2020). Research findings were categorized based on their content (Hiver et al., 2021; Petticrew & Roberts, 2006), and classified information was incorporated into the study by organizing it into headings (Gan et al., 2021; Pawson et al., 2005). The evaluation of classified information and titles formed the basis of the study (Page, 2021; Rahi, 2017), ensuring the integrity of the research subject and its contents (Egger et al., 2022; Victor, 2008).

Literature Review

As digital technologies increasingly permeate everyday life, e-privacy has emerged as a critical concern in Pakistan. E-privacy encompasses individuals' rights to protect their personal information in online spaces, and understanding its landscape is essential for safeguarding privacy in a rapidly digitizing society.

1. Legal frameworks

The Prevention of Electronic Crimes Act (PECA) 2016 primarily established the legal foundation for e-privacy in Pakistan. PECA was designed to combat cybercrime and enhance digital security while incorporating data protection and privacy provisions. However, critiques of PECA reveal that it lacks the comprehensiveness found in global data protection regulations, such as the European Union's General Data Protection Regulation (GDPR) (Mhajne & Henshaw, 2024).

The absence of robust regulations creates a significant gap in legal recourse for individuals facing data breaches or privacy violations. Additionally, the Constitution of Pakistan offers some protections under Article 14, which guarantees the right to privacy, but enforcement remains inconsistent and often ineffective in the digital context (Zaman et al., 2022).

2. Public awareness and perceptions

Public understanding of e-privacy rights is crucial for fostering a data protection culture. Research indicates that a large segment of the Pakistani population lacks awareness of their e-privacy rights and the risks associated with digital activities. Many users are unaware of the implications of sharing personal information on social media and the extent to which service providers collect data (Zahoor & Razi, 2021).

This lack of awareness is especially prevalent among marginalized communities with limited access to technology and education. Moreover, cultural attitudes towards privacy can influence individuals' willingness to protect their personal information, often leading them to prioritize convenience over privacy. It underscores the need for educational initiatives to enhance awareness of e-privacy issues and empower individuals to manage their personal data effectively (Akhtar, 2023).

3. Cybersecurity threats

The digital landscape in Pakistan is fraught with cybersecurity threats that jeopardize personal privacy. Data breaches, phishing attacks, and identity theft are common concerns among internet users. The prevalence of these threats is exacerbated by insufficient cybersecurity infrastructure and a general lack of awareness regarding data protection. Many organizations,

particularly small and medium enterprises, struggle to implement effective cybersecurity measures due to resource constraints (Al-Sartawi et al., 2024).

Additionally, government surveillance practices, often justified by national security interests, raise significant concerns about infringements on individual privacy rights. This tension between state security and personal privacy complicates the discourse on e-privacy in the country (Hasib, 2022).

4. Role of digital platforms

Digital platforms are central to the e-privacy landscape in Pakistan, as they collect enormous user data. Many users remain unaware of how their data is collected and utilized, resulting in a lack of informed consent. This situation is aggravated by the absence of stringent regulations requiring companies to disclose their data-handling practices transparently (Bhajaria, 2022).

Furthermore, the reliance on international tech companies raises questions about data sovereignty and local user protection, particularly when data is stored and processed outside Pakistan's jurisdiction. It necessitates comprehensive policies that not only regulate local practices but also address challenges posed by global digital ecosystems
(Peng et al., 2021).

Despite valuable insights from existing literature, several gaps that need further exploration remain. Empirical studies are needed to assess the effectiveness of current legal frameworks in protecting e-privacy rights. Evaluating the cybersecurity measures implemented across various sectors is also crucial to inform policy recommendations for enhancing data protection (Cinar & Vanberg, 2021; Gellers & Gunkel, 2023).

Historical Background of E-Privacy in Pakistan

The history of e-privacy in Pakistan reflects a progressive yet challenging journey in adapting to the rapid advancements in digital technology. The initial legal framework addressing electronic privacy concerns emerged with promulgating the Prevention of Electronic Crimes Act (PECA) in 2016. This landmark legislation was introduced to combat various cybercrimes, including unauthorized data access, cyber harassment, and data breaches. PECA marked a significant step forward in addressing digital privacy issues by providing a legal foundation for managing cybercrimes and protecting personal information in the online realm.

Before PECA, Pakistan's legal landscape lacked comprehensive regulations targeting electronic privacy. The country's approach to data protection was fragmented, relying on general legal provisions and ad hoc measures rather than a cohesive, dedicated framework. The introduction of PECA aimed to fill these gaps by criminalizing various forms of cybercrime and establishing mechanisms for addressing privacy breaches. Despite its advancements, PECA faced criticism for its limited scope, particularly in addressing emerging privacy challenges and international data protection concerns (Cubuk et al., 2022).

The evolving digital landscape highlighted gaps in PECA's coverage, necessitating further reforms and adaptations. As technology progressed, new privacy risks associated with big data, artificial intelligence, and other advanced technologies emerged, underscoring the need for ongoing legislative updates and enhanced enforcement mechanisms to keep pace with the digital age (Rehman, 2021b).

Provincial Laws of E-Privacy in Pakistan

In Pakistan, e-privacy regulation is primarily managed at the national level through the Prevention of Electronic Crimes Act (PECA) 2016. This national framework is complemented by provincial policies that indirectly contribute to the broader e-privacy landscape, although no provincial statutes specifically focus on e-privacy (Naimet al., 2023).

The provincial government has enacted the Sindh Information Technology Policy 2018 in Sindh. This policy aims to foster the development of the IT sector while emphasizing the importance of secure digital environments. Although it does not create specific e-privacy laws, the policy supports e-privacy objectives by focusing on cybersecurity and digital infrastructure protection. It aligns with national priorities by promoting secure practices and mitigating risks associated with digital data management (Al-Sartawi et al., 2024).

Similarly, the Punjab Information Technology Board (PITB) has spearheaded several initiatives to improve cybersecurity and data protection in Punjab. The PITB's efforts include developing and implementing systems designed to enhance digital

security and manage risks associated with cyber threats. While not constituting specific e-privacy legislation, these initiatives support the overarching goal of protecting personal data and ensuring secure digital practices in the province (Hasib, 2022).

The provincial IT policy in Khyber Pakhtunkhwa (KP) outlines strategies for advancing digital technology and enhancing cybersecurity. The policy addresses various IT infrastructure and data protection aspects, contributing indirectly to e-privacy. By focusing on secure digital environments and infrastructure development, the KP IT Policy complements national efforts to safeguard privacy in the digital realm.

Balochistan's IT Policy also reflects a commitment to improving digital infrastructure and promoting cybersecurity. Although it does not include specific provisions for e-privacy, the policy supports the broader objectives of digital security and privacy by emphasizing the importance of secure data management practice.

Overall, while no provincial laws in Pakistan specifically address e-privacy, provincial policies, and initiatives support the security and integrity of digital environments. These regional efforts work in tandem with the national legal framework established by PECA 2016, aiming to create a more robust and secure digital landscape across the country (Masood, 2023).

International Laws on E-privacy

International laws related to e-privacy have evolved significantly in response to the growing concerns about digital privacy and data protection (Lai-Ling & Zhu, 2024). The General Data Protection Regulation (GDPR) of the European Union, enacted in 2018, stands out as a landmark regulation in this area (Walters & Novak, 2021).

) GDPR provides a robust framework for data protection, emphasizing transparency, user consent, and the right to access and delete personal data. It has set a global benchmark for privacy standards and has influenced data protection laws in other jurisdictions (Roy & Bordoloi, 2023).

Another important international framework is the California Consumer Privacy Act (CCPA), enacted in 2020. The CCPA grants California residents broad rights over their personal data, including the right to know what data is collected, to opt out of data sales, and to request deletion of their data. This regulation has prompted similar privacy laws in other U.S. states and has significantly impacted privacy practices beyond California (Boukherouaa et al., 2021).

The Council of Europe's Convention 108 is also noteworthy. It updates the original Convention 108 and focuses on strengthening data protection standards globally. This treaty seeks to enhance cross-border cooperation and uphold privacy protections internationally (Elvy, 2021).

Objectives of E-Privacy in Pakistan

The objectives of e-privacy in Pakistan focus on enhancing the protection of personal information in the digital domain, addressing emerging privacy challenges, and ensuring that legal frameworks are practical and adaptable to technological advancements. One primary objective is safeguarding individuals' personal data from unauthorized access and misuse. It involves developing and enforcing robust mechanisms to prevent data breaches and cybercrimes, ensuring that individuals' digital privacy is respected and protected (Tariq et al., 2022).

Another key objective is to establish clear guidelines and standards for data protection that align with international best practices. It includes updating and refining existing laws, such as the Prevention of Electronic Crimes Act (PECA) 2016, to address the complexities of modern digital technologies and the global nature of data flows. By aligning with global privacy standards, Pakistan aims to enhance its regulatory framework and facilitate international cooperation on data protection matters (Cubuk et al., 2022).

Enhancing public awareness and understanding of e-privacy is also a crucial objective. Educating citizens about their digital rights, the risks associated with their online activities, and the available legal protections can empower individuals to take proactive measures to protect their personal information. Public awareness campaigns and educational initiatives are essential for fostering a culture of privacy and data protection (Elvy, 2021).

Furthermore, improving the enforcement of privacy laws is an objective that involves strengthening the capacity of law enforcement agencies and regulatory bodies. It includes providing adequate training, resources, and

technical expertise to implement and enforce e-privacy regulations (Rehman, 2021b).

Discussion

The history of e-privacy in Pakistan has evolved significantly, particularly with the introduction of the Prevention of Electronic Crimes Act (PECA) in 2016. This legislation aimed to combat cybercrimes and establish a legal framework for digital privacy. By addressing issues like unauthorized data access, cyber harassment, and data breaches, PECA represented a substantial advancement in protecting individuals' rights in the digital realm. However, it has faced criticism for its limited scope in addressing emerging challenges posed by new technologies such as big data and artificial intelligence.

In addition to national legislation, provincial policies play a vital role in shaping the e-privacy landscape in Pakistan. Various provinces have initiated efforts to enhance cybersecurity and promote secure digital practices. While these initiatives do not specifically address e-privacy, they contribute to a broader framework to ensure safe digital environments. For instance, policies in Sindh, Punjab, Khyber Pakhtunkhwa, and Balochistan reflect a commitment to improving digital infrastructure and security, aligning with national efforts.

International frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have set high standards for data protection. These regulations influence legal reforms in Pakistan, highlighting the need for alignment with global privacy standards. As digital technologies continue to evolve, Pakistan must refine its legal frameworks to safeguard personal data effectively.

Key objectives for e-privacy in Pakistan include enhancing personal information protection, establishing clear data protection guidelines, and increasing public awareness about digital rights. Strengthening enforcement mechanisms is also crucial, ensuring that law enforcement agencies have the capacity and resources to implement and uphold e-privacy regulations effectively. As the digital landscape becomes increasingly complex, a robust approach to e-privacy is essential for protecting individuals and fostering trust in the digital ecosystem.

Conclusion

The evolution of e-privacy in Pakistan highlights a journey of significant legislative milestones tempered by ongoing challenges. The Prevention n of Electronic Crimes Act (PECA), enacted in 2016, represents a cornerstone in the legal framework designed to combat cybercrimes and safeguard digital privacy. Addressing issues such as unauthorized data access and cyber harassment, PECA was a pivotal step toward establishing a more structured approach to digital privacy. Nevertheless, the Act's effectiveness has been compromised by its insufficient adaptability to rapid technological changes and emerging cyber threats, revealing the need for continuous legislative updates and enhancements.

The absence of specific e-privacy laws at the provincial level further complicates the regulatory landscape. While regional policies focus on IT infrastructure and cybersecurity, they do not directly address e-privacy concerns. This gap underscores the necessity for a more integrated approach that includes both national and provincial regulations tailored to address privacy issues comprehensively. Globally, frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) offer high data protection and privacy standards. Aligning Pak stan's regulatory framework with these international standards could significantly improve the country's data protection practices and facilitate better management of cross-border data flows.

To enhance e-privacy in Pakistan, it is crucial to modernize existing legislation, align with global privacy standards, increase public awareness about digital rights, and strengthen enforcement mechanisms. Addressing these areas with a comprehensive and proactive approach will be vital in developing a robust e-privacy framework, ensuring effective personal data protection amid an increasingly digital and interconnected world. Such advances are essential for fostering trust and security in the digital ecosystem, ultimately safeguarding individuals' rights and interests in Pakistan's evolving digital landscape.

Recommendations

1. Legislative reform: Regularly update the Prevention of Electronic Crimes Act (PECA) to

address emerging technologies and evolving cyber threats.

2. Provincial legislation: Develop and implement specific e-privacy laws at the provincial level to complement national regulations and address regional privacy concerns.

3.Alignment with international standards: Pakistan's data protection regulations should be aligned with international frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

4. Public awareness campaigns: Launch comprehensive public education campaigns to raise awareness about digital privacy rights and best practices for protecting personal information.

5. Strengthen e-enforcement: Enhance the capacity and resources of regulatory bodies to improve the enforcement of e-privacy laws and regulations.

6. Data protection mechanisms: Implement robust data protection mechanisms, including encryption and secure access controls, to safeguard personal information.

7. Privacy impact assessments: Mandate privacy impact assessments for new technologies and data processing activities to evaluate and mitigate potential privacy risks.

8. Cross-border data management: Establish clear guidelines for managing and transferring personal data across borders to ensure compliance with global privacy standards.

9. Stakeholder collaboration: Collaborate with government agencies, private sector entities, and civil society organizations to develop and implement effective e-privacy policies.

10. Technical training and capacity building: Provide ongoing training and capacity building for law enforcement and regulatory personnel to enhance their technical expertise in handling e-privacy issues.

Research Limitations

E-privacy in Pakistan faces several limitations that impact the depth and breadth of analysis. Firstly, the rapidly evolving nature of technology and cyber threats poses a challenge, as existing laws and regulations often lag behind technological advancements. This dynamic environment makes it difficult to evaluate the effectiveness of current legal frameworks and predict future needs. The constant evolution of digital technologies and cyber threats means that legislative and regulatory measures quickly become outdated, creating a persistent gap between legal provisions and actual technological realities.

Secondly, the lack of comprehensive and specific provincial e-privacy laws results in fragmented regulatory coverage, complicating efforts to assess the overall impact on digital privacy across different regions. This regulatory gap hinders a holistic understanding of the privacy landscape. While there are national laws such as the Prevention of Electronic Crimes Act (PECA) 2016, the absence of region-specific regulations means that privacy concerns are not uniformly addressed, leading to inconsistencies in protecting personal data.

Additionally, there is limited empirical data and research on implementing and enforcing e-privacy laws in Pakistan. The scarcity of detailed case studies and statistical analyses restricts the ability to draw conclusive insights about the efficacy of existing measures. Without comprehensive empirical research, it is challenging to assess how well current laws are enforced and to identify specific areas where improvements are needed.

Finally, cultural and social factors, including varying levels of public awareness and differing attitudes toward privacy, further complicate the research. These factors influence the effectiveness of privacy policies and the extent to which they are adopted and enforced, adding another layer of complexity to the analysis. Public perceptions and attitudes toward privacy can significantly impact how privacy measures are implemented and adhered to, highlighting the need for culturally sensitive approaches in policy formulation and enforcement.

Research Implications

The e-privacy in Pakistan has several important implications for policy, practice, and future research. Firstly, findings underscore the urgent need for legislative reform to keep pace with rapid technological advancements and emerging cyber threats. Policymakers must prioritize regular updates to the Prevention of Electronic Crimes Act (PECA) and consider developing specific e-privacy laws at the provincial level to ensure comprehensive protection across the country. The fast-paced evolution of digital technologies necessitates a dynamic legal framework that can

address new challenges effectively, ensuring that the country's legal infrastructure is not left behind as technology progresses.

Secondly, the research highlights the necessity for Pakistan to align its data protection regulations with international standards, such as the General Data Protection Regulation (GDPR). This alignment can enhance the country's data protection practices, facilitate international data transfers, and improve compliance with global privacy norms. By adopting international best practices, Pakistan can improve its regulatory environment, foster greater international trust, and attract foreign investment by demonstrating a commitment to high data protection standards.

The study also implies a need for increased public awareness and education regarding digital privacy rights. Effective awareness campaigns can empower individuals to better manage their personal information and understand their rights under existing laws. Public education is crucial for creating a culture of privacy and ensuring that citizens are informed about how to protect their digital identities in an increasingly connected world.

Moreover, strengthening enforcement mechanisms and providing technical training for regulatory personnel are critical for improving the implementation of e-privacy laws. Enhancing the capacity of law enforcement and regulatory bodies can ensure that privacy laws are enforced effectively and that violations are addressed promptly. It includes investing in developing technical expertise and resources to handle sophisticated cyber threats and privacy breaches.

Future Research Directions

Future research on e-privacy in Pakistan should focus on several key areas to address existing gaps and advance understanding of digital privacy issues. Firstly, the research should examine the effectiveness of current legislation, particularly the Prevention of Electronic Crimes Act (PECA), in addressing emerging technological threats. Studies can evaluate how well PECA adapts to rapid technological changes and identify necessary legislative updates to enhance its relevance and efficacy.

Secondly, empirical research is needed on the implementation and enforcement of e-privacy laws. Investigating real-world case studies, including the challenges faced by regulatory bodies and the effectiveness of enforcement mechanisms, can provide valuable insights into the practical application of e-privacy regulations. Thirdly, comparative studies between Pakistan and other countries with advanced e-privacy frameworks, such as those adhering to the General Data Protection Regulation (GDPR), could offer useful perspectives on best practices and regulatory approaches. These comparisons can inform potential improvements in Pakistan's regulatory landscape.

Additionally, future research should focus on public perception and awareness of e-privacy issues. Understanding how different population segments perceive privacy risks and their knowledge of digital privacy rights can help design more effective awareness campaigns and educational initiatives. Lastly, research should explore the impact of cultural and social factors on e-privacy practices in Pakistan. Examining how cultural attitudes toward privacy influence the adoption and effectiveness of e-privacy measures can provide a more nuanced understanding of privacy challenges and inform targeted policy interventions.

The manuscript has not been previously published elsewhere and is not being considered by any other journal. The authors read and approved the final version of the respective manuscript.

References

Akhtar, S. (2023). *Assessing the cybercrime legislation in Pakistan: A comparative study of European Union and Pakistani cybercrime laws.* SSRN. https://ssrn.com/abstract=4555751

Al-Sartawi, A. M. A. M., Al-Qudah, A. A., & Shihadeh, S. (Eds.). (2024). *Artificial intelligence-augmented digital twins: Transforming industrial operations for innovation and sustainability*. Springer Nature. https://doi.org/10.1007/978-3-031-43490-7

Bhajaria, N. (2022). *Data privacy: A runbook for engineers*. Simon and Schuster. https://www.google.com.pk/books/edition/Data_Privacy/47FYEAAAQBAJ?hl=en&gbpv=0

Boukherouaa, E. B., Shabsigh, M. G., AlAjmi, K., Deodoro, J., Farias, A., Iskender, E. S., & RaviKumar, R. (2021). *Powering the digital economy: Opportunities and risks of artificial intelligence in finance.* International Monetary Fund. https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/10/21/Powering-the-Digital-Economy-Opportunities-and-Risks-of-Artificial-Intelligence-in-Finance-494717

Burri, M. (Ed.). (2021). *Data flows and global trade law. Tracing developments in preferential trade agreements.* SSRN. https://ssrn.com/abstract=3482472

Cinar, O. H., & Vanberg, A. D. (Ed.). (2021). *The right to privacy revisited: Different international perspectives.* Routledge. https://doi.org/10.4324/9781003252191

Cubuk, E. B., Zeren, H. E., & Demirdoven, B. (2023). The role of data governance in cybersecurity for e-municipal services: Implications from the case of Turkey. In S. Saeed, A. Almuhaideb, N. Kumar, N. Zaman, & Y. Zikria (Eds.), *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications* (pp. 410-425). IGI Global. https://doi.org/10.4018/978-1-6684-5284- 4.ch020

Egger, M., Higgins, J. P., & Smith, G. D. (Eds.). (2022). *Systematic reviews in health research: Meta-analysis in context.* John Wiley & Sons.

Elvy, S. A. (2021). *A commercial law of privacy and security for the internet of things.* Cambridge University Press. https://www.cambridge.org/us/universitypress/subjects/law/e-commerce-law/commercial-law-privacy-and-security-internet-things?format=HB&isbn=9781108482035

Gan, J., Xie, L., Peng, G., Xie, J., Chen, Y., & Yu, Q. (2021). Systematic review on modification methods of dietary fiber. *Food Hydrocolloids, 119,* 106872. https://doi.org/10.1016/j.foodhyd.2021.106872

Gellers, J. C., & Gunkel, D. (2023). Artificial intelligence and international human rights law: Implications for humans and technology in the 21st century and beyond. In A. Zwitter and O.J. Gstrein (Eds.), *Handbook on the Politics and Governance of Big Data and Artificial Intelligence* (pp. 430-455). SSRN. https://ssrn.com/abstract=4072896

Hasib, M. (2022). *Cybersecurity leadership: Powering the modern organization.* Tomorrow's Strategy Today. https://www.google.com.pk/books/edition/Cybersecurity_Leadership/Id5-EAAAQBAJ?hl=en&gbpv=0

Hiver, P., Al-Hoorie, A. H., Vitta, J. P., & Wu, J. (2021). Engagement in language learning: A systematic review of 20 years of research methods and definitions. *Language Teaching Research,* 13621688211001289. https://doi.org/10.1177/13621688211001289

Jahankhani, H., Jamal, A., & Lawson, S. (Eds.). (2021). *Cybersecurity, privacy and freedom protection in the connected world: Proceedings of the 13th International Conference on global security, safety and sustainability.* Springer Nature. https://doi.org/10.1007/978-3-030-68534-8

Jenkinson, A. (2022). *Ransomware and cybercrime.* CRC Press. https://doi.org/10.1201/9781003278214

Komba, M. M., & Lwoga, E. T. (2020). Systematic review as a research method in library and information science. 10.4018/978-1-7998-1471-9.ch005.

Lai-Ling, C., & Zhu, G. (2024). *Personal data (Privacy) law in Hong Kong: A practical guide on compliance (3rd Edition).* City University of Hong Kong Press. https://www.cityu.edu.hk/upress/personal-data-privacy-law-in-hong-kong-3rd-edition

Masood, A. (2023). *Effectiveness of Pakistani cyber laws in mitigating cybercrime. Preserving freedom of expression and privacy in the digital age.* GRIN Verlag. https://www.grin.com/document/1357075

Mhajne, A., & Henshaw, A. (2024). *Critical perspectives on cybersecurity: Feminist and postcolonial interventions. Oxford studies in gender and international relations.* Oxford University Press. https://search.library.yale.edu/catalog/b1903669

Naim, A., Malik, P. K., & Zaidi, F. A. (2023). *Fraud prevention, confidentiality, and data security for modern businesses*. IGI Global. 10.4018/978-1-6684-6581-3

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

Page, X., Knijnenburg, B. P., Wisniewski, P., Lipford, H. R., Proferes, N., & Romano, J. (2022). *Modern socio-technical perspectives on privacy*. Springer Nature. https://doi.org/10.1007/978-3-030-82786-1

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), 21-34. 10.1258/1355819054308530

Petticrew, M., & Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide.* Blackwell Publishing. 10.1002/9780470754887

Peng, S., Yi, Lin, C. F., & Streinz, T. (Eds.). (2021). *Artificial intelligence and international economic law: Disruption, regulation, and reconfiguration.* Cambridge University Press. https://doi.org/10.1017/9781108954006

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues, and instruments development. *International Journal of Economics & Management Sciences, 6*(2). 10.4172/2162-6359.1000403

Rehman, T. U. (2021a). Cybersecurity for e-banking and e-commerce in Pakistan: Emerging digital challenges and opportunities. In K. Sandhu (Ed.), *Handbook of Research on Advancing Cybersecurity for Digital Transformation* (pp. 163-180). IGI Global. https://doi.org/10.4018/978-1-7998-6975-7.ch009

Rehman, T. U. (2021b). *E-banking and e-commerce in Pakistan: An analytical approach.* Eliva Press. https://www.google.com.pk/books/edition/E_Banking_and_E_Commerce_in_Pakistan/85spzgEACAAJ?hl=en

Roy, N. D., & Bordoloi., P. (2023). *The cyber law handbook: Bridging the digital legal landscape.* Authors Click Publishing. https://www.amazon.in/Cyber-Law-Handbook-Bridging-Landscape/dp/8119368134

Tariq, M. I., Balas, V. E., & Tayyaba, S. (Eds.). (2022). *Security and privacy trends in cloud computing and big data.* CRC Press. https://www.routledge.com/Security-and-Privacy-Trends-in-Cloud-Computing-and-Big-Data/ImranTariq-Balas-Tayyaba/p/book/9781003107286

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

Walters, R. (2023). *Cybersecurity and Data Laws of the Commonwealth: International Trade, Investment and Arbitration.* Springer Nature. https://doi.org/10.1007/978-981-99-3935-0

Walters, R., & Novak, M. (2021). *Cyber security, artificial intelligence, Data protection & the law.* Springer Nature. https://doi.org/10.1007/978-981-16-1665-5

Zahoor, R., & Razi, N. (2021). Analyzing the cyberspace laws to protect data privacy in Pakistan. *Law, State and Telecommunications Review*, 13(2), 42-55. https://doi.org/10.26512/lstr.v13i2.35977

Zaman, N., Shah, I. A., & Rajper, S. (2022*). Cybersecurity measures for e-government frameworks.* IGI Global. https://www.igi-global.com/book/cybersecurity- measures-government-frameworks/279863