# 

**Cybercrime Laws in Pakistan: An Examination and Strategies for Enhancement**

**Information Security Project**



National University of Computer and Emerging Sciences

Department of Computer Science

Lahore, Pakistan

**Table of Contents**

[**1. Abstract 3**](#_s7embupswueq)

[**2. Introduction 4**](#_j9b36dq3rlxc)

[**2.1 Goals 4**](#_fkei53n3lyqn)

[**3. Motivations 5**](#_c90u2rs1pdz6)

[**4. Literature Review 6**](#_lm64o4nvioyc)

[**4.1. Legal Framework for Policing Cyberspace in Pakistan: An Overview 6**](#_1jjyynhvx01i)

[**4.2. Analysis of Pakistan’s Cyber Crime Bill 6**](#_zc9h08k67ddw)

[**4.3. Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan 7**](#_ojoagin0q295)

[**4.4. Legal Challenges in Enforcing Cybercrime Laws 8**](#_qm871hk4kqg1)

[**4.5. Need of International Legislation Regarding Cyber Crime: Pakistan Perspective 8**](#_t6ju92tz6b3q)

[**4.6. Cyber Laws in Pakistan: Protecting Business and Personal Data 10**](#_19toa6ypubi)

[**4.7. Cybercrime in Pakistan: A Study of the Law Dealing With Cyber Crimes in Pakistan 11**](#_7wkie22lrbd3)

[**4.8. Assessing the Cybercrime Legislation in Pakistan: A Comparative Study of European Union and Pakistani Cybercrime Laws 11**](#_b1ld1kr9gcms)

[**4.9. Protecting Online Privacy in Pakistan 12**](#_nqx6vh7s8i0u)

[**5. Analysis 13**](#_bpllce3pz93h)

[**6. Conclusion 14**](#_vjzreo57idpu)

[**6.1. Recommendations 14**](#_egwg3xhbbjux)

[**7. References 16**](#_z0z8rb9gaje9)

# 

# 

# 

# **Abstract**

As technology advances, so do measures to bypass means of security. Cybercrime has become a prominent issue worldwide, but in matters like this, one is highly dependent on the legal system for protection. In Pakistan, a prominent issue that has been reported is inadequate laws. This gives rise to the risk of cybercrimes since there are no specific means of punishment or adequate protection from them. As a result, it has become a compulsion to analyze these laws to determine their efficiency. In this paper, we have first proven the need for this analysis. After this, ten publications have been examined thoroughly to determine the effectiveness of the laws that are currently in place in Pakistan. Lastly, we have provided recommendations to improve the legal system in areas that are lacking. As a result, this paper aims to persuade amendments in the legislature so that individuals may safeguard themselves in cyberspace.

# 

# **Introduction**

The way laws and regulations are structured is that to be considered in criminal court, one must, beyond any reasonable doubt, have committed a crime that goes against those laws. This is where the problem arises. If an attacker carries out a malicious activity that is not directly stated as a law, it is relatively easier for them to get away with it.

In this report, we will analyze the existing laws laid out by the Pakistani government and identify the extent of protection and criminalization they allow. After this, we will highlight differences, weaknesses, and areas for improvement in the current laws while comparing them to the laws of other countries. This analysis will highlight not only the negative but also the positive aspects.

An examination will allow us to determine the extent of success that Pakistan’s current laws provide. It will also help identify what it is lacking and what can be done to improve the state of these laws. As a result, the cyber sector in Pakistan, along with its users, will be more secure.

## **2.1 Goals**

With this project, we aim to accomplish the following:

* Analyze existing cyber laws in Pakistan.
* Identify the positives and negatives.
* Provide suggestions that could improve the state of cyber laws in Pakistan.

# 

# **Motivations**

The Prevention of Electronic Crimes Act (PECA) was introduced in Pakistan in 2016, which is incredibly late to begin with. It has since been updated in February 2022 [1] to include more instances. However, there are various elements that remain ambiguous or untouched throughout the act. “The Prevention of Electronic Crimes Act neither protects the public from legitimate cybercrime concerns nor respects fundamental human rights,” said Patricia Gossman [1]. This clearly proves the need for a detailed analysis of the laws that currently exist in this act and what can be done to improve them.

Here are some key reasons why this is important:

* The rapid advancement of technology has resulted in a surge in cyber dangers. Improving cybercrime laws gives legal resources to effectively tackle emerging threats and keep up with changing circumstances.
* To safeguard the rights and interests of people and companies doing business online, cybercrime laws must be strengthened [5].
* Strong cybercrime laws serve as a deterrent by defining violations precisely and imposing suitable punishments. This discourages cybercriminals and guarantees that those who commit cybercrime will face the proper consequences.
* Cybercrime laws are essential for protecting the interests of national security because they make it possible to prosecute individuals who engage in activities that endanger the stability and security of the nation.

# 

# **Literature Review**

This section discusses various papers that reflect on the conditions of cybercrime laws in Pakistan.

## **Legal Framework for Policing Cyberspace in Pakistan: An Overview**

In this overview, Adil goes into detail while analyzing the various cybercrime acts that have come forward in the past. He argues that modern states have tried to respond to challenges of cyberspace (social wants) through the (social) institution of law [2]. As a result, these laws end up being a form of criminal or regulatory law instead of being a separate entity. He believes that this is where the main problem lies.

The Federal Investigation Agency (FIA) serves as the primary federal police organization in Pakistan. The FIA's jurisdiction, outlined in a schedule, covers offenses such as human smuggling, trafficking, immigration, cybercrimes, official secrets, corporate crimes, money laundering, counter-terrorism financing, and high treason. Notably, the FIA is the sole authorized agency for investigating computer, internet, and information technology-related offenses.

In terms of preventive and regulatory responsibilities related to blocking websites and content regulation, the Pakistan Telecommunication Authority (PTA) plays a crucial role. Over time, the absence of a regulator for telecommunication media has led the PTA to take on policing functions through various delegated legislation.

The Prevention of Electronic Crimes Act, 2016 (PECA) is the primary legislation in Pakistan addressing cybercrimes, encompassing twenty-three offenses related to activities in cyberspace and on digital devices. PECA serves both substantive and procedural purposes, detailing the authorized investigation agency for cybercrimes, currently limited to the FIA. The law also addresses preventive measures, grathernting the Federal Government the power to issue directions to information system owners and establish Computer Emergency Response Teams. The PEC Rules outline the structure of the FIA's Cybercrime Wing, and a complaints registry mechanism is established. According to Adil, the comprehensive legal and regulatory approach reflects the country's commitment to addressing cybercrimes and securing the digital realm.

## **Analysis of Pakistan’s Cyber Crime Bill**

This paper [3] highlights some of the issues that exist in Pakistan’s latest cybercrime bill in great detail.

The bill's Sections 3 and 4 broadly criminalize intentional access to "any" information system or data and the unauthorized copying and transmission of "any" data[3]. This language criminalizes actions regardless of the nature of the data. To address this, the sections should be more specific. Additionally, the bill should be amended to criminalize only when done with the intent to cause loss or harm.

Section 10 of the bill defines cyberterrorism, encompassing acts like unauthorized access to critical infrastructure information systems, glorification of an offense, unauthorized copying or transmission of critical data, hate speech interference with critical infrastructure information and systems or data. The definition includes the intent to produce fear or foster religious, ethnic, or sectarian dispute. However, the lack of clear definitions raises concerns. Section 10 imposes severe penalties, including 14 years of imprisonment and/or a fine of up to 15 million rupees, for offenses related to cyber-terrorism or threats to commit these acts. The same penalties apply to glorification of a person with these charges.

Section 22 of the bill defines spamming as a transmission of "harmful, fraudulent, misleading, illegal, or unsolicited intelligence to any person without the express permission of the recipient." The inclusion of "unsolicited" implies that sending emails, photos, text messages, or posting content on social networks without a recipient's permission would be considered an offense. This provision is seen as a potential hindrance to the free flow of communication.

Section 43 of the bill grants the government the ability to issue guidelines to service providers for preventing offenses under the Act, but there is a lack of precision, safeguards, and restrictions. Several worrisome developments are noted, including the removal of many procedural guarantees present in previous versions of the bill. The disappearance of safeguards for self-incrimination and the absence of references to the defendant's right to know charges are particularly disturbing. However, some positive aspects are acknowledged compared to earlier drafts.

## **Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan**

In this paper [4], the authors discuss the cyber laws until 2019 and how they have influenced various scenarios. Their critique of the 2016 cybercrime bill is well-detailed. The bill aimed to address public concerns and prosecute offenders effectively. However, their analysis highlighted significant shortcomings. They emphasized a lack of clarity in the bill. This ambiguity could lead to multiple interpretations, potentially benefiting defense lawyers and undermining the integrity of cases.

One prevalent form of cybercrime is financial crimes, encompassing money laundering, tax refund scams, and other fraudulent financial activities. In Pakistan, the impact of rising cybercrimes is particularly evident in the struggling e-business sector, where companies face challenges in implementing effective countermeasures due to technological limitations and financial constraints. Compounding the issue is the inadequate support from law enforcement agencies in identifying and punishing perpetrators.

Email spoofing, a criminal activity often leading to hacking, involves sending emails from a source that appears to be different from the actual one. The cybercriminal's motive typically involves attacking a computer by obtaining the IP address, utilizing electronic device sequence numbers, altering packet sources to make it seem like it originates from the targeted machine, disrupting communications, and introducing viruses or backdoor access for future criminal activities. In Pakistan, law enforcement agencies show minimal action against such cybercrimes, with many of these programs being disseminated publicly through methods like SMS spoofing or sending fake messages from seemingly unrelated numbers.

The need for separate laws to address cyber crimes arises due to the lack of a centralized regulating system, allowing the uncontrollable spread of the internet. Developed countries recognize the significant impact of cybercriminals on society and prioritize advancing legal systems, cyber laws, and jurisdiction procedures. In contrast, Pakistan's cyber laws need redefinition, considering all aspects and limiting escape routes for criminals.

## **Legal Challenges in Enforcing Cybercrime Laws**

The paper [8], is a comprehensive review article titled "Challenges to enforcement of cyber-crimes laws and policy" by Ajayi E. F. G., published in the Journal of Internet and Information Systems.

The interconnected nature of the global information system provides an environment where cybercriminals can operate freely and anonymously. The issue is that cybercrime happens across countries, which makes legal issues complicated. Different places have different laws, which makes it hard to handle these crimes. The problems with international laws in dealing with cybercrime arise from jurisdictional complexities, diverse legal systems, enforcement challenges, extradition issues, the lack of a universal treaty, technological advancements, digital anonymity, political considerations, and limited international cooperation.

Cybercrimes are not confined by geographical borders and it’s often difficult to send cybercriminals to other countries for trial. Problems like differences in laws, human rights concerns, and politics can get in the way.Different countries have distinct legal systems and laws. What may be considered a cybercrime in one country might not have an equivalent or similar offense in another. The foundation of any criminal prosecution lies in evidence, which can take various forms such as testimony, documents, and real evidence.

Many cybercrimes are not reported because companies worry about their reputation, the cost, and the complicated nature of investigations.Companies often fear that disclosing cybercrimes will tarnish their reputation. The cost and effort associated with solving cybercrimes stem from the technical complexity of the investigations, the global nature of cyber threats, legal challenges, language and cultural considerations, travel costs, and the resource-intensive nature of addressing cybercriminal activities.

There's often a delay or problem in making international cybercrime treaties part of a country's own laws. Making international cybercrime treaties part of a country's own laws involves a complex process that includes legislative steps, legal harmonization, translation, technical considerations, public awareness, resource allocation, political will, capacity building, and coordination with stakeholders. Police forces often don't have the right training, tools, or protection to fight cybercrime. There's also a need for more legal experts in this field.

## **Need of International Legislation Regarding Cyber Crime: Pakistan Perspective**

The article[9] looks at the issues and needs for laws on cybercrime worldwide, focusing on Pakistan.The paper shows how cybercrimes harm society by causing money loss, threatening countries' safety, and making people trust digital systems less.

In current acts, the following crimes are discussed well:

* Crime against individuals
* Crime against property
* Crime against organization
* Crime against society

However, a big problem noted is that the laws in many countries aren't strong enough to deal with cybercrimes, especially those that happen across borders. Microsoft Encarta Premium (2009) elaborates on the need to adapt legal frameworks to the borderless nature of cyber activities, exploring the various dimensions of jurisdiction, from lawmaking powers to adjudicative processes and enforcement capabilities.

Some principles are stated below:

* **The Territorial Principle:**

It reflects the sovereignty of a nation-state, allowing it to forbid criminal conduct that occurs wholly or partially within its territory.

* **The Active Personality Principle:**

It’s also known as the 'nationality theory,' asserts jurisdiction based on the nationality of the criminal, irrespective of where the crime occurred.

* **The Passive Personality Principle:**

It is often termed the 'passive nationality principle, grants jurisdiction based on the nationality of the victim.

* **The Protective Principle:**

It is also known as the 'security principle' or 'harmed forum theory,' which allows a nation to exercise jurisdiction when actions occurring outside its borders threaten its security or essential functions.

The literature then reviews laws originating from the British colonial era, including:

* The Indian Telegraph Act, 1885
* The Indian Wireless Telegraphy Act, 1933
* The Electronic Transaction Ordinance, 2002, a pivotal step in promoting electronic banking and facilitating transactions in electronic form.
* Payment Systems and Electronic Fund Transfer Act, 2007, for the growth of financial applications and services
* The Prevention of Electronic Crimes Act, 2016 (PECA) aimed to prevent unauthorized activities related to information systems and addresses associated crimes.

The literature's view of PECA is worth noting, emphasizing its commitment to collaboration with other states or international entities. The Act's provisions align with international initiatives like the International Covenant on Civil and Political Rights and the Convention on Cybercrime, showcasing Pakistan's dedication to global cooperation in addressing cybercrimes.This literature reviews the domestic reaction to PECA, noting concerns raised by civil society and the IT industry. Criticisms include restrictions on internet freedom, limitations on free speech and privacy, and excessive powers granted to law enforcement agencies. The Act's impact on human rights and its perceived draconian nature are highlighted.

## **Cyber Laws in Pakistan: Protecting Business and Personal Data**

The document[10] "Cyber Laws in Pakistan: Protecting Businesses and Personal Data" gives a thorough look at the cyber laws in Pakistan, emphasizing how they help protect both businesses and individuals from cybercrime.

The document begins by noting how important cyber laws have become in Pakistan, especially with the rapid growth in technology. It points out the need for strong laws to defend against cybercrimes that can harm both personal data and businesses.Key laws (PECA 2016 and Cybercrime Act 2017) are central to Pakistan's fight against cybercrimes. They list different types of cybercrimes, such as unauthorized access, cyberstalking, online hate speech, identity theft, and cyberterrorism, and set the penalties for these crimes. It provides clarity on the types of activities that fall under the purview of cybercrime, covering offenses ranging from unauthorized access to electronic forgery.

The literature talks about how cybercrime can lead to money loss, damage to reputations, and loss of private data for companies. For individuals, the risks include identity theft, financial loss, and harm to their credit scores. The PECA law includes ways to protect personal and business data, security steps for companies, and punishments for cybercrimes. It mentions jail time and big fines, especially for repeat offenders and government officials.

The document discusses how PECA and the Personal Data Protection Bill of 2019 help protect personal and business data in Pakistan. It focuses on the importance of keeping data safe, legal measures, and making it a crime to access data without permission.

The Federal Investigation Agency (FIA) in Pakistan is in charge of looking into cybercrimes. It works with other police forces and international groups to deal with cybercrimes that cross borders.

Pakistan has come a long way in making cyber laws, but there's still more work to do to keep up with the fast-changing digital world. It underlines the need for international teamwork and regular updates to laws to effectively fight cybercrime.

## **Cybercrime in Pakistan: A Study of the Law Dealing With Cyber Crimes in Pakistan**

The article [7] examines the state of cybercrime in Pakistan. It also offers a critical analysis of PECA and the ways that Pakistani cyber law stifles freedom of speech in Pakistan.

Internet access in Pakistan has witnessed substantial growth since the mid-90s. However, as internet usage rises, so does the prevalence of cybercrimes. Despite this, many Pakistanis remain uninformed about cybersecurity issues. To address the escalating cyber threats, the government has established the "National Response Centre for Cybercrime" under the administration of the FIA. Complex cybercrimes, particularly financial frauds, are underreported, with the majority of reported cases involving cyber harassment, bullying, and defamation.

The recognition and seriousness of cybercrime in Pakistan have evolved in recent years due to a lack of initial awareness. Initially, there was no specialized legislation to address cyber threats, emphasizing the necessity for dedicated laws. In 2002, the ETO marked the first legislative step, focusing on electronic documentation and authentication.

The Prevention of Electronic Crimes Act in Pakistan, crafted to combat digital offenses, carries stringent penalties for cybercrimes. However, PECA has faced critique, particularly concerning its potential encroachment on the constitutional right to free speech, safeguarded by Article 19. The act is infamous for its excessive regulation of online content, conferring extensive powers upon authorities to remove or block content considered contrary to Islam's glory, national defense, public order, morality, and more. Criticism has been directed at PECA for providing the Pakistan Telecommunication Authority (PTA) with unchecked power, impacting the fundamental right to free speech.

## **Assessing the Cybercrime Legislation in Pakistan: A Comparative Study of European Union and Pakistani Cybercrime Laws**

The purpose of a comparative analysis of EU and Pakistani law is to identify areas of weakness and potential improvements for Pakistan's legal framework[12].

The impact of EU regulations is far-reaching, particularly for countries seeking business engagements with EU member nations. The following entities significantly contribute to enforcing cybercrime laws in EU member countries, aligning with the legal frameworks established by the EU.

The Electronic Transaction Ordinance of 2002, being the first of its kind at the time, aimed to protect data related to the E-commerce sector and establish legal sanctity. The Cybercrime Ordinance of 2007, enacted to combat cyberterrorism, online data disruption, theft, forgery, cyberstalking, and spoofing, specified penalties ranging from six months' imprisonment to the death penalty. Building upon the cybercrime bill of 2007, the Prevention of Electronic Crimes Act (PECA) of 2016 expanded the scope to include offenses such as hacking, denial-of-service attacks, forgery, online fraud, and cyberterrorism. PECA 2016 outlines penalties for various cybercrimes, including imprisonment and fines. The Federal Investigation Agency (FIA) serves as the primary agency handling cybercrimes through online proceedings. A weak enforcement system and a lack of public trust in the legal system contribute to ongoing cybercrime issues.

The legal framework in the EU strongly prioritizes the right to freedom of expression and speech, featuring well-defined laws and an efficient implementation mechanism. In comparison, Pakistan's cybercrime legal framework revolves around PECA, accompanied by the FIA Act, which stipulates fines and imprisonment. However, questions arise about the adequacy of these measures. The protection of citizens' privacy rights is notably lacking, with government bodies and intelligence agencies accessing private data without consent. Substantial efforts are required to enhance cybercrime laws in response to the evolving use of the internet.

The sluggish dispensation of justice in Pakistan raises concerns about PECA's effectiveness, particularly when assigning responsibilities to courts for expeditious trial decisions. Ambiguity surrounds the capacity of an overburdened judicial system to shield citizens from injustice and unfair trials, suggesting PECA may fall short in safeguarding fundamental human rights. There is a call for a more enduring solution to address citizens' concerns, emphasizing the preservation of freedom of expression. In this context, PECA may be perceived as a stringent law empowering state institutions to evade criticism from the public, human rights defenders, and online journalists.

## **Protecting Online Privacy in Pakistan**

This article [11] highlights that a number of the PECA-2016 provisions have a negative impact on the nation's online privacy. It is decided that in order to safeguard and advance citizens' right to online privacy, some of the PECA-2016's provisions ought to be strengthened or removed.

The protection and promotion of individuals' right to privacy, both online and offline, are enshrined in the Constitution of Pakistan. However, recent legislation and associated rules have faced significant criticism for allegedly violating the fundamental right to privacy in the country (State of Privacy Pakistan, January 26, 2019). Consequently, there is a critical need to examine these laws, which have a substantial impact on online privacy rights in Pakistan.

The legal framework in Pakistan has witnessed the implementation of several laws impacting the right to privacy, both in offline and online contexts. Notably, due to the absence of specific legislation on data protection, privacy regulation has been governed by laws as stated above. More recently, the "Pakistan Electronic Crimes Act 2016" (PECA 2016) has been introduced, featuring provisions with significant implications for online privacy in the nation. Crucial sections of PECA 2016, specifically 31, 32, 37, and 42, confer extensive powers on government agencies concerning individual data, posing a substantial threat to digital privacy. This provision lacks judicial oversight, potentially enabling unilateral assistance between countries and agencies. The absence of checks on how acquired data is utilized raises significant concerns about potential misuse by both domestic and foreign entities.

In conclusion, the introduced provisions in PECA 2016, particularly those related to data access and sharing, present serious challenges to online privacy in Pakistan. The potential for misuse and the lack of robust safeguards raises questions about striking a balance between security and individual privacy in the digital age.

# **Analysis**

The cyber laws in Pakistan, notably the Prevention of Electronic Crimes Act (PECA) introduced in 2016 and updated in February 2022, require a thorough implementation. Inadequacies such as legal gaps and delays in implementation raise concerns, necessitating a proactive legislative approach to keep pace with evolving cyber threats.

This research embarks on a thorough examination of Pakistan's cyber laws, with a primary focus on evaluating the efficacy and implications of the Prevention of Electronic Crimes Act (PECA) introduced in 2016. The study involves a meticulous comparative analysis with international cyber laws to delineate the strengths, weaknesses, and areas necessitating improvement within Pakistan's legal framework. A critical aspect of this analysis involves scrutinizing the human rights implications, striking a delicate balance between robust cybersecurity measures and the protection of individual liberties. The research extends its inquiry into the practical effectiveness of these laws in prosecuting cyber crimes, delving into the role of the Federal Investigation Agency (FIA) in cybercrime investigations. Furthermore, it explores the extent of public awareness and corporate compliance with these cyber laws. The study aims to provide nuanced insights into adapting legal frameworks to rapidly evolving technologies, fostering global collaboration, and fortifying privacy safeguards. Ultimately, the research seeks to offer comprehensive recommendations for fortifying and refining Pakistan's legal landscape concerning cybersecurity.

Striking a balance between cybersecurity and individual rights is paramount, emphasizing the need for continuous adaptation and improvement in Pakistan's cyber laws to combat cyber threats effectively and protect national security. The research will contribute insights into adapting the legal framework to emerging technologies, ensuring global collaboration, and enhancing privacy protection, ultimately providing recommendations for strengthening Pakistan's cybersecurity legal landscape.

# 

# **Conclusion**

In summary, Pakistan has made significant legislative efforts to counter cybercrime, as exemplified by the enactment and enforcement of various laws. However, a more detailed analysis exposes certain complexities. The absence of specific legislation on data protection gives rise to concerns regarding the safeguarding of individual privacy, both in physical and virtual realms. Although initiatives like the Pakistan Electronic Crimes Act 2016 (PECA 2016) aim to comprehensively address cyber threats, certain sections that confer extensive powers to government agencies in terms of personal data handling pose potential risks.

Provisions within PECA, especially those pertaining to data management, raise questions about the potential for misuse and the effectiveness of protective measures. The mandated prolonged retention of data, coupled with the lack of explicit data protection laws, creates an environment where privacy vulnerabilities could emerge. Provisions allowing unilateral international cooperation without robust judicial oversight also elicit apprehensions.

In essence, while Pakistan's legislative efforts to combat cybercrime are commendable, ongoing assessment and adjustments are necessary to strike a balance between national security needs and the protection of individual rights, particularly in the context of online privacy. Continuous adaptation to the evolving digital landscape is imperative to ensure that the legal framework remains effective and upholds the fundamental rights of citizens.

## **Recommendations**

The following steps can be taken to improve cybersecurity in Pakistan:

1. **Introduction of Pen/Trap Surveillance:**

In the USA, the introduction of Pen/Trap surveillance in 2001 proved effective for computer forensics, providing the government with the authority to monitor electronic communication sources. This method, focused on communication metadata rather than content, maintains privacy and simplifies judicial authorization.

1. **Amendment of PECA:**

To ensure the protection of rights, it is proposed to amend PECA. This amendment aims to align PECA with the provisions of the International Covenant on Civil and Political Rights (ICCPR), to which Pakistan is a signatory. Specific areas for amendment include refining the definition of 'Persons' and adjusting the duration of punishments outlined in the act. Additionally, reconsideration of the provision mandating courts to conclude cases within six months is suggested, given the prevailing sluggish pace of court proceedings in Pakistan, to ensure fair trials for victims of cybercrime.

1. **Staying Abreast of IT Advancements:**

In light of ongoing developments in IT and the government's efforts to enhance cyberspace security, it is crucial for the Pakistani government to implement stringent measures to stay informed about IT progress. This proactive approach will facilitate the formulation of updated laws that align with evolving requirements.

1. **Digital Content Regulation:**

The integration of content regulation into cyber offenses within PECA should be considered distinct concepts. A dedicated framework for 'digital content moderation' or 'digital content regulation' should be established to safeguard the fundamental right of freedom of expression.

1. **Active FIA:**

The FIA should establish 24/7 call centers or physical support centers to offer comprehensive guidance and effective feedback to the public regarding their complaints. Enhancements should be made to the user-friendliness of the FIA reporting portal, and additional facilitation measures, such as online chat or calls, should be implemented.

# 

# **References**

1. “Pakistan: Repeal amendment to draconian cyber law,” Amnesty International, 2022. [Online]. Available:https://www.amnesty.org/en/latest/news/2022/02/pakistan-repeal-draconian-cyber-crime-law/. [Accessed: 05-Nov-2023].
2. K. Adil, “Legal framework for policing cyberspace in Pakistan: An overview,” *Research Society of International Law | RSIL*, 07-Mar-2023. [Online]. Available: https://rsilpak.org/2023/legal-framework-for-policing-cyberspace-in-pakistan-an-overview/. [Accessed: 26-Nov-2023].
3. “Analysis of Pakistan’s cybercrime bill,” *Rsf.org*. [Online]. Available: https://rsf.org/sites/default/files/analysis\_of\_pakistan\_s\_cyber-crime\_bill.pdf. [Accessed: 26-Nov-2023].
4. *“*Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in\_ akistan*”Researchgate.net*. [Online]. Available: https://www.researchgate.net/profile/Asif-Kamran/publication/338885893\_Existing\_Cyber\_Laws\_and\_Their\_Role\_in\_Legal\_Aspects\_of\_Cybercrime\_in\_Pakistan/links/5e315595299bf1cdb9f985ea/Existing-Cyber-Laws-and-Their-Role-in-Legal-Aspects-of-Cybercrime-in-Pakistan.pdf?origin=journalDetail&\_tp=eyJwYWdlIjoiam91cm5hbERldGFpbCJ9. [Accessed: 26-Nov-2023].
5. K. kiener-manu, “Cybercrime module 3 key issues: The role of cybercrime law,” *Unodc.org*. [Online]. Available: https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html. [Accessed: 26-Nov-2023].
6. S. Akhtar, “Assessing the cybercrime legislation in Pakistan: A comparative study of European union and Pakistani cybercrime laws,” *SSRN Electron. J.*, 2023.
7. M. Akhlaq, “Cybercrime in Pakistan: A study of the law dealing with cybercrimes in Pakistan,” *Leappakistan.com*. [Online]. Available: https://leappakistan.com/wp-content/uploads/2021/05/CYBERCRIME-IN-PAKISTAN-A-STUDY-OF-THE-LAW-DEALING-CYBERCRIME-IN-PAKISTAN.pdf. [Accessed: 26-Nov-2023].
8. *Academicjournals.org*. [Online]. Available: https://academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210. [Accessed: 26-Nov-2023].
9. I. A. Sandhu, “Cyber laws in Pakistan : Protecting Businesses and Personal Data,” *Attorney & Legal Affairs*, 24-Jan-2023. [Online]. Available: https://validlaws.com/cyber-laws-in-pakistan-protecting-businesses-and-personal-data/. [Accessed: 26-Nov-2023].
10. *“*NEED OF INTERNATIONAL LEGISLATION REGARDING CYBER CRIMES PAKISTAN PERSPECTIVE*”Researchgate.net*. [Online]. Available: https://www.researchgate.net/publication/365277420\_NEED\_OF\_INTERNATIONAL\_LEGISLATION\_REGARDING\_CYBER\_CRIMES\_PAKISTAN\_PERSPECTIVE. [Accessed: 26-Nov-2023].
11. Y. Aleem, M. Tariq, M. Umar, M. Z. Rafique, and M. U. Ashraf, “Protecting online privacy in Pakistan,” *PalArch’s J. Archaeol. Egypt/Egyptol.*, vol. 18, no. 6, pp. 607–615, 2021.
12. S. Akhtar, “Assessing the cybercrime legislation in Pakistan: A comparative study of European union and Pakistani cybercrime laws,” *SSRN Electron. J.*, 2023.