▪ **Pages:** 1– 8 ▪ **Vol.** I, **No.** I (Spring 2022) ▪ **p- ISSN:** 3078-3666 ▪ **e- ISSN:** 3078-3283

Corresponding Author: Bilal Khan Niazi (Advocate, District Bar Association/Director Coordination, Indus Mediation & Dispute Resolution Centre, Lakki Marwat, KP, Pakistan. Email: bilalniazi972@Gmail.Com)

Doi: 10.31703/ijlss.2022(I-I).01 | Link: https://doi.org/10.70540/ijlss.2022(I-I).01

Cite Us

Exploring and Critically Analyzing Cybercrime Legislation and Digital Rights in Pakistan: Challenges and Prospects

Bilal Khan Niazi[1] | Javed Iqbal[2]

Abstract: *Cybercrime legislation and digital rights are critical components of modern legal frameworks, especially in the context of Pakistan's rapidly evolving digital landscape. This paper provides a comprehensive analysis of the challenges and prospects surrounding cybercrime legislation and digital rights protection in Pakistan. Beginning with a historical overview, the paper traces the development of cybercrime laws in the country, highlighting key legislative milestones and the evolving nature of cyber threats. It then examines the current legal framework governing cybercrimes and digital rights, including the Prevention of Electronic Crimes Act (PECA) and related statutes, assessing their strengths and weaknesses. The paper identifies challenges in the implementation and enforcement of cybercrime laws, such as capacity constraints and procedural hurdles, and explores the impact of prevalent cyber threats on individuals, businesses, and national security. Furthermore, it discusses the protection of digital rights, including freedom of expression, privacy, and access to information, within the Pakistani legal context. Drawing on case studies and international legal standards, the paper offers recommendations for reform aimed at strengthening cybercrime legislation and enhancing the protection of digital rights in Pakistan. By addressing these issues, Pakistan can better navigate the complexities of the digital age while upholding fundamental rights and ensuring cyber security for all its citizens.*

Keywords: Cybercrime Legislation, Digital Rights, Prevention of Electronic Crimes Act (PECA), Cyber Threats, Privacy, Freedom of Expression, Access to Information

Introduction

Modern nations have sought to address the complexities of the digital realm by employing legal frameworks. These legal structures typically manifest as either regulatory measures or criminal statutes. For instance, the United States maintains a robust competition law, exemplified by the Sherman Anti-Trust Act of 1890, which scrutinizes the market dominance of tech corporations and governs their behavior through punitive enforcement actions. While the U.S. has adapted existing legislation to oversee the activities of private entities in cyberspace, the European Union (EU) has taken a distinct approach. In 2016, it enacted the EU General Data Protection Regulation 2016/679 (GDPR), which focuses on regulating the data practices of major tech firms, prioritizing individuals' privacy rights over the commercial interests of corporations. On the criminal front, the U.S. passed the Computer Fraud and

[1] Advocate, District Bar Association/Director Coordination, Indus Mediation & Dispute Resolution Centre, Lakki Marwat, KP, Pakistan.

[2] LLB. ,MA Political Science, MA Islamyat, MA English, M Phil Political Science, Diploma in Sharia and Law.

Citation: Niazi, Bilal Khan and Javed Iqbal. 2022. "Exploring and Critically Analyzing Cybercrime Legislation and Digital Rights in Pakistan: Challenges and Prospects." *Global Strategic & Security Studies Review* I (I):1-8. doi: 10.31703/ijlss.2022(I-I).01.

Abuse Act in 1986, serving as its primary legislation against cybercrimes, while the United Kingdom relies on the Computer Misuse Act of 1990 for similar purposes.

Following the suit, Pakistan has established its own legal framework to address both regulatory and criminal aspects of cyber activities. This research paper adopts an exploratory approach to delve into the intricacies of Pakistan's legal framework in this domain.

Origin of Legal Framework on Cyberspace

The inception of Pakistan's legal framework concerning cyberspace can be traced back to the Constitution of Pakistan, 1973, which though does not explicitly mention information technology or cyberspace. However, it delineates legislative powers to the Federation through the Federal Legislative List in the Fourth Schedule. These include authority over communications (Item 7), copyright, inventions, and designs (Item 25), international treaties and conventions (Item 32), the State Bank of Pakistan (Item 28), implying e-banking and e-commerce mechanisms, and insurance law (Item 29).

Regarding criminal jurisdiction, the constitutionality of the Federation's powers is anchored in articles 142 and 143, which declare criminal law, criminal procedure, and the law of evidence as shared responsibilities of both the Federation and the Provinces. Leveraging this constitutional framework, the Federation has enacted several laws pertaining to cyberspace. Foremost among these legislations are: (1) the Federal Investigation Act, 1974, (2) the Pakistan Telecommunication (Re-Organization) Act, 1996, and (3) the [3]This overview serves as a preliminary exploration, providing foundational knowledge for more in-depth research on the subject. Each of these laws will be briefly discussed in subsequent sections.

The Federal Investigation Agency Act, 1974

The Federal Investigation Agency (FIA) stands as the primary federal law enforcement body established under the Federal Investigation Agency Act, 1974. As with many policing laws in Pakistan, the Federal Government holds authority over its oversight, while the Director General, endowed with powers akin to those of an Inspector General of Police, assumes administrative control. Members of the FIA possess powers on par with provincial police officers, enabling them to effect arrests and seize property throughout Pakistan. The agency's operational framework comprises territorial and functional directorates, each headed by police officers holding the rank of Deputy Inspector General of Police, with individual directorates housing police stations manned by officers-in-charge (Station House Officers) not below the rank of Sub-Inspectors of Police. The Act's appended Schedule delineates offences and laws falling within the FIA's purview. Notably, the FIA's scope encompasses critical areas such as human smuggling, trafficking, immigration, cybercrimes, official secrets, corporate crimes, money laundering, counter-terrorism financing, and high treason.

Of particular significance in the realm of cybercrimes, the FIA assumes authority as the sole investigative agency authorized to probe offences pertaining to computers, the internet, and illicit utilization of information technology. Furthermore, the agency possesses the mandate to initiate legal proceedings under extraterritorial jurisdiction in criminal matters, thereby solidifying its pivotal role within the national security framework, particularly concerning internal security. Strengthening its cross-border reach, the FIA houses the National Central Bureau (NCB), facilitating singular coordination with INTERPOL, the International Police Organization. As the paradigm increasingly shifts towards a rule of law approach in combatting counterterrorism and cybercrimes, the FIA emerges as a pivotal lead agency, tasked with addressing inter-provincial and transnational organized crime.

[3] Government of Pakistan. 2016. *Prevention of Electronic Crimes Act*. § 49. Accessed June 27, 2024. https://na.gov.pk/uploads/documents/1470910659_707.pdf.
4o

The Pakistan Telecommunication (Re-Organization) Act, 1996

The Pakistan Telecommunication Authority (PTA) assumes a pivotal role in preventive and regulatory measures, particularly concerning the initiation of policing actions such as website blocking and content regulation, in coordination with Social Media Companies (SMCs). Established under the Pakistan Telecommunication Authority (Re-organization) Act, 1996, the PTA's inception aimed to foster competition within the deregulated telecommunications market following Pakistan's accession to the General Agreement on Trade in Services (GATS) under the World Trade Organization Agreement in 1994. Over time, in the absence of a dedicated regulator for the telecommunications media, the PTA has expanded its functions to encompass policing responsibilities under various sets of delegated legislation, including:

i. The Citizens Protection (Against Online Harm) Rules, 2020;
ii. The Critical Telecom Data and Infrastructure Security Regulations, 2020;
iii. Mobile Device Identification, Registration & Blocking (Amendment) Regulations, 2018;
iv. Data Retention of Internet extended to Public Wi-Fi-Hotspots Regulations, 2018;
v. Subscribers Antecedents Verification Regulations, 2015;
vi. The Telecom Consumer Protection Regulations, 2009.

Moreover, the PTA supplements and coordinates efforts in providing computer emergency response teams for the protection of critical infrastructure, as mandated by Section 49 of the Prevention of Electronic Crimes Act, 2016. This multifaceted role underscores the PTA's significance in safeguarding telecommunications integrity and ensuring regulatory compliance within the digital sphere. Prevention of Electronic Crimes Act, 2016, § 49

The Prevention of Electronic Crimes Act, 2016

The Prevention of Electronic Crimes Act, 2016 (PECA) stands as the primary criminal legislation addressing cybercrimes in Pakistan, encompassing a broad spectrum of offenses occurring in cyberspace and involving digital devices. With a comprehensive framework, PECA delineates twenty-three distinct offenses, ranging from unauthorized data access and interference with critical infrastructure to cyber terrorism, hate speech, electronic forgery, and child pornography, among others. Notably, only three offenses—cyber terrorism and those pertaining to the dignity and modesty of individuals—are cognizable, necessitating judicial authorization for legal action, which may impede swift redress for aggrieved parties seeking recourse through executive authorities or the police. Beyond its substantive criminal provisions, PECA assumes a procedural and regulatory role, designating only authorized investigative agencies to handle cybercrime probes. The Prevention of Electronic Crimes Investigation Rules, 2018 (PEC Rules), promulgated under PECA's mandate, entrust the Federal Investigation Agency (FIA) as the sole agency authorized to investigate cybercrimes. However, given the pervasive nature of cybercrimes and digital devices' involvement in various offenses, the exclusion of provincial police organizations from investigative authority is poised for review. PECA incorporates a robust preventive framework, empowering the Federal Government to issue directives to information system owners and establish Computer Emergency Response Teams (CERTs). The legislation also facilitates the issuance of search and seizure warrants and warrants for content data disclosure, obligating service providers to promptly retain and furnish data to authorized police officers.

Moreover, PECA outlines detailed procedures for data seizure by authorized officers, and the PEC Rules establish a dedicated Cybercrime Wing within the FIA, comprising sections for cybercrime investigations, forensics, and data and network security. Additionally, the PEC Rules institute a cybercrime complaints registry mechanism for efficient citizen redressal, while also outlining training protocols for Cyber Wing officers and procedures for transferring cybercrime investigations. Emphasizing international cooperation, the Rules delineate protocols for collaboration with INTERPOL, while underscoring principles of victim confidentiality and witness protection during investigations. Overall, PECA and its accompanying

regulations represent a multifaceted legal framework aimed at combating cybercrimes while ensuring procedural fairness and effective enforcement.

Background of PECA

The Prevention of Electronic Crimes Act, 2016 (PECA) emerged as a cornerstone of Pakistan's anti-terrorism efforts, prominently featured within the National Action Plan (NAP) formulated in response to the harrowing attack on the Army Public School (APS) in December 2014. The severity of the APS attack prompted the government to prioritize counterterrorism measures, emphasizing the imperative of unfettered surveillance and prosecution capabilities to combat militant activity effectively. This urgency influenced the drafting of PECA, along with other laws enacted in the aftermath of the APS tragedy. Similar to the legislative response in the United States following the 9/11 attacks, wherein the Patriot Act of 2001 was swiftly passed by Congress, and in the United Kingdom with the Anti-Terrorism, Crime and Security Act of 2001, Pakistan's post-APS legislative landscape reflected a sense of urgency and determination to confront terrorism head-on. However, akin to criticisms leveled against the Patriot Act and the UK's anti-terrorism legislation, PECA has faced scrutiny for its potential encroachment on civil liberties. Critics argue that such legislation, crafted in the wake of traumatic events, may inadvertently curtail fundamental rights in the name of security, invoking a state of panic to justify restrictions on individual freedoms.

General Analysis

The concept of due process of law is a constitutional guarantee ensuring fair treatment within the normal judicial system, [4]entailing notice of charges and a hearing before an impartial judge. [5]Understanding due process is crucial to grasp the significance of constitutional rights, as it serves as a safeguard against potential government abuses of power. Every citizen of Pakistan is entitled to be treated according to the law, requiring any infringement upon citizen rights to be justified under the country's legal framework. [6]Similarly, Article 10-A further guarantees citizens a fair trial and due process, albeit limited to criminal charges. (ibid, art. 10.) These constitutional guarantees have undergone judicial interpretation, notably in the case of Begum Shorish Kashmiri (Government of West Pakistan and another v Begum Agha Abdul Karim Shorish Kashmiri PLD 1969 SC 14), where the scope of due process was expanded. The court affirmed that every citizen has the constitutional right to be tried in accordance with the law, interpreting "law" in a broad sense encompassing judicial principles established by superior courts. [7]Consequently, due process extends beyond procedural considerations to encompass substantive due process, ensuring that laws uphold the liberties and rights of citizens. In essence, due process protections in Pakistan emphasize adherence to the ethical principles of the law, ensuring that legislation safeguards the fundamental freedoms and rights of the populace. PECA appears to violate the inherent guarantees of due process enshrined in the Constitution, raising concerns that could potentially lead to the legislation being invalidated.

[4] ibrary of Congress. 2018. "Due Process of Law - Magna Carta: Muse and Mentor." Accessed June 27, 2024. https://www.loc.gov/exhibits/magna-carta-muse-and-mentor/due-process-of-law.html.

[5] Chauhan, D. S. 2016. "Evolution of 'Due Process of Law' under Indian Constitution: A Special Comparative Analysis with the Concept under Pakistani Constitution." *Imperial Journal of Interdisciplinary Research* 11, no. 2: 2.

[6] Constitution of the Islamic Republic of Pakistan, 1973, art. 4. Accessed June 27, 2024. http://www.commonlii.org/pk/legis/const/1973/2.html#:~:text=4.,the%20time%20being%20within%20Pakistan.

[7] Khan, E. A. n.d. "The Prevention of Electronic Crimes Act 2016: An Analysis." Accessed June 27, 2024. https://sahsol.lums.edu.pk/sites/default/files/202209/11._the_prevention_of_electronic_crimes_act_2016-_an_analysis.pdf.

Ambiguous terms over broadening Scope

The language used in the statute renders it challenging to determine what constitutes criminal conduct. For instance, terms in the definitions section are subjectively defined, such as the term "act," which is vaguely described as "a series of acts" without clear elucidation. [8]Similarly, the definition of dishonest intention includes subjective elements, such as the intent to "create hatred," leading to ambiguity. (Ibid, s. 2 (1) (xvi).

) Section 10, addressing cyber-terrorism, has also been criticized for its broad definition. Critics argue that cyber-terrorism offenses should be explicitly linked to violence and the risk of harm, yet the provision includes qualifiers like "advancement of inter-faith, sectarian, or ethnic hate," blurring the line between terrorism and offenses related to inciting violence or hostility. [9]

Ambiguous and technical provisions in the law are typically scrutinized based on the vagueness doctrine, which mandates criminal laws to precisely define punishable conduct. [10]Several provisions in PECA risk being invalidated for potentially contravening due process provisions guaranteed in the Constitution. For instance, Section 48 grants the government and Pakistan Telecommunications Authority (PTA) unchecked authority to issue directives to service providers, lacking precision and safeguards that could exacerbate issues, particularly concerning the restriction of free speech. [11]

Similarly section 31, addressing "expedited preservation and acquisition of data," grants broad authority to an authorized agent to obtain data without a court warrant if it is deemed "reasonably required" for a criminal investigation. (ibid, s. 31) However, the lack of defined criteria for what constitutes a "reasonable requirement" and the absence of judicial oversight pose significant concerns. This provision grants the executive discretionary power without adequate checks and balances, potentially infringing upon fundamental rights and undermining due process. Such provisions could be susceptible to misuse for political agendas, suppressing lawful debate or dissent.

Contrary to Freedom of Speech

PECA has come under significant scrutiny for its perceived infringement upon the fundamental right to freedom of speech, as guaranteed under Article 19 of the Constitution. Freedom of speech and press are essential pillars of democratic institutions, albeit subject to reasonable restrictions imposed by law. ([12]Assessing the reasonableness of such restrictions typically falls within the purview of the courts. [13]One major concern revolves around whether certain powers vested in authorities under PECA are appropriate. Section 37 of the Act addresses unlawful online content, granting extensive powers to the Pakistan Telecommunications Authority (PTA) to block or remove online content, thereby encroaching upon the right to freedom of expression. PTA's track record of arbitrary censorship and content removal adds to the apprehensions. (Prevention of Electronic Crimes Act 2016, s. 37)

The executive authority of PTA holds sole discretion in interpreting and applying Article 19, with the authority to regulate internet content access and remove deemed objectionable content. Furthermore, section 37 allows complainants to petition PTA to block content without requiring a court order, providing the state with a mechanism to censor content it deems undesirable. For instance, political

[8]Prevention of Electronic Crimes Act, 2016, § 2(1)(i)(a).

[9] Baig, A. (2016). Prevention of Electronic Crimes Bill 2016 – Implications for Investigative and Public Interest Journalism. Media Matters for Pakistan.

[10] Daudpota, F. (2016). An Examination of Pakistan's Cybercrime Law. SSRN, 14.

[11] Prevention of Electronic Crimes Act 2016, s. 48

[12] Article 19 and threat to media. (2018, May 3). The News

[13] Tofazzal Hossain v Government of West Pakistan PLD 1969 Dacca 589

content could be blocked under the guise of preventing harm. Throughout its history, the Pakistan Telecommunications Authority (PTA) has gained notoriety for its informal and regular engagements in censorship, often characterized by arbitrary blocking and removal of content. In April 2015, the Pakistan Telecommunications Authority (PTA) blocked the political forum Siasat.pk, citing its perceived anti-government stance. Siasat.pk is a prominent platform known for enabling people to voice their criticisms of the government. The incident garnered significant attention in Pakistani media, and following public pressure, the government eventually restored access to the forum. This case was reported by Haroon Baloch, Maria Xynou, and Arturo Filasto in their research on internet censorship in Pakistan spanning from 2014 to 2017 Facebook's transparency report revealed that numerous pieces of content were restricted in Pakistan based on PTA requests citing local laws on blasphemy and condemnation of the country's independence. Several other provisions in the Act also pose threats to free speech. For instance, section 9 addresses the glorification of an offense but is drafted broadly, potentially breaching international standards of freedom of speech. [14]This provision, similar to a chiling effect, could deter legitimate exercise of free speech rights due to the threat of legal repercussions. A similar phenomenon was observed in the US Supreme Court's Reno v. ACLU case, where vague regulations led to concerns about chiling effects on free speech. (Reno v American Civil Liberties Union, 117 S.Ct. 2329, 138 L.Ed.2D 874 (1997)' (Cornell University Law School, 2018)

) In a notable development, the Indian Supreme Court struck down section 66-A of the Information Technology Act 2000 in 2015, citing violations of freedom of speech. This underscores the significance of freedom of speech. Pakistan, like India, is a signatory to the International Covenant on Civil and Political Rights (ICCPR), obligating the government to uphold and implement provisions related to freedom of expression and speech. (Farooqui, O., & Alam, A. (2015) The court discussed the phenomenon of the 'chilling effect' as the basis for invalidating the excessively broad and ambiguous statutory provision.

This judicial action underscores the critical significance of safeguarding the right to freedom of speech. Moreover, similar to India, Pakistan has ratified the International Covenant on Civil and Political Rights (ICCPR). Consequently, the government is obligated to uphold and enforce the provisions of the ICCPR, particularly those pertaining to freedom of expression and speech.

Contrary to Right to Privacy

The Constitution of Pakistan upholds the right to privacy as a fundamental right. [15]Additionally, the International Covenant on Civil and Political Rights (ICCPR), to which Pakistan is a signatory, prohibits arbitrary or unlawful interference with privacy, family, or correspondence. [16]The interpretation and scope of Article 14 were deliberated upon by the Supreme Court in the case of Mohtarma Benazir Bhutto v President Pakistan. (PLD 1998 SC 388.) The Court affirmed the inviolability of an individual's dignity and privacy, extending the protection of privacy beyond the confines of one's home to public spaces, emphasizing the significance of privacy regardless of location. The case of Mehram Ali v Federation of Pakistan (PLD 1998 SC 1445.) addressed the conflict between the right to privacy and the authority to conduct searches and seizures. In this case, the Supreme Court of Pakistan declared section 10 of the Anti-Terrorism Act (ATA) unconstitutional. Section 10 of the ATA empowered authorized officials to conduct searches and seizures if they had reasonable grounds to suspect that a person possessed written material or recordings violating section 8 of the ATA. The Supreme Court's decision highlighted the importance of balancing individual privacy rights with the government's duty to maintain security. While acknowledging that the right to privacy is subject to reasonable restrictions, the Court emphasized that any laws infringing upon privacy must be reasonable and aligned with constitutional principles. By declaring section 10 of the ATA unconstitutional, the Supreme Court reaffirmed the constitutional

[14] Prevention of Electronic Crimes Act 2016, s. 9
[15] The Constitution of Islamic Republic of Pakistan 1973, art. 14
[16] Article 17 of the International Covenant on Civil and Political Rights (ICCPR)

mandate to protect individual privacy rights and prevent arbitrary intrusions by the government. This decision underscored the judiciary's role in upholding fundamental rights and ensuring that government actions comply with constitutional norms.

Despite these constitutional and international provisions, a report by Privacy International reveals the absence of direct data protection authorities or laws in Pakistan. [17]Data privacy and protection are theoretically regulated through provisions of the Electronic Transactions Ordinance 2002 and The Freedom of Information Ordinance 2002. However, the Prevention of Electronic Crimes Act (PECA) also includes several provisions concerning data privacy, often aimed at granting government agencies access to private citizen data or restricting citizens from accessing government data. Certain provisions of PECA encroach upon the right to privacy by empowering authorities such as the Pakistan Telecommunications Authority (PTA) and law enforcement agencies to access private citizen data and restrict citizen access to government data. For instance, section 31 of PECA allows law enforcement agencies to demand data from individuals without a court warrant if deemed "reasonably required" for a criminal investigation, granting significant discretion to officers. This provision raises concerns regarding privacy infringement, particularly in cases of vaguely defined offenses such as "cyberterrorism."

Additionally, PECA mandates Internet Service Providers (ISPs) to retain specified traffic data for a minimum of one year and provide it to investigation agencies or authorized agents upon demand. [18]

This requirement exceeds international standards for data retention and poses risks of extensive surveillance. In 2014, the UK High Court ruled that the Data Retention and Investigatory Powers Act 2014 (DRIPA) was unlawful after it was challenged on the grounds of violating the right to privacy. [19]This decision was based on the finding that DRIPA was inconsistent with Article 8 of the European Convention on Human Rights, which protects the right to respect for one's private and family life, as well as the protection of personal data. Similarly, the Court of Justice of the European Union highlighted that the retention of data could lead to detailed insights into individuals' private lives. Consequently, it was deemed as a disproportionate intrusion on the right to privacy.

These legal precedents from Europe provide grounds for challenging the constitutionality of similar provisions in Pakistan. The arguments against data retention and its potential impact on privacy rights can be applied to scrutinize the legality of relevant sections within Pakistani laws. The lack of judicial oversight and accountability mechanisms exacerbates these concerns. Furthermore, PECA grants sweeping powers to the government for international data sharing without adequate safeguards or oversight, potentially compromising privacy rights. [20]The absence of accountability mechanisms and oversight processes in the law raises doubts about its effectiveness in protecting citizen privacy

Conclusion

the legal framework governing cyberspace in Pakistan, primarily anchored by the Prevention of Electronic Crimes Act (PECA) 2016, reflects a complex interplay between national security imperatives, law enforcement objectives, and the protection of fundamental rights. While PECA was conceived as a response to evolving cybersecurity threats and the need to combat cybercrimes, its implementation has raised significant concerns regarding its compatibility with constitutional guarantees of freedom of speech, privacy, and due process. Critics have pointed out several flaws in PECA, including vague definitions of criminal conduct, broad powers granted to authorities for content regulation and data access, and the lack of judicial oversight in certain provisions. The legislation's expansive scope and ambiguous language have led to instances of government overreach, arbitrary censorship, and violations

[17] 'State of Privacy Pakistan' (Privacy International, 2018) accessed 10 September 2018

[18] Prevention of Electronic Crimes Act 2016, s. 32

[19] DRIPA Struck Down by High Court in Judicial Review Challenge. (2015). Focus on Regulation.

[20] Prevention of Electronic Crimes Act 2016, s. 42

of individuals' rights to privacy and free expression. Moreover, PECA's provisions allowing for the retention and sharing of data without adequate safeguards raise serious concerns about the potential for abuse and infringement of privacy rights.

The absence of comprehensive data protection laws further compounds these challenges, leaving individuals vulnerable to unwarranted surveillance and intrusion into their personal information. In light of international legal standards and precedents, particularly regarding the right to privacy and freedom of speech, there is a pressing need for reforms to ensure that Pakistan's cyber laws strike an appropriate balance between security concerns and the protection of fundamental rights. Any revisions to PECA should prioritize clarity, transparency, and accountability, with robust mechanisms for judicial review and oversight to safeguard against abuse of power. Furthermore, there is a need for greater public awareness and engagement regarding cyber laws and their implications for individual rights and freedoms. Civil society, legal experts, and policymakers must work together to address the shortcomings of current legislation and promote a more rights-respecting approach to cybersecurity in Pakistan.