THE JOURNAL OF RESEARCH REVIEW

P-ISSN: 3006-2632	E-ISSN: 3006-2640
Vol. 1. No. 04 (Oct-Dec) 2024	Page 228-242

Challenges in Combating Cybercrime: A Comparative Study of Pakistani and International Legal Frameworks

Syeda Mina Faisal **(Corresponding Author)**	Assistant Professor, College of Law, The University of Lahore, Pakistan mina.faisal@law.uol.edu.pk
Nain Tara Khan	Lecturer, College of Law, The University of Lahore, Pakistan nain.tara@law.uol.edu.pk
Ishaq Ahmad	Lecturer, Department of Pakistan Studies, Shaheed Benazir Bhutto University, Sheringal, Pakistan ishaq@sbbu.edu.pk

Abstract: *Cybercrime poses significant threats in today's digital landscape, with transnational crimes complicating legal responses and jurisdictional reach. This study examines the challenges Pakistan faces in combating cybercrime, comparing its Prevention of Electronic Crimes Act (PECA) 2016 with international standards like the Budapest Convention, the EU's GDPR, and the US CFAA. Through a comparative legal analysis, this paper identifies gaps in Pakistan's legislative framework, particularly in the areas of international cooperation, data protection, and adaptability to emerging cyber threats. It also addresses institutional limitations in enforcement and procedural safeguards for privacy and human rights. Key findings reveal that while PECA 2016 is a foundational step, its limited provisions on cross-border collaboration, human rights protections, and digital forensics hamper effective cybercrime management. The study recommends legislative amendments, capacity building, and Pakistan's potential accession to the Budapest Convention to align with global standards. These measures could enhance Pakistan's cybercrime resilience, legal coherence, and international cooperation, establishing a more secure digital environment.*

Keywords: Data Protection, Digital Forensics, Electronic Evidence, International Cooperation, Jurisdictional Challenges, Privacy Rights, Transnational Crime

Introduction

One of the crimes which emerged as a global challenge is cybercrime; the crime that threatens individual, corporate and even government security, stability and privacy. The evolution of digital technology has resulted in changing sophistication and frequency of cybercriminal behavior, targeting weaknesses in digital technologies and often crossing international borders. The purpose of this study is to evaluate the legal response of Pakistan against cybercrimes with special reference to PECA 2016, and its strength of being an antibiotic against the sui generis diseases of the cybercrimes, and the resistance which have a stronghold in the loopholes as compared to the world. The research draws important attention to the efficacy of international frameworks in addressing cyber threats with an emphasis on strengthening legislation, enforcement and international cooperation as these threats continue to become more sophisticated (Saleem et al., 2024; Riaz et al., 2022).

As Pakistan creates a growing digital infrastructure, the demand for cybercrime has exploded. As more citizens are turning towards the internet for financial transactions, online social networking, and data sharing, it is making users exposed to a range of risks, including hacking, identity theft, cyberstalking, and financial fraud. These types of crimes usually cause great financial losses while getting rid of

everyone's minutiae. The main law governing cybercrime in Pakistan is the Prevention of Electronic Crimes Act 2016 (PECA 2016), which seeks to create deterrence through precise offenses and punishment. In some respects, however, PECA is too broad where it ought to be specific, and too specific where it should be broad compared with better-developed international frameworks such as the Council of Europe's Budapest Convention, the European Union's GDPR, and the United States' Computer Fraud and Abuse Act (CFAA). Examining the structure in Pakistan against this global backdrop highlights specific advocacy points and reveals the need to align domestic legal structures with global best practices (Akhtar, 2023; Khan et al., 2022).

The research is guided by the hypothesis that, while foundational, Pakistan's current cybercrime framework lacks the comprehensive measures required for effective cross-border collaboration, data protection, and privacy safeguards found in international frameworks. These gaps limit their overall efficacy. To explore this hypothesis, the study addresses several central questions: How does Pakistan's cybercrime legislation compare with international frameworks in terms of defining offenses, procedural protections, and facilitating international cooperation? What are the main enforcement challenges Pakistan faces, and how do institutional limitations impact these efforts? Finally, how can Pakistan enhance its cybercrime framework to better align with international standards and address emerging cyber threats?

This is a comparative legal study to assess PECA 2016 in the light of key international frameworks. The article draws on legislative texts and international treaties as primary sources for the analysis, supplemented by scholarly publications, governmental publications, and reports issued by international organizations. The article illustrates cybercrime incidents from both Pakistan and the world as case studies, offering a view of real-life challenges and solutions, and providing a balanced perspective on the shortcomings of the Pakistani framework.

This study aims to develop a comprehensive analysis of Pakistan's cybercrime laws against international standards and identify key areas for improvement. These areas include the need for greater international cooperation, the need to bring clarity to the definitions of cybercrime, strengthening the resources to implement it, and providing better privacy protections. Given these findings, we anticipate that the study's recommendations will concentrate on implementing legislative reforms, enhancing institutional capacity, and potentially securing Pakistan's ratification for international conventions such as the Budapest Convention. Those reforms would help Pakistan to respond better to cybercrime and would bring the country into the world framework of facilitating a safer cyber environment (Khan, 2022).

The article proceeds as follows: a background section on cybercrime and its impacts; an overview of Pakistan's cybercrime legislation; a review of relevant international frameworks; comparative analysis; discussion of the challenges Pakistan face; the lessons international frameworks present; and a conclusion summarizing key findings and highlighting calls for reform. This study seeks to contribute both to the academic and policy-oriented discourse on cybersecurity law by comparing Pakistan's approach to cybercrime with global standards and also providing pragmatic recommendations for legal and policy reform to bring about a more digitally secure Pakistan.

LITERATURE REVIEW

Cybercrime has become an increasingly critical issue globally, prompting extensive research into effective legal frameworks and international cooperation mechanisms. The *Budapest Convention on Cybercrime* stands out as a pivotal international treaty, providing a comprehensive framework for harmonizing cybercrime laws and facilitating cross-border collaboration in investigations (Council of Europe, 2001). Gercke (2012) emphasizes the Convention's role in enhancing mutual legal assistance and real-time information sharing, which are essential for addressing the transnational nature of cyber threats. However, the absence of Pakistan from this Convention limits its ability to engage in streamlined international cooperation, thereby hindering its capacity to respond effectively to global

cybercrime challenges (Gercke, 2012).

Developing countries, including Pakistan, face unique obstacles in combating cybercrime, such as limited resources, inadequate technical expertise, and fragmented legal structures. Yar and Steinmetz (2019) highlight that these nations often struggle with enforcing cyber laws due to constrained institutional capacities and the rapid evolution of digital technologies outpacing legislative developments. This gap is evident in Pakistan's PECA 2016, which, while a significant step forward, has been criticized for its broad and sometimes vague provisions that can lead to inconsistent enforcement and potential human rights infringements (Khan, 2018).

Comparative analyses of international legal frameworks further illuminate the strengths and weaknesses of Pakistan's approach. The European Union's GDPR offers robust data protection measures and clear guidelines for privacy rights, setting a high standard for member states (Voigt & Von dem Bussche, 2017). In contrast, the United States' CFAA provides detailed definitions of cyber offenses and stringent penalties but has faced criticism for its broad application and potential for misuse (Smith, 2020). Pakistan's PECA 2016, while addressing key cybercrime issues, lacks the comprehensive data protection mechanisms found in GDPR and the precise legal definitions present in CFAA, limiting its effectiveness in safeguarding privacy and prosecuting offenders with clarity (Ali, 2019).

Institutional capacity is another critical area were Pakistan lags behind international standards. The Federal Investigation Agency (FIA), responsible for enforcing PECA, often grapples with insufficient resources, limited technical training, and a high caseload, which impede its ability to conduct thorough investigations and prosecutions (Raza, 2020). Studies by Ahmad and Khan (2021) indicate that enhancing the technical capabilities and providing specialized training for law enforcement officials are essential for improving the efficacy of cybercrime laws in Pakistan.

Moreover, the interplay between cybercrime legislation and human rights has garnered significant attention. PECA 2016 has been critiqued for granting extensive powers to authorities, which can infringe upon individual privacy and freedom of expression if not adequately checked (Hussain, 2017). In contrast, international frameworks like the Budapest Convention incorporate safeguards to balance security measures with the protection of civil liberties, highlighting the need for Pakistan to integrate similar protections within its legal framework (Council of Europe, 2001).

Emerging cyber threats, such as ransomware and sophisticated phishing attacks, further challenge existing legal structures. As cybercriminal tactics evolve, so must the legislative responses. Research by Lee and Kim (2022) underscores the importance of continuously updating cybercrime laws to address new forms of digital offenses, a practice that Pakistan must adopt to maintain the relevance and effectiveness of PECA 2016.

In summary, literature discussions indicate that international standards exist, and Pakistan is lagging behind in developing a legal framework to combat cybercrime. This results from a lack of legislative clarity, shallow institutional capacity, and weak privacy and human rights safeguards. Pakistan must address these issues, along with others, to effectively combat the growing threat of cybercrime through legislative reforms, capacity building, and increased international cooperation.

CONCEPTUAL AND THEORETICAL FRAMEWORK

The conceptual framework for this study is based on the interrelationship between legal structures, enforcement mechanisms, and international collaboration as fundamental pillars of an efficient cybercrime regime. Based on background in international law and comparative legal theory, this framework considers how differences in legal definitions, procedural guarantees, and jurisdictional agreements can affect the ability of individual countries to combat cybercrime. The framework of the study is cybercriminal justice theory, which states that cybercrime deterrence demands not just laws that are extensive and flexible but also institutions, capabilities, and cross-border relations to deal with

the real challenges posed by such crimes in the digital age. The investigation assesses the impact of compliance with worldwide trends on the ability of domestic policies, specifically Pakistan's PECA 2016, through comparative analysis with the parameters formed by the Budapest Convention as well as other international frameworks. Using this, a structured analysis can be conducted on the comprehensiveness combined with enforcement capacity of PECA within the laws of Pakistan, exploring the relationship between these factors and international cooperation in order to combat cyber threats in both domestic and international environments.

RESEARCH METHODOLOGY

The methodology of this study is based on a comparative legal analysis to explore to what extent the cyberspace of Pakistan effectively addresses the digitally conducted offenses, with a special focus on the PECA 2016. We identify primary legal texts such as PECA, the Budapest Convention, GDPR, and the CFAA as the central comparison sources. Utilizing secondary sources, from academic articles to government reports and case law, to contextualize and underscore practical difficulties enforcing the law. Analysis: The required task involves identifying key provisions of law and enforcement mechanisms in each of these frameworks, as well as assessing the synergy and effectiveness of these frameworks in countering cybercrime. This method is followed to delve into the capacity of Pakistani laws against the international approach, considering the matters of limitations of jurisdiction, protection of data, and international cooperation. This paper looks into what's wrong with the Pakistan Cyber Crime Act, 2016 (PCCA) by using and analyzing both international legal texts and real-life cybercrime cases. The goal is to find the problems with Pakistan's legal system and suggest fixes based on what works best in other countries.

CYBERCRIME IN THE DIGITAL AGE

The digital age is marked by the rapid expansion of the Internet, which has led to the evolution of cybercrime to encompass any illegal activity that involves the use of a computer, an Internet connection, or the penetration of an IT system. As technological progress permeates every aspect of life, including the economic system, social order, and lifestyle, crime has become increasingly sophisticated. Cybercrime is a prime example of this growth, as it has become an immeasurable dimension of ubiquitous illegal conduct that takes place in cyberspace, transcends geographical boundaries, and adversely impacts individuals, industries, and even governments. Examples of cybercrime include hacking, identity theft, data breaches, cyberbullying, financial fraud, online extortion (like ransomware attacks), and intellectual property theft (Khan et al., 2024; Khan & Wu, 2021).

One of the characteristics that define cybercrime in this age is the global nature of the digital world. National laws often fail to effectively combat such crimes, given that criminals can operate from anywhere in the world. The anonymity provided by the internet and digital technologies allows offenders to conceal their identities, making identification and prosecution of these offenses challenging. In addition, with many people storing more sensitive information online, cybercrime can inflict considerable financial, social, and reputational harm on its victims (Biedron, 2024; Abdelrehim Hammad et al., 2021).

Consequently, fighting cybercrime in the digital era is a complex challenge that necessitates a multi-pronged response, including the creation of comprehensive legal frameworks, cross-border collaboration, innovation in security technologies, and initiatives to educate the public and businesses on safeguarding themselves against cyber threats. Treaties between countries, such as the Budapest Convention on Cybercrime, focus on enabling countries to work together given how international cybercrime can be. Despite the existence of such laws, many nations still face challenges in effectively enforcing them, leading cybercriminals to exploit gaps and loopholes in legislation and enforcement mechanisms to evade detection and prosecution (Wall, 2024; Khan et al., 2021).

OVERVIEW OF CYBERCRIME LEGISLATION IN PAKISTAN

The greatest cybercrime legislation in Pakistan is PECA 2016, which was enacted to tackle the impending threats of cybercrime in the ever-evolving digital era. The law provides a legal structure for the prosecution of a broad spectrum of cybercrimes, ranging from hacking and data breaches to cyberstalking, internet defamation, and financial fraud. The PECA 2016 safeguards against digital violations or criminal activities that arise from the use of information technology and have since spread to almost all sectors of Pakistan's economy (Akhtar, 2023; Usman et al., 2021).

PECA carries provisions from cybercrime types. Among the key offenses under the Act are unauthorized access, cyber fraud, cyberbullying, identity theft, and cyberterrorism, among others. While the protection of data and privacy has increased, critics argue that the bill lacks clarity in defining specific crimes and has broad provisions that could lead to misuse. This includes things like "defamation" and "online blasphemy," which leads to obviously problematic free speech problems under PECA being used to silence discourse (Zahoor et al., 2020; Khan & Wu, 2021).

It also established the FIA as the sole investigative and prosecuting authority in Pakistan to investigate and prosecute relevant cybercrimes. The Cyber Crime Wing of the FIA assumes responsibility for cyber-related crimes, possesses the authority to probe online crimes, collect evidence from digital platforms, and prosecute these offenders. But the agency is severely underresourced and lacks sufficient trained personnel who can handle cross-border digital investigations, as many cybercrimes are transnational (Niazi et al., 2022; Khan et al., 2021).

The act also solidified Pakistan's existing legislative foundation for international cooperation commitments against cybercrime under various international regimes, such as the Council of Europe Cybercrime Convention, which Pakistan ratified in 2016. However, Pakistan only partially participates in international treaties such as the Budapest Convention on Cybercrime, which raises global concerns about the practical aspects of cross-border collaboration, particularly in relation to cybercrime. Furthermore, PECA has also attracted criticism because of the surveillance and data retention provisions that many local human rights activists have condemned as security overreach that could give authorities the power to infringe on individual privacy rights without sufficient checks against abuse (Zahid et al., 2024; Khan et al., 2021).

PECA has become old, and there is a need to amend it in the wake of new and emerging threats, including cyber terrorism, ransomware attacks, and data breaches, experts say. Legal experts have been advocating for enhanced coordination between government and private entities, as well as the implementation of robust data privacy laws, to enable Pakistan to tackle the escalating cyber threats without compromising the rights of its citizens. In assumption, even though PECA 2016 holds significant importance, there is still room for improvement in terms of international cooperation and assistance, institutional capacity and legitimacy, and the protection of fundamental rights. These improvements are necessary to ensure that Pakistan can effectively respond to cybercrime (Jamshed, et al., 2022; Khan et al., 2020).

THE INTERNATIONAL LEGAL FRAMEWORK

The international legal regime against cybercrime encompasses treaties, conventions, and agreements that work to harmonize and unify laws within countries, thus allowing for greater cooperation between states in fighting cyber threats that do not respect national boundaries. Considering the universal scope of cybercrime, the need arises for countries across the globe to cooperate and address issues such as hacking, identity theft, data breaches, cyberbullying, and cyberterrorism by way of international legal instruments. Maura Johnson lists out important international frameworks, including provisions such as the Budapest Convention on Cybercrime, the GDPR, and regional efforts such as the African Union Convention on Cyber Security and Personal Data Protection (Khan et al., 2020).

Budapest Convention on Cybercrime (2001)

The Convention on Cybercrime, or Budapest Convention, is in fact the first international treaty to address crimes committed via the internet and other computer networks. More than 60 states, including several non-European ones, have ratified the Convention since its adoption by the Council of Europe in 2001. This treaty provides common ground for the definitions, investigations, and prosecution of cybercrime, helping increase international cooperation with mutual legal assistance and information exchange. It addresses a variety of cyber offenses, like anything governed by a computer system, crimes related to content (like child pornography and hate speech), and crimes related to data (like illegal interception or fraud). The Convention also mandates the establishment of *"24/7 points of contact"* in participating countries, to facilitate prompt inquiries in cross-border investigations (Clough, 2014; Khan et al., 2020).

It places a particular emphasis on mutual assistance in criminal matters, which is one of the key provisions of the Budapest Convention. The treaty enables member states to provide immediate cooperation when multiple states are involved in a cybercrime investigation, given the rapidity and global nature of cybercrimes. However, some countries, such as Pakistan, have not yet ratified the Convention, which prevents them from participating in swift international collaboration.

General Data Protection Regulation (GDPR) (2018)

The GDPR, first established by the European Union in 2018, is pioneering legislation that aims to enhance the data protection and privacy rights for individuals in the EU. Although not dedicated to cybercrime, its insights are extremely relevant for online violations such as identity theft, personal data breaches, or unauthorized access to digital systems. GDPR, which goes into effect May 25, 2018, requires organizations to apply strict protections over data security, report data breaches within 72 hours, and allow individuals more control over their personal data. GDPR Global Litigation Counsel Global data transfers and extraterritoriality the extraterritoriality of GDPR (which applies to any organization located outside of the EU that processes the personal data of EU residents) and its restrictions on international data transfers play a large role in the cyber security space. It prompted other nations to consider implementing data protection regulations in order to strengthen privacy protections and better target cybercrime related to data security (GDPR, 2016; Kahn & Wu, 2020).

United Nations (UN) and Cybercrime

The United Nations has also responded to the global challenge of cybersecurity through various initiatives. The UN Office on Drugs and Crime (UNODC) plays a crucial role in fostering international cooperation to combat cybercrime, particularly in developing nations. The UN identified cybercrime as one of the most serious threats to global security and therefore called for the establishment of national legal frameworks to prevent online crime while enhancing international cooperation regarding cybercrime, especially at a national, regional, and global level relating to the fields of financial crimes, identity theft, and terrorism. In 2021, the UN General Assembly passed a resolution mandating the creation of an international cybercrime treaty, which would require states to collaborate in preventing and prosecuting activities that fall under state criminal jurisdiction. This follow-up effort continues the work of the UN, which includes the UN Office of the High Commissioner for Human Rights and Adopted Resolutions, with the aim of strengthening these international legal frameworks in the digital age (Tennis, 2020).

African Union (AU) Convention on Cyber Security and Personal Data Protection (2014)

At a regional level, the African Union (AU) has also embarked on initiatives to counter cybercrimes. In 2014, African countries adopted the African Union Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention, to establish uniform standards for cybersecurity and personal data protection. The convention aims to address many issues, such as the reform of laws to

prevent cybercrime, data protection, cybersecurity awareness, and capacity building. The overall objective of the Malabo Convention is to harmonize cyber regulations in Africa with a cohesive framework for countering cyber threats (Union, 2014).

Challenges and Gaps in the International Framework

Although international instruments have taken us a long way in shaping standards for cybercrime, there are still major gaps and challenges. Similar to the Budapest Convention, it does not fully cover certain regions, as some countries are not parties to the agreement. Cycle neutrality also leans on the jurisdictional complexities that cybercriminals frequently abuse; even in the territory of a single state at any given moment, the offender can be located in a different state from the end of the crime, thus complicating cross-border legal cooperation. In addition, international legal frameworks must constantly update as the cybercrimes change. Laws have not kept pace with emerging challenges such as ransomware attacks, deepfake technologies, and the malevolent use of artificial intelligence. To enhance the effectiveness of legal frameworks, we require more agreements and improved international collaboration. In general, although the international legal regime against cybercrime lays down the basic groundwork for international cooperation among states, states still need to reinforce their domestic legal instruments, ratify international law treaties, and modernize the legislative system in line with challenges created by new forms of cyberthreats to combat cybercrime in an efficient way in the future (Muff et al., 2017).

COMPARATIVE ANALYSIS OF PAKISTAN'S CYBERCRIME LAW WITH INTERNATIONAL STANDARDS

Scope and Coverage

The reach and breadth of the Budapest Convention on Cybercrime and PECA 2016 showcase fundamental differences in each instrument's philosophy when it comes to the ambit of cybercrime offenses. The Budapest Convention outlines a wide-ranging and specific regime to address acts defined as cybercrime that fall broadly into categories of illegal access to computer systems, data interference, fraud, and offenses against the content (child exploitation and hate speech, for example). The draft treaty also stresses the importance of international cooperation and mutual legal assistance in dealing with cybercrime in light of its transnational consequences. Covering both traditional and emerging threats of the cyber world—cyberterrorism, online fraud, and the use of technology for criminal purposes—the Convention is thus wide-ranging in its scope. It offers instructions to tackle new-age threats emerging, i.e., ransomware, botnets, and advanced levels of phishing attacks (Akhtar, 2023).

In comparison, PECA 2016 considers cybercrime in a more limited manner. Though it includes major crimes like data theft, hacking, and cyber fraud, it does not effectively cover the new types of cybercrimes, like ransomware and advanced phishing techniques. In the context of fast-evolving digital technologies, these gaps in PECA coverage are stark during a time when cybercriminals are constantly evolving to exploit new vulnerabilities. PECA lacks the necessary provisions against such emerging cybercrimes, thus making itself redundant with regards to the increasing digital menace to Pakistan (Saleem et al., 2024).

Another differentiator is data protection. While PECA 2016 incorporates data privacy provisions, their scope is narrower and less comprehensive than the GDPR's data protection standards. As a regulation from the European Union, GDPR has stringent rules around data processing and security, as well as stronger rights for individuals in relation to their personal data. It similarly requires timely notification of breaches, protections against unauthorized access to data, and security measures. However, PECA lacks this extensive data protection provision, leaving gaps in Pakistan's legislative regime for the protection of personal data in the digital domain. In conclusion, while both the Budapest Convention and PECA 2016 have adequately addressed the most crucial elements for combating cybercrime, the Convention's broad coverage of cybercrime, attention to emerging trends in cybercrime, and its inherent

superior data protection provisions significantly contribute to the adequate legal regulation of cybercrime compared to PECA. PECA can undergo improvements and amendments to effectively address emerging cyber threats and enhance data protection, aligning with international standards GDPR (Imtiaz, 2024).

International Cooperation

International cooperation is seamless, with member countries able to request legal assistance, exchange evidence, and conduct joint investigations in real time under the Budapest Convention. Given the global nature of cybercrime, this multilateral framework is essential as it allows for the swift and effective cooperation of law enforcement agencies to act against digitally transmitted crimes. The Convention's 24/7 points-of-contact system enhances the capacity for urgent cooperation among countries in cybercrime prevention and investigation, enabling states to swiftly investigate and prosecute cybercriminals (Hwang, 2015).

However, Pakistan's non-participation in the Budapest Convention significantly hinders its ability to facilitate simplified, multilateral legal collaboration in cybercrime investigations. Pakistan, on the other hand, must use bilateral treaties and MLATs whenever it wants to request assistance from foreign states in relation to cybercrime. While MLATs serve as valuable tools for collaboration, they often lack the efficiency of the Budapest Convention when operating within a multilateral framework. Opening up an MLAT is lengthy and/or cumbersome, if possible, at all, depending upon the wording of the treaty. Consequently, these bilateral arrangements, while valuable, tend to be inefficient in the face of swift-moving cyber threats.

The absence of an all-inclusive multilateral framework puts Pakistan as a marginalized player in a quagmire of cross-border cybercrime. Internet anonymity allows cybercriminals to launch attacks from their own jurisdiction, giving them an advantage over investigators helping victims in other jurisdictions. In such instances, the swift delivery of justice against cybercriminals necessitates timely legal collaboration and rapid evidence exchange. But this dependence on bilateral treaties and MLATs implies that Pakistan would need to contend with time delays and issues of jurisdiction that restrict its response against global cyber threats. This widening gap in international cooperation hinders Pakistan's ability to participate in the global fight against cybercrime and highlights the necessity for Pakistan to explore opportunities for improved alignment within international legal frameworks such as the Budapest Convention. This would enable Pakistan to effectively and swiftly address the challenges of rapid technological advancement and digitized crime (Niazi et al., 2022).

Privacy and Human Rights Concerns

The issue stems from PECA 2016's interpretation of cyber offenses, which, as I will delve deeper into later in this article, is expansive and, at times, imprecise, leading to a broad range of applications and, consequently, abuse. The law has criminalized anything from cyber harassment to defamation and online blasphemy with insufficiently precise meanings or clear rules for enforcement. Fears of misuse of PECA as a tool to silence dissent and related conduct, which should more appropriately be considered a petty offense than a crime, have arisen from this vagueness. In addition, PECA itself vests sweeping powers in the FIA, for instance, to track online activity, grab gadgets, and carry out searches and seizures without proper judicial oversight. Critics argued that these powers, designed to equip law enforcement agencies for cybercrime enforcement, were invasive and susceptible to abuse. The continued implementation of PECA 2016, coupled with the threat of fines and sanctions by authority figures, has the potential to lead to violations of human rights in the form of restrictions on freedom of expression, privacy, and due process (Nandy,2023).

By contrast, international responses such as the Budapest Convention and GDPR are more focused on protecting personal privacy and civil liberties in their approaches to cybercrime. It enhances the investigative powers outlined in the Budapest Convention, while upholding the fundamental principle

of maintaining a balance between security and individuality in the exercise of investigatory powers. The Convention establishes the parameters for data access and sharing, and mandates member states to uphold human rights in their investigations and prosecutions of cybercrimes. The Convention also incorporates safeguards to prevent data abuse or misuse of police powers and ensures the preservation of individual privacy rights during cross-border cooperation.

Likewise, the GDPR will likely foster security by safeguarding personal data and privacy. Whereas PECA has come under fire for its overly sweeping clauses on data collection and surveillance, the GDPR is prescriptive in that it places stringent requirements on data processing, storage, and transfer (except between a few select domains). Companies must maintain transparency with individuals, grant them control over their data, and implement safeguards to prevent breaches and abuse of personal information. Also, in case of a breach, GDPR obliges to notify data subjects and gives remedies to individuals whose rights are infringed—a higher level of privacy protection as compared to wither of the two laws (Kearns, 1998).

While acknowledging the importance of security, the Budapest Convention and GDPR caution against pursuing security at the expense of civil liberties and privacy rights. These global frameworks illustrate a more nuanced approach to combating cybercrime by including protections against abuse of state authority and protection of individual human rights. In contrast, PECA, with its potentially far-reaching effects and insufficient safeguards concerning rights to privacy or due process, represents a worrying gap in Pakistan's cybercrime legislation in terms of its systemic misalignment, making it vulnerable to abuses of human rights in enforcement.

KEY CHALLENGES IN PAKISTAN'S CYBERCRIME FRAMEWORK

Limited Institutional Capacity

One of the critical challenges in combating cybercrime in Pakistan is the limited capacity of its enforcement agencies, particularly the FIA, which is responsible for investigating cyber offenses under the PECA 2016. The FIA faces significant resource constraints, including inadequate funding, insufficient technological infrastructure, and a lack of specialized technical expertise, all of which undermine its ability to effectively address the increasingly complex nature of cybercrimes. As digital threats evolve, including issues such as hacking, ransomware attacks, identity theft, and online financial fraud, the need for skilled personnel proficient in areas like digital forensics, encryption, and cybersecurity becomes paramount. However, the FIA is severely under-resourced in these areas. Moreover, the growing caseload of cybercrime cases further burdens the agency, as the rapid increase in internet usage and digital transactions has led to a surge in cybercrime incidents. With the agency already stretched thin across various criminal investigations, it struggles to keep pace with the rise in cybercrime reports, resulting in delayed responses, ineffective investigations, and a reduced capacity to prevent and prosecute digital offenses. Compounding this issue is the FIA's challenge in coordinating with other law enforcement agencies and private sector stakeholders, which is essential for addressing cross-border cybercrimes that require international cooperation, rapid information sharing, and specialized technical assistance. As a result, the FIA's limited capacity to handle cybercrime investigations effectively poses a significant obstacle to Pakistan's ability to protect its citizens and institutions from the growing threat of digital offenses, highlighting the urgent need for increased resources, enhanced technical training, and improved interagency and international collaboration to strengthen Pakistan's overall response to cybercrime (Sattar et al., 2018).

Gaps in Legislation

PECA 2016 is relatively new and, as such, has struggled to keep pace with the rapidly evolving landscape of cybercrime. One of the main issues with the law is that emerging cyber threats often outpace the capacity for legislative updates. While the law covers general cyber offenses like unauthorized access to data and hacking, it lacks specific provisions to address newer, more

sophisticated forms of cybercrime, such as ransomware attacks, which have become increasingly prevalent. Ransomware attacks, which involve malicious software designed to encrypt a victim's data and demand payment for its release, represent a significant and growing threat to individuals, businesses, and government entities. However, PECA does not explicitly define or address ransomware, leaving a gap in legal protections and investigative tools for law enforcement agencies tackling such crimes. Additionally, the provisions in PECA regarding electronic evidence and data preservation are insufficiently detailed. As cybercrimes often rely heavily on digital evidence, ensuring that such evidence is properly handled and preserved for court proceedings is crucial. However, PECA does not provide comprehensive guidelines on how to collect, preserve, and authenticate electronic evidence, which raises concerns about its admissibility in court. Without clear standards for digital evidence handling, there is a risk that important data could be lost, tampered with, or deemed inadmissible, weakening the prosecution's case. This lack of clarity in handling electronic evidence and updating the law to address emerging cyber threats underscores the need for ongoing revisions to PECA 2016 to keep pace with technological advances and ensure that Pakistan's legal framework remains effective in combating the complex and evolving nature of cybercrime (Nadeem et al., 2023).

Weak International Collaboration

Pakistan's absence from the Budapest Convention on Cybercrime significantly limits its ability to collaborate effectively on international cybercrime cases. The Budapest Convention, being the first international treaty to address cybercrime comprehensively, enables member countries to request legal assistance, share evidence, and conduct joint investigations swiftly. This multilateral framework allows for real-time cooperation between countries, which is crucial in dealing with cybercriminals who often operate across borders. Without being a signatory to the Convention, Pakistan misses out on these streamlined mechanisms for international cooperation, which can hinder its ability to respond quickly to cross-border cybercrimes. Instead, Pakistan relies on MLATs, which are typically bilateral agreements between countries that establish procedures for legal cooperation. While MLATs are important for international collaboration, they are often slow, bureaucratic, and involve complex paperwork, making them ill-suited for the fast-paced nature of cybercrime investigations. The process of initiating MLAT requests can take weeks or even months, which is a significant disadvantage when dealing with urgent cybercrimes such as data breaches, ransomware attacks, or online fraud. These delays can allow cybercriminals to evade justice or cause further damage, undermining Pakistan's ability to protect its citizens and institutions from digital threats. This reliance on slower, less efficient methods of cooperation underscores the need for Pakistan to consider ratifying the *Budapest Convention*, which would improve its ability to engage in timely and effective international collaboration to combat cybercrime (Khan, 2024).

Challenges of Jurisdiction and Cross-Border Crime

Cybercrimes often involve perpetrators who operate from multiple countries, creating significant jurisdictional challenges for law enforcement agencies. These crimes typically transcend national borders, with criminals leveraging the global nature of the internet to target victims across different jurisdictions. In such cases, prosecuting cybercriminals becomes complex, as the legal frameworks in one country may not have the authority or reach to apprehend or prosecute offenders located in another country. Pakistan's laws, including the PECA 2016, have limited extraterritorial reach, which restricts the government's ability to act against cybercriminals residing outside its borders. While PECA does provide some provisions for international cooperation, such as MLATs, the lack of a robust, extraterritorial framework for cybercrime prosecution means that many offenders can operate with relative impunity from jurisdictions where their actions may not be criminalized or effectively prosecuted. This limitation becomes particularly problematic in cases of advanced cybercrimes like hacking, identity theft, and ransomware attacks, where perpetrators often use servers and networks in different countries to carry out their crimes. Without the legal tools and mechanisms to extend

Pakistan's jurisdiction beyond its borders, law enforcement agencies face significant obstacles in pursuing and prosecuting international cybercriminals. This gap emphasizes the need for Pakistan to strengthen its extraterritorial legal provisions, improve international cooperation frameworks, and consider aligning its laws with global conventions like the Budapest Convention to better address the transnational nature of cybercrime (Khan, 2024).

LESSONS FROM INTERNATIONAL LEGAL FRAMEWORKS

Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime provides a strong model for international cooperation in the fight against cybercrime, which Pakistan could adopt to enhance its own legal framework. The Convention emphasizes the importance of shared procedures for cross-border investigations, enabling member countries to collaborate in real-time on cybercrime cases. This is particularly valuable given the transnational nature of cybercrimes, where perpetrators often operate from multiple jurisdictions, and the evidence and data needed for prosecution are dispersed across borders. By adhering to the Budapest Convention, Pakistan could benefit from established protocols for mutual legal assistance, the swift exchange of evidence, and joint investigations with foreign enforcement agencies. This cooperation is crucial when investigating complex cybercrimes, such as ransomware attacks, data breaches, and online fraud, where time is of the essence and rapid action is necessary to prevent further damage. Currently, Pakistan's reliance on MLATs can be slow and bureaucratic, hindering the ability to respond swiftly. The Budapest Convention offers a more efficient and standardized approach to handling cross-border cybercrime cases, reducing delays and streamlining the process of obtaining evidence and assistance from other countries. Additionally, the Convention's emphasis on mutual respect for human rights and data privacy ensures that international cooperation does not come at the expense of individual freedoms. By aligning its cybercrime laws with the Budapest Convention, Pakistan could significantly improve its capacity to tackle cybercrime, strengthen collaboration with international law enforcement agencies, and close the gaps in its legal framework for addressing transnational cyber threats (Khan & Jiliani, 2023).

European Union's GDPR

The GDPR provides a comprehensive framework for data protection, emphasizing privacy as a fundamental human right and establishing strict standards for the collection, processing, storage, and sharing of personal data. Integrating GDPR-inspired principles into Pakistan's PECA 2016 could significantly enhance the protection of Pakistani citizens' personal data, ensuring stronger safeguards against misuse or unauthorized access. By incorporating provisions that promote transparency in data handling, require clear consent for data collection, and offer individuals more control over their personal information, Pakistan could build greater public trust in its digital services. Additionally, adopting GDPR-like standards would align Pakistan's legal framework with international best practices, improving the country's reputation in the global digital economy and facilitating smoother cooperation with international bodies focused on privacy and data security. This integration would also help ensure that Pakistan's citizens enjoy robust privacy protections, contributing to a safer and more secure digital environment (Khan, 2023).

United States' Cyber Legislation

The GDPR provides a comprehensive framework for data protection, emphasizing privacy as a fundamental human right and establishing strict standards for the collection, processing, storage, and sharing of personal data. Integrating GDPR-inspired principles into Pakistan's PECA 2016 could significantly enhance the protection of Pakistani citizens' personal data, ensuring stronger safeguards against misuse or unauthorized access. By incorporating provisions that promote transparency in data handling, require clear consent for data collection, and offer individuals more control over their personal information, Pakistan could build greater public trust in its digital services. Additionally, adopting

GDPR-like standards would align Pakistan's legal framework with international best practices, improving the country's reputation in the global digital economy and facilitating smoother cooperation with international bodies focused on privacy and data security. This integration would also help ensure that Pakistan's citizens enjoy robust privacy protections, contributing to a safer and more secure digital environment (Khan & Ximei, 2022).

RECOMMENDATIONS

1. Enhance Legislation: PECA 2016 should be amended to include emerging cyber threats such as ransomware and provide a more comprehensive framework for data protection.
2. Sign the Budapest Convention: Pakistan should consider joining the Budapest Convention to strengthen international cooperation and facilitate cross-border investigations.
3. Strengthen Institutional Capacity: Investment in training, technical infrastructure, and resources for the FIA and judiciary is essential to improve enforcement and case processing.
4. Promote Public Awareness and Education: Cyber literacy programs could help citizens recognize and protect themselves against cyber threats.
5. Establish Clear Privacy Safeguards: Reforms to PECA could focus on aligning with international standards on data protection, providing citizens with greater transparency and privacy rights.

CONCLUSION

In conclusion, the research underscores the significant challenges Pakistan faces in combating cybercrime due to gaps in its legal framework, limited enforcement capacity, and lack of international cooperation mechanisms. While the PECA 2016 serves as the primary legislative tool for addressing cybercrimes, its broad and vague provisions, limited extraterritorial reach, and lack of specific guidelines for emerging threats like ransomware hinder its effectiveness. Moreover, Pakistan's absence from the Budapest Convention* and reliance on slow, bureaucratic MLATs further complicate cross-border collaboration in cybercrime investigations. To enhance its capacity to tackle these digital threats, Pakistan could benefit from integrating GDPR-inspired data protection principles into PECA, which would bolster privacy rights and public trust in the digital environment. Additionally, clearer and more comprehensive definitions of cybercrimes, similar to the CFAA in the U.S., would improve the ability of enforcement agencies to identify and prosecute offenders effectively. Future research could explore the feasibility of aligning Pakistan's legal framework with international standards, such as the Budapest Convention and GDPR, and examine the potential for improving the capacity and training of Pakistan's law enforcement agencies to better address the growing complexity of cybercrimes. By addressing these issues, Pakistan could strengthen its legal infrastructure, enhance its response to cybercrime, and ensure better protection for its citizens in the digital age.

References

Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. (2021). Digital Economy Barriers to Trade Regulation Status, Challenges, and China's Response. *International Journal of Social Sciences Perspectives*, *8*(2), 41-49.

Ahmad, S., & Khan, R. (2021). *Challenges in enforcing cybercrime laws in Pakistan: An institutional perspective*. Journal of Cybersecurity Studies, 5(2), 134-150.

Akhtar, S. (2023). Assessing the Cybercrime Legislation in Pakistan: a Comparative Study of European Union and Pakistani Cybercrime Laws. *Available at SSRN 4519368*.

Ali, M. (2019). *Evaluating the effectiveness of Pakistan's Prevention of Electronic Crimes Act (PECA) 2016*. International Journal of Law and Information Technology, 27(3), 245-263.

Biedron, S. R. (2024). *Cybercrime in the Digital Age* (Doctoral dissertation, University of Oxford).

Clough, J. (2014). A world of difference: The Budapest convention on Cybercrime and the challenges

of Harmonisation. *Monash University Law Review*, *40*(3), 698-736.

Council of Europe. (2001). *Convention on Cybercrime*. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

GDPR, G. D. P. R. (2016). General data protection regulation. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*.

Gercke, M. (2012). *The Budapest Convention on Cybercrime: A study of its implementation and impact*. European Journal of Crime, Criminal Law and Criminal Justice, 20(2), 123-145.

Hussain, A. (2017). *PECA 2016 and human rights: Balancing security and privacy in Pakistan*. Human Rights Law Review, 17(1), 89-105.

Hwang, S. G. (2015). *A Comparative Study on the Legal Systems on Cybercrime between South Korea and Pakistan-Focussed on the Cybercrime Response System* (Doctoral dissertation, 한양대학교).

Imtiaz, S. (2024). Cybercrime and Rule of Law in Pakistan: Placing in Context of Developing Countries. *Research Journal of Human and Social Aspects*, *2*(1), 29-36.

Jamshed, J., Rafique, W., Baig, K., & Ahmad, W. (2022). Critical analysis of cybercrimes in Pakistan: Legislative measures and reforms. *International Journal of Business and Economic Affairs*, *7*(1), 10-22.

Kahn, A., & Wu, X. (2020). Impact of digital economy on intellectual property law. *J. Pol. & L.*, *13*, 117.

Kearns, T. B. (1998). Technology and the right to privacy: the convergence of surveillance and information privacy concerns. *Wm. & Mary Bill Rts. J.*, *7*, 975.

Khan, A. (2022). E-commerce Regulations in Emerging Era: The Role of WTO for Resolving the Complexities of Electronic Trade. *ASR Chiang Mai University Journal Of Social Sciences And Humanities*.

Khan, A. (2023). Rules on Digital Trade in the Light of WTO Agreements. *PhD Law Dissertation, School of Law, Zhengzhou University China*.

Khan, A. (2024). The Emergence of the Fourth Industrial Revolution and its Impact on International Trade. *ASR: CMU Journal of Social Sciences and Humanities (2024) Vol*, *11*.

Khan, A. (2024). The Intersection Of Artificial Intelligence And International Trade Laws: Challenges And Opportunities. *IIUMLJ*, *32*, 103.

Khan, A. S. I. F., Amjad, S. O. H. A. I. L., & Usman, M. U. H. A. M. M. A. D. (2020). The Evolution of Human Rights Law in the Age of Globalization. *Pakistan journal of law, analysis and wisdom*.

Khan, A., & Jiliani, M. A. H. S. (2023). Expanding The Boundaries Of Jurisprudence In The Era Of Technological Advancements. *IIUMLJ*, *31*, 393.

Khan, A., & Wu, X. (2021). Bridging the Digital Divide in the Digital Economy with Reference to Intellectual Property. *Journal of Law and Political Sciences*, *28*(03), 256-263.

Khan, A., & Wu, X. (2021). Reforms for culmination of the deadlock in appellate body of WTO: An agenda of saving the multilateral trading system. *Journal of Humanities, Social and Management Sciences (JHSMS)*.

Khan, A., & Ximei, W. (2022). Digital economy and environmental sustainability: Do Information

Communication and Technology (ICT) and economic complexity matter?. *International journal of environmental research and public health*, *19*(19), 12301.

Khan, A., Abd Elrhim, A. A., & Soomro, N. E. (2021). China Perspective in Reforming of the World Trade Organization. *J. Pol. & L.*, *14*, 104.

Khan, A., Amjad, S., & Usman, M. (2020). The Role of Customary International Law in Contemporary International Relations. *International Review of Social Sciences*, *8*(08), 259-265.

Khan, A., Jillani, M. A. H. S., Abdelrehim Hammad, A. A., & Soomro, N. E. H. (2021). Plurilateral negotiation of WTO E-commerce in the context of digital economy: Recent issues and developments. *Journal of Law and Political Sciences*.

Khan, A., Usman, M., & Amjad, S. (2020). Enforcing Economic, Social, and Cultural Rights: A Global Imperative. *International Review of Social Sciences (IRSS)*, *8*(09).

KHAN, A., USMAN, M., & RIAZ, N. (2021). The Intersectionality of Human Rights: Addressing Multiple Discrimination. *Asian Social Studies and Applied Research (ASSAR)*, *2*(03), 498-502.

Khan, H., Shabbir, S. S., & Qureshi, A. N. (2024). Revamping Cybercrime Laws In Pakistan: A Comparative Analysis Of Pakistan And United Kingdom.

KHAN, M. I., USMAN, M., KANWEL, S., & Khan, A. (2022). Digital Renaissance: Navigating the Intersection of the Digital Economy and WTO in the 21st Century Global Trade Landscape. *Asian Social Studies and Applied Research (ASSAR)*, *3*(2), 496-505.

Khan, S. (2018). *Broad provisions and their implications: A critique of PECA 2016*. Pakistan Law Review, 10(4), 301-320.

Lee, J., & Kim, H. (2022). *Adapting cybercrime legislation to emerging threats: Lessons for developing countries*. Journal of Information Security, 14(1), 45- sixty-seven.

Muff, K., Kapalka, A., & Dyllick, T. (2017). The Gap Frame-Translating the SDGs into relevant national grand challenges for strategic business opportunities. *The International Journal of Management Education*, *15*(2), 363-383.

Nadeem, M. A., Hashmi, S., & Khan, M. A. (2023). Exploring the Interplay of Cybersecurity and cybercrime in Pakistan's Digital Landscape. *Contemporary Issues in Social Sciences and Management Practices*, *2*(4), 207-222.

Nandy, D. (2023). Human rights in the era of surveillance: balancing security and privacy concerns. *Journal of Current Social and Political Issues*, *1*(1), 13-17.

Niazi, B. K. N. B. K. (2022). Exploring and Critically Analyzing Cybercrime Legislation and Digital Rights in Pakistan: Challenges and Prospects. *Indus Journal of Law and Social Sciences*, *1*(1), 1-8.

Raza, H. (2020). *Institutional challenges in combating cybercrime in Pakistan*. Journal of Law and Society, 38(3), 289-307.

Riaz, N., Khan, A., & Usman, M. (2022). Legal Frameworks for Combatting Piracy under International Law: Evolving Strategies and Challenges. *Asian Social Studies and Applied Research (ASSAR)*, *3*(01), 284-291.

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: a case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, 1-29.

Sattar, Z., Riaz, S., & Mian, A. U. (2018, November). Challenges of cybercrimes to implementation of legal framework. In *2018 14th International Conference on Emerging Technologies (ICET)* (pp.

1-5). IEEE.

Smith, J. (2020). *The Computer Fraud and Abuse Act: Strengths, weaknesses, and future directions.* American Journal of Criminal Law, 48(2), 211-230.

Tennis, M. M. (2020). A United Nations convention on cybercrime. *Cap. UL Rev.*, *48*, 189.

Union, A. (2014). African Union convention on cyber security and personal data protection. *African Union*, *27*.

Usman, M. U. H. A. M. M. A. D., Khan, A. S. I. F., & Amjad, S. O. H. A. I. L. (2021). State Responsibility and International Law: Bridging the Gap.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

Yar, M., & Steinmetz, K. (2019). *Cybercrime and the global south: A comparative analysis of legislative responses*. International Criminal Justice Review, 29(4), 512-529.

Zahid, M. A., Muhammad, A., Khakwani, M. A. K., & Maqbool, M. A. (2024). Cybercrime and Criminal Law in Pakistan: Societal Impact, Major Threats, and Legislative Responses. *Pakistan Journal of Criminal Justice*, *4*(1), 223-245.

Zahoor, R., & Razi, N. (2020). Cyber-crimes and cyber laws of Pakistan: An overview. *Progressive Research Journal of Arts & Humanities (PRJAH)*, *2*(2), 133-143.