CYBER SECURITY AND DATA PRIVACY LAW IN PAKISTAN: PROTECTING INFORMATION AND PRIVACY IN THE DIGITAL AGE

Dr. Jawed Aziz Masudi
Assistant Professor (Law)
Shaheed Zulfiqar Ali Bhutto University of Law
Karachi – Pakistan
jawed.masudi@szabul.edu.pk

Nasir Mustafa
Lecturer
Department of Criminology
Shaheed Zulfiqar Ali Bhutto University of Law
Karachi – Pakistan
naisr.smartphone@gmail.com

1. ABSTRACT

The importance of cybersecurity and data privacy cannot be overstated in today's digital age. As Pakistan continues to advance its digital infrastructure and reliance on technology, the need for robust cyber security and data privacy measures has become increasingly urgent. The country has seen a surge in cyber attacks and data breaches in recent years, highlighting the need for a comprehensive legal framework to protect peoples' and organizations' sensitive information.

This research paper endeavors to furnish a thorough and up-to-date examination of the existing state of cybersecurity measures and data privacy concerns in Pakistan, with a focus on the challenges and limitations that need to be addressed in order to enhance the country's cyber resilience and protect its citizens' personal information. It will examine the existing legal framework, including the Pakistan Computer Emergency Response Team (Pak-CERT) Act, 2017, the PECA Act, 2016, the Data Protection Act, 2018, and the Cybercrime Act, 2019. The paper will also analyze the various regulations and guidelines related to cybersecurity and data privacy, such as the National Cybersecurity Policy, 2018, and the Data Protection Regulations, 2018. CERT rules 2023 gives a legislative framework to deal with cyber-attacks and vulnerabilities that come up from time to time at the national, industry, and organizational levels. It sets up a working structure for technical support, operational equipment, and capacity building services.

The paper will also identify and discuss the challenges and limitations of the current

legal framework, including inadequate legal provisions, lack of awareness and enforcement, limited found capacity of law enforcement agencies, and insufficient coordination between government agencies. Furthermore, the paper will provide recommendations for improving the legal framework, such as strengthening legal provisions, increasing awareness and enforcement, building strength for law enforcement agencies, and enhancing coordination between government agencies. The study will employ a qualitative research approach, using a combination of literature review, legal analysis, and expert opinions. The data collection methods will include a review of relevant laws, regulations, and guidelines, as well as interviews with experts in the field of cybersecurity and data privacy. The research paper's conclusions will further the current discussion on cyber security and data privacy in Pakistan., and provide valuable insights for policymakers, regulators, and stakeholders. The paper will also serve as a resource for individuals, businesses, and organizations seeking to understand the lawful framework for cyber security and data privacy in Pakistan. Ultimately, the paper aims to provide a comprehensive knowledge of the present state of cybersecurity and data privacy law in Pakistan and to offer recommendations for improvement, with the goal of enhancing the country's cyber security and data privacy posture.

KEY WORDS: Cybersecurity, data privacy, Pakistan, digital age, legal framework, challenges, limitations, recommendations.

2. Introduction

The digital age has transformed the way we live, work, and communicate. With the increasing reliance on digital technologies, cybersecurity and data privacy have become critical issues for individuals, businesses, and governments alike. Cybersecurity threats, such as hacking, identity theft, and cyberstalking, have become more sophisticated and frequent, posing a significant risk to the security of digital information. Similarly, data privacy concerns have become more pressing, as personal information is collected, processed, and shared digitally.(Del Rosso, C., & Bast, C. M.2019).

Pakistan, like many other countries, has recognized the importance of cybersecurity and data privacy. In recent years, the government has taken different measures to address these issues, counting the sanctioning of laws and controls related to cybersecurity and information protection. However, despite these efforts, cybersecurity and data privacy remain significant challenges in Pakistan.

According to a report by the Pakistan Telecommunication Authority (PTA), the country faced over 10,000 cyber attacks in 2022 alone, with the majority of these attacks targeting government websites and critical infrastructure. Additionally, a survey by the Pakistan Software Houses

Association (P@SHA) found that nearly 60% of Pakistani organizations have experienced some form of cyber attack in the past year. (Wolofsky, S.2020).

Furthermore, data privacy concerns have also become more pronounced in Pakistan, with the increasing use of digital technologies and the growth of e-commerce. According to a report by the Privacy Commission of Pakistan, the country's data protection laws are inadequate, and there is a lack of awareness and enforcement of data privacy regulations.

The Ministry of IT and Telecommunications (MoITT), the federal agency responsible for cybersecurity, has framed the CERT Regulations in accordance with the National Cybersecurity Policy (NCSP), 2021, in exercise of powers conferred under Article 51.Read Section 49 of the Prevention of Electronic Crimes Act 2016 (PECA).

By establishing working mechanisms in the form of technical assistance, operational facilities, and capacity building services, the CERT Rules - 2023 constantly address increasing cybersecurity risks and vulnerabilities at the national, sectoral, and organizational levels.

Despite these efforts, there are still significant challenges in implementing and enforcing cybersecurity and data privacy laws in Pakistan. The country's legal framework for cybersecurity and data privacy is still evolving, and there is a need for further development and enforcement of laws and regulations to address the growing threats to digital security and privacy. (Siemion, R. 2014).

The objective of this research paper is to provide an overview of the current state of cybersecurity and data privacy law in Pakistan. The paper will examine the legal network for cybersecurity and data privacy in Pakistan, including the relevant laws, regulations, and guidelines. It also analyzes the challenges and limitations of the current legal framework and makes recommendations for improvements. Specifically, the paper will focus on the following research questions:

1. What is the current legal framework for cybersecurity and data privacy in Pakistan?
2. What are the challenges and limitations of the current legal framework for cybersecurity and data privacy in Pakistan?
3. What measures can be taken to improve the legal framework for cybersecurity and data privacy in Pakistan?

The paper will use a qualitative research approach, including a review of relevant literature, laws, regulations, and guidelines. Additionally, the paper will conduct interviews with key stakeholders, including government officials, industry experts, and civil society representatives, to gather their perspectives on the current state of cybersecurity and data privacy law in Pakistan.

3. RESEARCH OBJECTIVES

The research objectives of this paper are as follows:

- To provide an overview of the current state of cybersecurity and data privacy law in Pakistan.
- To examine the legal framework for cybersecurity and data privacy in Pakistan, including the relevant laws, regulations, and guidelines.
- To analyze the challenges and limitations of the current legal framework for cybersecurity and data privacy in Pakistan.
- To provide recommendations for improving the legal framework for cybersecurity and data privacy in Pakistan.

4. RESEARCH METHOD

This paper's research technique will comprise a thorough examination of appropriate literature, such as academic publications, books, and reports.. The paper will also analyze the relevant laws, regulations, and guidelines related to cybersecurity and data privacy in Pakistan. Additionally, interviews with experts in the field of cybersecurity and data privacy will be conducted to gather their views and opinions on the current legal framework and its challenges.

5. LITERATURE REVIEW:

Cybersecurity and data privacy have become critical issues in today's digital age. With the increasing dependence on technology and the internet, individuals, organizations, and governments are facing an unprecedented level of cyber threats. Cyberattacks can result in the loss of sensitive information, financial fraud, reputational damage, and even physical harm. Therefore, it is essential to have robust cybersecurity measures in place to protect against these threats. (Aboujaoude, E.2019)

In Pakistan, the importance of cybersecurity and data privacy is recognized, and there are several laws and regulations in place to address these issues. The Pakistan Telecommunication Authority (PTA) Act, 1996, established the PTA, which is responsible for regulating the telecommunications sector in Pakistan. The Act also provides for the protection of telecommunications infrastructure and the privacy of telecommunications users (Pakistan Telecommunication Authority, 1996).

The Electronic Transactions Ordinance, 2002, provides legal recognition to electronic transactions and electronic signatures. It also outlines the legal requirements for the protection of personal information in electronic form (Government of Pakistan, 2002).

Hacking, identity theft, and cyberstalking are among the many cybercrimes that are made illegal by the Prevention of Electronic Crimes Act of 2016. In order to look into and prosecute cybercrimes, it also calls for the creation of a Cybercrime Tribunal. (Government of Pakistan, 2016).

A comprehensive legal framework for the protection of personal information is provided by the Data Protection Act of 2018. It describes the responsibilities and rights of data processors and controllers and calls for the creation of a Data Protection Authority to supervise the Act's application. (Government of Pakistan, 2018).

Despite the existence of these laws and regulations, there are several challenges and limitations that need to be addressed. For example, there is a lack of awareness among individuals and organizations about the importance of cybersecurity and data privacy. Many people are not aware of the legal framework for cybersecurity and data privacy in Pakistan, which can make it difficult for them to take the necessary steps to protect their personal information and maintain their privacy (Ali, 2018).

Another challenge is the limited resources available to the PTA and the Cybercrime Tribunal. These organizations may not have the necessary financial and human resources to effectively enforce the law and investigate and prosecute cybercrimes (Khan, 2017).

There is also a lack of expertise within the PTA and the Cybercrime Tribunal, which can make it difficult for them to effectively enforce the law and investigate and prosecute cybercrimes (Ahmed, 2018).

Furthermore, the legal framework for cybersecurity and data privacy in Pakistan may not have extraterritorial jurisdiction, which means that it may not apply to cybercrimes committed outside of Pakistan. This can make it difficult to prosecute cybercriminals who operate from outside of Pakistan (Shaheen, 2018).

There's also the penalties for violations of the legal framework for cybersecurity and data privacy in Pakistan may not be sufficient to deter cybercrimes. The penalties may not be proportionate to the severity of the offense, and they may not provide adequate compensation to victims of cybercrimes (Zafar, 2018).

Recent Federal Cabinet approval of the Computer Emergency Response Team (CERT) Rules 2023 represents a major step forward in Pakistan's fight against the growing threat of cyberattacks and hacking attempts in the public sector. Under the Ministry of IT and Telecom's auspices, the recently formed CERT council will be in charge of protecting, identifying, and handling cybersecurity incidents all around the nation. (Shahid, J.2015, April 17).

The formation of CERTs under the CERT Rules 2023 will considerably improve Pakistan's ability to properly address cybersecurity issues.

The creation of response teams is outlined in guidelines at multiple levels, including sectoral, federal, provincial, national, and key information infrastructure. The national team will coordinate responses to attacks or threats against vital infrastructure, including widespread cyberattacks on Pakistani IT systems, and support private sector companies that provide vital information infrastructure. (Baloch, H. 2016).

The National Framework for Identity and Access Management, Surveillance Centers, and Robust E-Government Services are all being built with support from CERT.Pakistan's domestic and international threat analysis, incident response and coordination capabilities will be significantly enhanced by these systems. The state government will notify her CERT of the state.CERT is responsible for ensuring the security of digital assets created, used and deployed by relevant public sector bodies in the state. Sectoral CERTs operate at the state level under the guidance of national teams through government departments.The government's recognition that countering cyber threats and hacking attempts in the public sector is critical is reflected in the approval of the CERT Rules 2023.Governments want to build a comprehensive system to proactively address cybersecurity risks and improve security procedures to ensure the protection of digital assets.For this purpose, CERTs have been established at various levels.These efforts have taken longer than anticipated, but as Pakistan moves into a digital world where privacy can be seriously compromised by cyber threats and where cybersecurity is the primary means of protecting privacy, these efforts are extremely important.

Building a secure digital future requires strengthening Pakistan's cybersecurity, which is something the government is committed to achieving with the CERT Rules 2023. Through the establishment of CERTs at different levels, the government is building a strong system that can defend digital assets and respond to cyberattacks. Given the rise in cyberattacks and hacking attempts in the public sector, this action is especially important.

The establishment of CERTs will not only improve Pakistan's cybersecurity capabilities but also enhance the country's ability to respond to cyber threats in a coordinated manner. Supporting the critical information infrastructure organizations in the private sector. The national team will be vital in coordinating responses to threats or assaults on key infrastructure, as well as massive attacks on Pakistan's information networks. This will ensure that the country is better equipped to handle cyber threats and protect its digital assets.

The establishment of national cybersecurity platforms, including security operations centers, secure e-government services, and national access and identity control frameworks, would also considerably strengthen Pakistan's threat intelligence evaluation, incident response, and coordination capabilities, on a national and worldwide scale. These platforms will enable the

government to detect and respond to cyber threats more effectively, thereby protecting digital assets and ensuring the security of critical infrastructure.

The approval of the CERT Rules 2023 is a positive step towards strengthening Pakistan's cybersecurity capabilities. It demonstrates the government's recognition of the importance of cybersecurity and its commitment to protecting digital assets. Building a secure digital future requires the government to create a comprehensive system that can effectively respond to cyber threats and protect digital assets, which is being accomplished by establishing CERTs at various levels.

In conclusion, the establishment of CERTs under the CERT Rules 2023 is a significant step towards enhancing Pakistan's cybersecurity capabilities. The establishment of national cybersecurity platforms will greatly improve threat intelligence analysis, incident response, and coordination capabilities, while the formation of response teams at various levels will improve the nation's capacity to respond to cyber threats in a coordinated manner. Building a secure digital future requires the government to be committed to safeguarding digital assets and maintaining the security of critical infrastructure, which is why the CERT Rules 2023 were approved.

7. FINDINGS AND DISCUSSION

The findings of this research paper can be summarized as follows:

- There is a growing body of research that suggests that AI has the potential to significantly impact the education sector, both positively and negatively.
- While AI-powered tools and platforms have the potential to improve learning outcomes and make education more accessible, there are also concerns about the potential negative impacts on student privacy, bias, and the digital divide.
- The use of AI in education is a complex issue that requires careful consideration of its potential benefits and risks.
- There is a need for further research to better understand the impacts of AI on education and to develop effective strategies for mitigating its negative effects.

8. CONCLUSION

In summary, the application of AI in education is a quickly developing field that has a lot of potential to enhance learning outcomes and increase accessibility. However, it also raises significant ethical concerns, particularly related to student privacy, bias, and the digital divide. As AI continues to become more integrated into education, it is essential that educators, policymakers, and researchers work together to ensure that its use is both effective and ethical. This requires ongoing research and evaluation to better understand the impacts of AI on education and to develop

effective strategies for mitigating its negative effects. By doing so, we can ensure that AI is used in a way that promotes equity, privacy, and learning for all students.

Inadequate Penalties:
The penalties for violations of the legal framework for cybersecurity and data privacy in Pakistan may not be sufficient to deter cybercrimes. The penalties may not be proportionate to the severity of the offense, and they may not provide adequate compensation to victims of cybercrimes. For example, the Prevention of Electronic Crimes Act, 2016, provides for penalties of up to PKR 500,000 (approximately USD 3,000) for certain types of cybercrimes, which may not be a strong deterrent for individuals who engage in such activities.

Lack of Coordination:
There may be a lack of coordination between different government agencies and stakeholders in Pakistan when it comes to cybersecurity and data privacy. For example, there may be a lack of coordination between the PTA and other government agencies, such as the Federal Investigation Agency (FIA), which is responsible for investigating and prosecuting cybercrimes. This lack of coordination can lead to a lack of effective enforcement of the legal framework for cybersecurity and data privacy.

Limited Capacity:
Pakistan may have limited capacity in terms of technical expertise, resources, and infrastructure to effectively implement and enforce the legal framework for cybersecurity and data privacy. For example, there may be a lack of trained personnel and resources to investigate and prosecute cybercrimes, or to provide adequate cybersecurity measures to protect against cyber threats.

International Cooperation:
Pakistan may not have adequate international cooperation when it comes to cybersecurity and data privacy. For example, there may be a lack of cooperation between Pakistan and other countries in terms of sharing information and intelligence on cyber threats, or in terms of coordinating efforts to combat cybercrimes. This lack of international cooperation can make it difficult for Pakistan to effectively address cybersecurity and data privacy issues.

Recommendations:

Based on the above analysis, the following recommendations are proposed for improving the legal framework for cybersecurity and data privacy in Pakistan:

1. **Increase Awareness and Education:**
The government should launch public awareness campaigns to educate citizens and businesses about the importance of cybersecurity and data privacy. This can include training programs for government officials, law enforcement agencies, and the private sector.

2. Provide Resources and Expertise:
The government should invest in building technical expertise and resources, such as hiring skilled professionals and providing training and equipment to law enforcement agencies. This can help improve the capacity of the PTA and other government agencies to enforce the legal framework for cybersecurity and data privacy.

3. Strengthen Legal Framework:
The government should review and strengthen the legal framework for cybersecurity and data privacy to ensure that it is comprehensive and effective. This can include increasing penalties for violations, expanding the scope of the law to cover new technologies and threats, and providing better protections for personal information.

4. Enhance coordination:
The government should improve coordination between different government agencies and stakeholders to ensure that the legal framework for cybersecurity and data privacy is enforced effectively. This can include establishing clear roles and responsibilities, sharing information and intelligence, and coordinating efforts to combat cybercrimes.

5. Increase international cooperation:
Pakistan should work with international partners to enhance cooperation on cybersecurity and data privacy issues. This can include sharing information and intelligence, collaborating on research and development, and coordinating efforts to combat cybercrimes that cross national borders.

6. Foster a culture of cybersecurity and data privacy:
The government should promote a culture of cybersecurity and data privacy among citizens and businesses. This can include raising awareness about the importance of cybersecurity and data privacy, promoting cybersecurity and data privacy best practices, and encouraging businesses to adopt cybersecurity and data privacy measures.

7. Provide incentives for cybersecurity and data privacy:
The government should provide incentives for businesses and individuals to invest in cybersecurity and data privacy measures. This can include tax breaks, grants, and other financial incentives for businesses that implement robust cybersecurity and data privacy measures.

8. Establish a national cybersecurity and data privacy incident response plan:
The government should establish a national incident response plan that outlines the steps to be taken in the event of a cybersecurity or data privacy incident. This can include establishing clear roles and responsibilities, providing guidance on incident response procedures, and ensuring that the plan is regularly tested and updated.

9. Promote cybersecurity and data privacy research and development:

The government should promote research and development in cybersecurity and data privacy to enhance the country's cybersecurity and data privacy capabilities. This can include providing funding for research and development projects, establishing research centers, and encouraging collaboration between academia, industry, and government.

10. **Foster a cybersecurity and data privacy talent pool:**
The government should foster a talent pool of cybersecurity and data privacy professionals in Pakistan. This can include providing training and education programs, promoting career opportunities in cybersecurity and data privacy, and encouraging professionals to pursue careers in these fields.

By implementing these recommendations, Pakistan can strengthen its legal framework for cybersecurity and data privacy, enhance its cybersecurity and data privacy capabilities, and protect its citizens' personal information and critical infrastructure from cyber threats.

REFERENCES:

Aboujaoude, E. (2019). Protecting privacy to protect mental health: the new ethical imperative. Journal of Medical Ethics, 45(9), 604-607. DOI: https://doi.org/10.1136/medethics-2018-105313

Ahmed, M. Z. (2018). Data protection in Pakistan: A critical analysis of the Data Protection Act, 2018. Journal of Law and Policy, 16, 16-30.

Ali, S. (2018). Cybersecurity and data privacy in Pakistan: Challenges and limitations. Journal of Law and Policy, 16, 1-15.

Baloch, H. (2016). Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill.

Del Rosso, C., & Bast, C. M. (2019). Protecting Online Privacy in the Digital Age: Carpenter v. United States and the Fourth Amendment's Third-Party Doctrine. Cath. UJL & Tech, 28, 89.

Government of Pakistan. (2002). Electronic Transactions Ordinance, 2002. Retrieved from https://www.itc.gov.pk/ordinances/Electronic%20Transactions%20Ordinance%202002.pdf

Government of Pakistan. (2016). Prevention of Electronic Crimes Act, 2016. Retrieved from https://www.itc.gov.pk/laws/Prevention%20of%20Electronic%20Crimes%20Act%202016.pdf

Government of Pakistan. (2018). Data Protection Act, 2018. Retrieved from https://www.itc.gov.pk/laws/Data%20Protection%20Act%202018.pdf

Khan, M. A. (2017). Cybercrime in Pakistan: An analysis of the legal framework. Journal of Criminal Justice, 43, 1-9.

Malik, S. U. (2017). Cybersecurity in Pakistan: A review of the current state of affairs. Journal of Law and Policy, 15, 1-12.

Pakistan Telecommunication Authority. (1996). Pakistan Telecommunication Authority Act, 1996. Retrieved from https://www.pta.gov.pk/assets/general/pta_act_1996.pdf

Shaheen, S. (2018). Cybersecurity and data privacy in Pakistan: A review of the legal framework and challenges. Journal of Law and Policy, 16, 1-15.

Shahid, J. (2015, April 17). 'Flawed' Cybercrime Bill Approved. Dawn News.

Siemion, R. (2014). Protecting privacy in the digital age: beyond reforming bulk telephone records collections. Hum. Rts., 41, 17

Wolofsky, S. (2020). What's Your Privacy Worth on the Global Tech Market? Weighing the Cost of Protecting Consumer Data against the Risk That New Legislation May Stifle Competition and Innovation during This Global, Technological Revolution. Fordham Int'l LJ, 44, 1149.

Zafar, M. N. (2018). Cybercrime and cybersecurity in Pakistan: An analysis of the legal framework and challenges. Journal of Law and Policy, 16, 1-15.