Comparative Public Law and Cyber Law Governance: A Study of Cybercrime Legislation in India, Bangladesh and Pakistan

Mohammad Tarek Hasan[1], Prof(Dr) SK Bose[2]
[1]LL.M Student, [2]Professor
[1,2]School of Law, Manav Rachna University, India

Abstract: This research article provides a comparative study of cybercrime legislation within the frameworks of public law in India, Bangladesh, and Pakistan. These South Asian countries have experienced rapid technological growth, leading to an increased dependency on digital platforms, which has simultaneously opened new avenues for cybercrime, including data theft, online fraud, hacking, and cyber terrorism. As a result, each country has developed distinct legal responses to combat these threats, notably through the Information Technology Act (2000) in India, the Digital Security Act (2018) in Bangladesh, and the Prevention of Electronic Crimes Act (2016) in Pakistan. While these laws share common objectives of safeguarding digital integrity and security, they differ considerably in scope, enforcement mechanisms, and adherence to public law principles like transparency, accountability, and protection of fundamental rights. This study explores the unique legal and socio-political factors shaping each country's cybercrime legislation, examining how well these laws address emerging cyber threats and protect individual freedoms. The article critically assesses each country's approach to integrating international standards and balancing national security concerns with individual rights, particularly regarding freedom of expression and privacy. Additionally, it investigates the role of comparative public law in enhancing cyber governance and cross-border cooperation within the region, identifying significant gaps in harmonization that hinder effective collaboration against transnational cybercrime. Through an analysis of legislative effectiveness, enforcement challenges, and human rights considerations, the article provides insights into the potential for a unified approach to cyber governance in South Asia. The findings underscore the importance of establishing robust, rights- based frameworks for cyber law governance that align with global standards. Recommendations for improving these frameworks highlight the need for enhanced regional cooperation, a commitment to international legal norms, and reforms that ensure the protection of digital rights and effective cybercrime prevention across India, Bangladesh, and Pakistan.

Keywords: Cyber Law, Cybercrime Legislation, Comparative Public Law, Cyber security Governance, Digital Security Act, Information Technology Act, Prevention of Electronic Crimes Act, South Asia, Legal Frameworks, Cross-border Cooperation, Data Privacy, Freedom of Expression, International Standards, Cyber Threats, Human Rights in Cyberspace

Introduction : The digital transformation in South Asia has brought significant economic, social, and technological advances, with countries like India, Bangladesh, and Pakistan integrating digital platforms into essential aspects of daily life, from finance to communication. However, the region's increasing reliance on digital infrastructure has also led to a surge in cybercrimes, including identity theft, hacking, data breaches, and cyber terrorism. The rise in cyber threats has made it imperative for governments to establish effective legal frameworks for cyberspace governance and cybercrime prevention. India, Bangladesh, and Pakistan have each developed distinct legal mechanisms to address the unique challenges of cybercrime, shaped by their socio-political contexts and governance models. India's Information Technology Act (2000), Bangladesh's Digital Security Act (2018), and Pakistan's Prevention of Electronic Crimes Act (2016) represent national efforts to secure cyberspace. However, these frameworks differ significantly in terms of scope, enforcement mechanisms, and adherence to public law principles. These differences are partly due to varying levels of economic development, political priorities, and legal traditions, all of which influence how each country perceives and addresses the balance between cyber security, individual rights, and national security. A comparative analysis of these cybercrime laws reveals important insights into each country's approach to public law principles, including transparency, accountability, and the protection of fundamental rights. It is crucial to examine whether these laws align

with international cyber governance standards, safeguard fundamental rights such as privacy and freedom of expression, and effectively address emerging cyber threats. Furthermore, as cybercrimes are often transnational, the effectiveness of these laws is increasingly linked to regional cooperation, which remains a challenge due to inconsistent legislative standards and limited cross-border frameworks. This paper explores the alignment of cybercrime legislation

One of the primary criticisms of PECA is its impact on privacy and freedom of speech, as it grants authorities significant powers to monitor and control digital content. Critics argue that PECA includes ambiguous language that allows for broad interpretation, potentially leading to the misuse of power in cases where online activities are perceived as a threat to national security. While the law aims to address both cyber terrorism and online harassment, some scholars contend that the Act lacks the necessary judicial oversight to prevent abuse, which may lead to infringements on individual rights (Ahmad, 2018). The complexity of enforcing PECA, coupled with limited technical expertise within law enforcement agencies, has also been noted as a barrier to its effectiveness.

Comparative Public Law and Cyber Law Governance: The principles of public law—such as transparency, accountability, and the protection of fundamental rights—are essential for evaluating the effectiveness of cybercrime legislation in India, Bangladesh, and Pakistan. Despite their shared colonial legal legacy, these countries have adopted different approaches to cyber law governance, reflecting unique socio-political contexts and national priorities. Comparative studies by scholars like Mehta (2020) suggest that while there is a common goal of cyber security, the countries diverge in their governance models. India's approach to cybercrime legislation has been to align with international standards where possible, emphasizing both individual rights and national security. In contrast, Bangladesh's Digital Security Act prioritizes national security concerns, which often leads to limitations on freedom of expression. Pakistan's PECA, on the other hand, attempts to strike a balance between combating cyber threats and protecting civil liberties, though its vague language and limited judicial oversight raise concerns about transparency and accountability. The divergence in governance models across these three countries has implications for regional cooperation on cybercrime. Scholars argue that the lack of harmonization in cyber laws across South Asia creates challenges for cross-border cooperation, hindering effective responses to transnational cybercrime. This misalignment also limits the potential for collaborative frameworks that could facilitate information-sharing and joint enforcement mechanisms, both of which are critical in the increasingly globalized domain of cyber threats. Comparative public law literature underscores the importance of harmonized legal frameworks to enhance regional cyber security, suggesting that more coordinated efforts could strengthen the region's resilience against cybercrime.

Challenges in Implementation and Governance: Despite their distinct legislative approaches, India, Bangladesh, and Pakistan face common challenges in the implementation of their cyber laws. Issues such as inadequate technical expertise, limited resources within law enforcement, and procedural delays are prevalent across the region. Studies, such as those by Bailey (2021), highlight the need for stronger regulatory frameworks and international collaboration to address cross-border cyber threats effectively. Additionally, the tension between national security and individual rights remains a critical issue, with each country grappling with how best to balance these often-competing interests. The existing literature underscores that while each country has made strides in establishing cybercrime legislation, gaps remain, particularly in aligning these laws with international standards and ensuring adequate protection for fundamental rights. These challenges suggest the need for a more unified approach to cyber law governance in South Asia, one that could foster regional cooperation and create a cohesive framework for addressing transnational cybercrime. The literature on cybercrime legislation in India, Bangladesh, and Pakistan reveals both progress and limitations in the region's approach to cyber security. While each country has developed legal frameworks to combat cyber threats, challenges persist in balancing national security and individual rights, as well as ensuring effective enforcement. The comparative analysis of cyber laws in these countries suggests that a more harmonized approach, informed by public law principles and aligned

with international standards, could enhance the effectiveness of cyber law governance across South Asia. Through further research and cross-border collaboration, there is potential to create a stronger and more resilient regional framework for cybercrime prevention, contributing to a safer and more secure digital environment in South Asia.

Methodology: This qualitative and comparative legal research follows UGC and Manav Rachna University guidelines. Primary sources include legal statutes from each country, while secondary data encompasses scholarly articles and international cybercrime frameworks like the Budapest Convention. The study analyzes the structure, enforcement, and rights protections in each legal framework and evaluates alignment with global standards.

Results: The comparative analysis of cybercrime legislation in India, Bangladesh, and Pakistan reveals distinct approaches influenced by each country's unique socio-political context and legal priorities. The findings underscore the variations in these laws regarding cyber security, governance, and the balance between national security and individual rights.

Cybercrime Law Comparisons: India's Information Technology Act (ITA) primarily emphasizes cyber security through a rights- based framework. The ITA's 2008 amendment strengthened provisions against cyber offenses such as data breaches, identity theft, and cyber terrorism, with a focus on protecting individuals' rights while maintaining national security. However, the enforcement of the ITA faces certain challenges, particularly due to limited technical resources and occasional ambiguities in the Act's provisions. These enforcement issues have led to varied judicial interpretations, highlighting the complexities of aligning legal measures with rapidly evolving cyber threats. Bangladesh's Digital Security Act (DSA) of 2018, on the other hand, adopts a more restrictive approach, prioritizing national security and stability. The DSA includes broad language that allows significant governmental control over online content, including the ability to remove or restrict access to information deemed threatening to national security. This approach has led to criticisms for potentially curbing civil liberties, particularly freedom of expression. The restrictive stance reflects Bangladesh's emphasis on controlling digital threats that could disrupt social order, albeit at a cost to certain individual rights. Pakistan's Prevention of Electronic Crimes Act (PECA) of 2016 attempts to balance regional and international cyber security obligations with national security needs. PECA addresses cyber offenses such as unauthorized access, cyber terrorism, and electronic fraud, incorporating provisions that align with international cybercrime standards. However, PECA also faces challenges in enforcement, with some vague terms leading to broad interpretations. These challenges impact the consistency of enforcement and create potential for misuse, particularly regarding privacy and freedom of expression.

Public Law Influences on Cyber Governance: The influence of public law principles—such as transparency, accountability, and the protection of fundamental rights—is evident to varying degrees across the three countries. India's ITA aligns most closely with public law standards, as it emphasizes both individual rights and cyber security. The Act's provisions incorporate principles of transparency and accountability, though enforcement issues occasionally impede these ideals. In contrast, Bangladesh's DSA shows the least adherence to public law principles, adopting a security-centric approach that places limits on free expression and digital rights. Pakistan's PECA, while attempting to balance rights and security, falls somewhere in between, facing challenges in fully aligning with public law principles due to the Act's ambiguities and limited judicial oversight.

Impact on Fundamental Rights: Each country's cyber laws affect fundamental rights, particularly freedom of expression and privacy, though to different extents. India's ITA impacts individual rights but seeks to maintain a balance, with judicial oversight providing some checks against misuse. Bangladesh's DSA has faced the most criticism for its impact on fundamental rights, with provisions that enable government monitoring and control over digital content. The DSA's restrictions on online expression and privacy have led to debates on whether the Act adequately respects individual rights. Pakistan's PECA has

also faced criticism, particularly regarding privacy concerns, as the Act allows for extensive monitoring powers. However, unlike Bangladesh, Pakistan has attempted to incorporate certain safeguards, though these remain limited by vague language and inconsistent enforcement. Overall, the results indicate that while India, Bangladesh, and Pakistan share common objectives in combating cyber threats, their approaches diverge due to different governance models and priorities. India emphasizes a rights-based approach despite enforcement challenges, Bangladesh prioritizes national security with restrictive measures, and Pakistan seeks a balance but struggles with enforcement consistency. These findings suggest the need for greater regional cooperation and alignment with international standards to ensure effective cyber governance while safeguarding fundamental rights across South Asia.

Discussion: The comparative analysis of cybercrime legislation in India, Bangladesh, and Pakistan underscores the significant role that socio-political contexts and legal traditions play in shaping each country's approach to cyber governance. Despite sharing a similar legal heritage rooted in colonial law, these countries have developed distinct frameworks for addressing cybercrime, reflecting different priorities and challenges. This study highlights how these variations impact not only domestic governance but also regional cyber security cooperation in South Asia. India's approach, exemplified by the Information Technology Act (ITA), aligns more closely with international standards, particularly in protecting individual rights alongside cyber security. India's participation in global forums on cyber security, as well as its attempts to harmonize laws with international cybercrime conventions, indicates an effort to address cyber threats through a framework that balances security with respect for civil liberties. Nonetheless, enforcement challenges persist, largely due to the rapid evolution of cyber threats and a lack of technical infrastructure in some regions. These issues point to a gap between legislative intent and practical enforcement, suggesting that while India's legal structure is relatively advanced, it requires ongoing updates and improvements in implementation to stay effective. In contrast, Bangladesh's Digital Security Act (DSA) adopts a markedly different stance, prioritizing national security and control over digital content. This approach, while effective in curbing certain forms of cybercrime, has raised concerns over civil liberties, particularly freedom of expression. Bangladesh's focus on national stability in its cyber laws reflects its government's sensitivity to social and political dynamics, especially the need to prevent misuse of online platforms for dissent or destabilization. However, the DSA's broad language and limited provisions for oversight raise questions about its compatibility with public law principles, particularly in balancing state control with individual rights. The findings indicate that Bangladesh's cyber governance framework, while aimed at maintaining security, may benefit from clearer guidelines and stronger protections for civil liberties to align more closely with international human rights standards. Pakistan's Prevention of Electronic Crimes Act (PECA) sits between these two approaches, aiming to balance national security needs with obligations toward individual rights. PECA's provisions for cybercrimes such as electronic fraud and cyber terrorism demonstrate an attempt to align with international standards, yet enforcement remains inconsistent. The Act's vague language and lack of clear judicial guidelines have led to varied interpretations, creating challenges in enforcement and raising concerns over potential misuse. These findings suggest that while Pakistan seeks to maintain a balanced approach, the effectiveness of PECA could be enhanced through more precise language and stronger enforcement mechanisms that support both national security and civil liberties.A common theme across these countries is the challenge of cross-border cyber threats, which frequently transcend national boundaries and call for regional cooperation. South Asia's unique cyber environment characterized by shared language and cultural ties but differing political systems, creates both opportunities and obstacles for effective cooperation. While India, Bangladesh, and Pakistan recognize the need for collaboration on cyber issues, their divergent legislative priorities and enforcement challenges hinder collective action. The study suggests that regional cyber governance could benefit from a shared framework or cooperative mechanisms to address cybercrimes that operate across borders. Standardizing certain aspects of cyber legislation, along with establishing regional protocols for data sharing and mutual legal assistance, could foster a more cohesive and effective response to cyber threats in South Asia.In conclusion, while India, Bangladesh, and Pakistan have each developed distinct cyber governance frameworks, these differences highlight the broader tensions between national

security, civil liberties, and regional cooperation. India's rights-based approach, Bangladesh's security-centered stance, and Pakistan's balancing act each present valuable insight into the complexities of governing cyberspace. Strengthening regional partnerships and aligning cyber legislation with international standards may enhance cyber security while supporting individual rights, laying the groundwork for a more resilient and cooperative South Asian response to cyber threats.

Conclusion: This study emphasizes the critical need for harmonized cyber laws across South Asia, particularly to improve regional cooperation and address the growing prevalence of cross-border cyber threats. While India, Bangladesh, and Pakistan have each made significant progress in developing legal frameworks to counter cybercrime, each faces unique challenges rooted in socio-political priorities, enforcement limitations, and varying degrees of alignment with international standards. India's relatively rights-oriented approach offers a model for balancing cyber security with respect for civil liberties, although challenges in enforcement and infrastructure still hinder its effectiveness. Bangladesh, on the other hand, emphasizes national security within its cyber legislation, yet this has raised concerns over freedom of expression and privacy, signaling a need for reforms that can better protect fundamental rights while maintaining national security. Pakistan's Prevention of Electronic Crimes Act (PECA) seeks a middle ground, but its enforcement difficulties and ambiguous language point to areas where clarification and stronger protections are necessary. The study suggests that an integrated approach to cyber governance in South Asia could enhance security and build trust among these neighboring countries. Establishing collaborative mechanisms such as shared cyber security resources, mutual legal assistance agreements, and data-sharing protocols could streamline responses to cyber threats that transcend national borders. Additionally, aligning cyber legislation with global best practices would support more consistent enforcement, protect individual rights, and address the regional cyber security gaps that cybercriminals often exploit. Furthermore, adopting transparent enforcement processes and prioritizing data privacy across all three countries would not only improve public trust but also help ensure that cyber laws respect individual rights. By aligning regional efforts, South Asia has the potential to create a cohesive and resilient response to cyber threats, fostering a legal environment that upholds security while supporting personal freedoms. This unified approach would benefit each nation individually and strengthen the collective cyber security posture of the region, making it better prepared to tackle future challenges in the digital realm.

References:

1. Bari, M. E. (2021). Digital Security Act of Bangladesh: Challenges in Safeguarding Freedom of Expression. Dhaka University Law Journal, 15(2), 45-60.
2. Dug gal, P. (2014). Cyber Law: The Indian Perspective. Universal Law Publishing.
3. Khan, A. (2020). Cybercrime and Cyber security in Bangladesh: Legislative Responses and Challenges. Bangladesh Journal of Law, 18(1), 75-92.
4. Mehta, N. (2020). Public Law and the Regulation of Cyberspace in South Asia: A Comparative Study. International Journal of Law and Information Technology, 28(3), 245-270.
5. Rastogi, A. (2014). Cyber Law in India: Pioneering in the Digital Age. Oxford University Press.
6. Yasin, M. (2017). Cybercrime and the Law in Pakistan: Addressing Security and Privacy Issues. Pakistan Law Review, 25(1), 115-130.
7. Bailey, R. (2021). Challenges in Cybercrime Enforcement in South Asia: A Comparative Perspective. Journal of Information Law, 10(2), 145-162.
8. Multimedia University Law Journal. (2019). Comparative Law and Digital Governance: Cybercrime in Asia. 7(2), 101-115.
9. Rahman, M. (2018). *Cyber Governance and Public Law in Bangladesh: A Legislative Overview*. Law and Policy Review, 22(4), 55-70.
10. Google Scholar. (n.d.). *Cybercrime Legislation in South Asia: India, Bangladesh, and Pakistan*. Retrieved from https://scholar.google.com.

11. Semantic Scholar. (n.d.). *Comparative Public Law in Cyber Governance: Challenges in South Asian Jurisdictions*. Retrieved from https://www.semanticscholar.org.