https://doi.org/10.62585/slpr.v1i1.21

Volume & Issues Obtainable at www.centeriir.org
SOCIETY, LAW AND POLICY REVIEW
ISSN (P): 3005-821X ISSN (E):3005-8228
Volume 1, No.1 , 2022
https://journals.centeriir.org/index.php/slpr

Society, Law & Policy Review
A Multidisciplinary Research Journal

Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges

Hobashia Saleem[1] **Junaid Jan**[2] **Azzalfa Areej**[3]

[1] LL.M. Scholar, Department of Law, The Islamia University of Bahawalpur. Email: Hobashiasaleem@gmail.com
[2] Lecturer, Department of Law, The Islamia University of Bahawalpur. E-Mail: Junaid.jan@iub.edu.pk
[3] LL.B. Student, Department of Law, The Islamia University of Bahawalpur. E-Mail: azzalfaarrej@gmail.com

ABSTRACT

This study looks at the growing problem of cybercrime in Pakistan, concentrating on the legislative framework and the issues that law enforcement authorities face. It examines the rise of cybercrime in the country, the evolution of cyber legislation, and the passage of the Prevention of Electronic Crimes Act (PECA) in 2016. The report emphasizes the importance of a strong legal framework in combating cybercrime efficiently. Despite PECA, internet crimes remain a big threat. The study highlighted enforcement challenges such as technology constraints, data breaches, terrorist risks, and a lack of public awareness. It underlines the significance of specialized courts, public awareness campaigns, and improved technical capabilities for law enforcement. The conclusion underlines the importance of Pakistan strengthening its law enforcement and amending existing legislation to effectively combat cybercrime. Implementing the study's recommendations can help to preserve citizens' rights and privacy while also reducing cybercriminal risks. Pakistan must take decisive steps to combat cybercrime, and the study's recommendations provide a good framework for this effort.

Article History: Received: 01-10-2022 **Accepted**: 29-10-2022 **Published**: 02-11-2022
Keywords: Cyber Crimes, Pakistan, PECA, Digital Piracy, Cyber laws

Corresponding Author's Email: Junaid.jan@iub.edu.pk
How To Cite: Saleem, H., Jan, J., & Areej, A. (2022). Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges. *Society, Law and Policy Review*, *1*(1), 10–22.

https://doi.org/10.62585/slpr.v1i1.21

1. Introduction

Computers have revolutionized human life and made it significantly more manageable. Nowadays, every person and business relies heavily on computers as they have become an integral part of our lives. Our day begins with the alarm on our cell phone, a computer networking type. We rely on computers to efficiently accomplish our daily tasks with ease and accuracy (McQuade III, 2008). Computers have become an integral part of our lives, from mobile phones and laptops to desktops and digital watches. They can store vast amounts of data and process it to achieve our goals with utmost accuracy and efficiency. In the vast world of computer networks and the internet, cyberspace is the powerful realm where data and information are processed with utmost precision and efficiency (Usman, 2017). Criminals penetrate cyberspace and tamper with a person's or organization's data. Computers are undoubtedly used as weapons to commit crimes (Kundi et al., 2014). Cybercrime refers to any offence committed using a computer as a tool or target.

Cybercrime is a broad term that is used loosely. For example, cybercrime is the term used to describe a crime committed using a digital device over the internet (Sharma & Alam, 2016). In summary, *"cybercrime"* involves a computer, the internet, advanced technology, and cyberspace. In 1995, the term "cybercrime" was coined to refer to crimes committed using computers. It was also discovered that cybercrime is executed through a computer, either targeting a computer itself or through a combination of tactics involving the use of technology (Kundi et al., 2014). Another feature of this crime is that it never requires the perpetrator to be physically present at the crime scene. Unlike traditional crimes, digital crimes necessitate the use of cyberspace to cause harm to a person or their property (Munir & Shabir, 2018). For example, hackers from anywhere in the world can access a bank account in Pakistan, and software piracy can be committed remotely.

Dealing with sophisticated cybercrimes requires firm and decisive management. To achieve this, there must be a robust legal framework in place (Kundi et al., 2014). Pakistan has been identified as a country with a higher rate of cybercrime than other nations. It includes various cyber threats and attacks such as hacking, identity theft, financial fraud, phishing scams, and ransomware attacks. This trend could be attributed to a lack of awareness about cybersecurity, poor implementation of cyber laws, limited resources for law enforcement, and the increasing use of technology in the country (Mohiuddin, 2006).

Cyber laws handle concerns in cyberspace and deal with cyber offenders. The primary objectives of this study are to examine the prevalence of cybercrimes in Pakistan and the applicable cyber laws. Despite the existence of the Prevention of Electronic Crimes Act, 2016 (PECA), which doesn't encompass various modern-day electronic acts, numerous electronic crimes are widespread in Pakistan and remain unregulated.

2. Common Types of Cybercrimes

Cybercrime is a vast field that covers a multitude of offenses, ranging from privacy violations to the dissemination of harmful and illegal content, as well as activities such as facilitating prostitution and other moral offences, organized crime, and various economic crimes, including industrial espionage, computer fraud, forgery, theft, extortion, product piracy, and other intellectual property crimes (Goodman & Brenner, 2002). As previously stated, there is no precise definition of cybercrime. However, the following activities have been classified as cybercrime:

2.1.Hacking

Hacking is the illegal act of entering or manipulating computer network security systems with malicious intent. It involves using one computer system to breach the security of another, usually to gain access to sensitive information. Cybercrime is a growing concern in Pakistan, with hacking being one of the most prevalent types of attacks. Reports indicate that hacking incidents targeting banks, organizations, and even personal Facebook accounts are rising. Hacking poses a significant threat to digital systems and information security.

2.2.Fraud

The most common type of cybercrime is fraud. The internet has made it possible to commit borderless fraud. The spectrum of what constitutes fraud is relatively broad. Online vendors may scam customers by providing fake products, misleading advertisements, or failing to deliver purchased items. The category includes anything from minor incidents to large-scale bank frauds.

2.3.White Collar Crime

Bank fraud constitutes a major form of white-collar crime that involves a range of illegal activities such as impersonating bank employees, deceiving account holders into revealing their personal and financial information, creating fake financial institutions, and swindling individuals into depositing money or securing illegal loans.

2.4.Cyber Bullying

Cyberbullying and cyber-harassment are forms of bullying and harassment that occur online on gaming platforms, messaging apps, social media, etc. These incidents occur frequently in Pakistan. Women, in particular, are subjected to harassment on internet platforms. Based on the data collected in 2018-2019, it can be confidently stated that blackmailing and harassment are the most commonly reported cybercrimes in Pakistan (Allia Bukhari, 2020).

2.5.Cyber Stalking

Cyberstalking is a type of stalking that occurs via the internet or digital devices with the intent of intimidating or harassing someone by repeatedly contacting them. These acts are directed toward a specific individual, and the victims typically experience anxiety and apprehension. Harassment and stalking, both online and offline, are major concerns for women in Pakistan, who are especially vulnerable to such incidents.

2.6.Digital Piracy

Copyright infringement is a serious crime involving the unauthorized reproduction, copying, or distribution of digital work without the copyright holder's permission. It is a clear violation of copyright laws and can have severe legal and financial consequences (Ingram, 2014). The act seriously infringes on the intellectual property rights of the holders and poses a significant threat to the spread of viruses, causing severe damage to businesses.

2.7.Denial of service attacks

A denial of service attack is a cyberattack that renders a targeted computer or device inoperable by disrupting its normal operation. Pakistan-based websites are frequently targeted by Distributed Denial of Service (DDoS) attacks that render them inoperable for users. Such attacks are carried out by using software or bots to drive an enormous amount of traffic towards the targeted sites. According to reports, these attacks become more common on or around 14 August and are primarily carried out by India (Talha Khan, 2015).

2.8. Spoofing

The act of presenting a message from an unidentified source as authentic is called spoofing. Faking is a versatile technique that can be applied in various scenarios, such as emails, phone conversations, websites, or even more complex technical situations, like a computer faking an IP address or DNS (Domain Name Servers)(Forcepoint, n.d.). According to the PECA, it is defined as:″Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website to be an authentic source commits spoofing. And is punishable by up to three years in prison, a fine, or both."

2.9.Cyberterrorism

Cyberterrorism is defined as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data by subnational groups or clandestine agents that result in violence against non-combatant targets." (Pollitt, 1997)

Cyberterrorism can take many different forms. An attacker can easily breach a domestic banking computer system and cause massive disruptions or even take control of the air traffic control system, manipulating it to cause catastrophic plane crashes and collisions. It is not difficult for an attacker to penetrate a domestic financial system and cause significant disruptions. In fact, they can easily take control of the air traffic control system and manipulate it to cause catastrophic jet crashes and collisions (Goodman & Brenner, 2002). All of these are examples of cyberterrorism. Under the Prevention of Electronic Crimes Act (PECA), cyberterrorism is punishable by up to 14 years in prison, a fine of up to 50 million Pakistani rupees, or both.

2.10. Phishing

Phishing is one of the most common criminal techniques that involve impersonating a legitimate or authentic entity through email, phone, or text messages to trick individuals into revealing sensitive and personal data such as bank card details or passwords (Phishing.org, n.d.). Because of its ability to capture individuals quickly, phishing is one of the most successful types of cybercrime.

2.11. Viruses and harmful software

Viruses are malicious code attachments to other executable programs that, if loaded, reproduce the malicious code and self-propagate it to other systems. It corrupts the files and data on the hard disk and other storage disks. Distributing viruses or any kind of harmful code is a clear violation of Section 20 of the PECA and is strictly punishable by up to two years in prison, a fine of up to one million rupees, or both. Be assured that such actions will not go unnoticed and will be dealt with accordingly.

2.12. Cyber pornography

Cyber pornography refers to the creation, display, distribution, importation, or publication of pornographic or obscene materials using the internet or other electronic means. Pedophilic images depicting youngsters engaging in sexual actions with adults are commonly shared. According to Section 19 of the Pakistan Penal Code, which deals with offences against the dignity of natural persons and minors, such acts are considered criminal. In recent years, there has been an increase in these types of incidents in Pakistan. The Federal Investigation Agency (FIA) Cybercrime unit recently detained a man in December 2020 for illegally downloading and sharing child pornographic material. Six people involved in child pornography were arrested in the past year by the FIA's cybercrime department (Shakeel & Qarar, 2020).

3. Legal Framework of Cyberspace Technology in Pakistan

As technology continues to advance, the need for laws and regulations governing cyber activities becomes increasingly important. Cyber legislation is a critical component of legal frameworks that aims to prevent cybercrimes and regulate online activities carried out using computer resources. In Pakistan, the Government has taken significant steps to address these concerns by enacting essential cyber legislation to guarantee the safety and security of its citizens as they engage in online activities. The brief description of such legislation is as follows:

3.1.Telegraph Act, 1885

The act in question must be revised to account for the latest technological advancements. Nonetheless, it continues to serve as a powerful tool for federal and local authorities to protect the privacy of individuals, and we are confident in its ability to do so. Government exercises unrestricted powers in the name of the public interest without the interference of courts. In the event of a national emergency or for the sake of public safety, the Government may seize control of the telegraph. Moreover, *"Entering telegraph offices without lawful permission and interfering with telegraph messages is a serious offence that is punishable by law"* (The Telegraph Act, 1885).

3.2.The Pakistan Telecommunications (Re-organization) Act, 1996

Any unauthorized communications must be promptly reported to the Court through the Telecommunication Authority or Frequency Allocation Board as per the provisions of this act. The Court is vested with the authority to issue search warrants, enabling the search of locations where crimes are believed to have occurred. Law enforcement authorities have the power to seize equipment used for criminal activities and conduct thorough investigations (The Pakistan Telecommunications Act, 1996).

3.3.National Information Technology Policy and Action Plan, 2000

In the year 2000, the Pakistani Government implemented its information technology policy. The goal of this policy was to create legislation dealing with cybercrime. After reviewing the legal frameworks of various common law and civil law nations, this policy was developed based on the UNCITRAL Model Laws. Based on the sound approaches adopted by various nations, we have concluded that the "International Consensus Principles on Electronic Authentication" developed by the Internet Law and Policy Forum is the most appropriate guideline for devising our policy (Mushtaque et al., 2014). Developing IT policies and action plans ensures individual data's safety and protects E-commerce's integrity (National Information Technology Policy, 2000). This legislation is a significant step toward securing cyberspace protection.

3.4.Electronic Transactions Ordinance, 2002

In September 2002, an ordinance came into effect with a clear objective: establishing legal support for a wide range of Internet transactions. This act played a pivotal role in creating a solid legal foundation for electronic signatures and records. Furthermore, the Federal Government must establish clear data protection and user privacy guidelines (Electronic Transaction Regulation, 2002). However, there are several murky areas under this regulation. International cyber laws from various nations list several offences which the current act disregards. Moreover, the ordinance has become outdated as it has not been modified to keep up with the rapid advancement of cybercrimes and new technologies.

3.5.The Electronic Crimes Act, 2004

In compliance with the terms of the Electronic Transactions Ordinance of 2002, this act was enacted with the support of the Ministry of Information Technology. The different offences relating to cyberspace were introduced as cybercrimes in this act. According to the Electronic Crimes Act of 2004, cybercrime encompasses a broad range of unauthorized activities, such as interception, cyberstalking, spamming, spoofing, and unauthorized access. It also includes more severe offences such as electronic fraud, forgery, system damage, and cyberterrorism. Additionally, the misuse of devices and encryption, as well as the introduction of malicious code, can also be considered cybercrime. As a result, no enforcement unit was established under this act. Furthermore, the acts made publishable by this act needed to be better defined. The definitions of criminal conduct were too broad for comprehension. This legislation could have been more effective due to the lack of enforcing measures and the complexities of the wording used to define cybercrime.

3.6.The Prevention of Electronic Crimes Act (PECA), 2016

The National Assembly adopted the bill for this Act in April 2015, and was finally voted on by the Senate in August 2017. This act was established as part of the Pakistani Government's National Action Plan to combat terrorism following the devastating terrorist attack on a school in Peshawar. The act provides comprehensive coverage for cybercrime, encompassing a wide range of offences such as cyberstalking, cyber spoofing, phishing, cyber harassment, illegal access to devices or information systems, illegal access to data or information, illegal interference with data or information systems, cyberterrorism, blasphemy, and cyber forgery. Rest assured that any illicit activities in the cyber realm will not go unpunished under the Act (Prevention of Electronic Crimes Act, 2016). Although the act's text could be more straightforward, it is a significant step towards ensuring the safety and security of the citizens of Pakistan.

Many human rights organizations and legal experts assert that the language of the act needs to be more precise, as the current ambiguity poses a threat to privacy and freedom of expression. According to the Act, individuals who use another person's identity to commit fraud are guilty of invading their privacy. Similarly, sharing one's identification information for fraudulent or deceptive purposes clearly violates an individual's right to privacy. It is strictly prohibited to unlawfully intercept any information or hack data to access it, commit any crime, or gain any wrongful benefit or loss when it is not made public. Law enforcement agencies may intercept any information to ensure national security. The ability to intercept any information is crucial to ensuring national security. As a result, the Court has the power to issue a search and seizure warrant to an investigative officer when it is convinced that data or information is necessary for the inquiry. As a result of the communication, the Court may require anyone in possession of the information to provide it to the appropriate party within seven days.

Moreover, the right to privacy and data protection deserves to be respected at all times, without any exceptions. The fact that service providers are authorized to retain data for a minimum of one year poses a serious threat to the privacy of individuals. Notably, the Pakistan Telecommunications Authority (PTA) has the power to block or remove any information deemed harmful to the country's interest, security, integrity, good relations with other countries, morality, ethics, decency, or the general public interest. Furthermore, if required for evidence, the investigating officer may request real-time collection and recording of such data. However, it is important to ensure that the privacy of individuals is not compromised in any way while carrying out such procedures.

Moreover, the investigating officer must submit an oath application to facilitate the legal process. Additionally, the Federal Government has the power to exchange information related to the investigation with foreign intelligence agencies without requiring a judicial order. The Government has the authority to confiscate and share data as required. It is worth noting that the regulations governing this process are well-established and legally enforceable, even though there may not be a specific document outlining human rights in this context (Mariam Sherwani, 2018). Since the passage of this act, several agencies have been granted the authority to monitor and regulate individuals and organizations involved in cybercrime effectively. The FIA has been entrusted with the crucial responsibility of overseeing cyberspace activities. To ensure the effectiveness of this act, funding has been allocated to create state-of-the-art forensic laboratories and cybercrime police stations. The act has a two-fold purpose: it protects individuals and safeguards the state by preventing cybercrime. This act empowers individuals to seek justice for identity theft and data theft.

This act provides some protection for women, safeguarding their reputation from any sexual threats and preventing the unauthorized use of their images. However, it falls short in terms of protecting individuals' privacy and is not currently supported by any data protection laws (Kundi & Shah, 2009). Consequently, establishing a commission to defend people's privacy and data is crucial. With the necessary revisions, this act can become an effective tool in protecting the rights and dignity of women and individuals alike.

4. Enforcement Challenges

Pakistan is still dealing with a slew of problems, including corruption, poverty, a lack of technological growth, and an insecure democratic system. These variables pose several problems to the organization's internal security, with cybersecurity emerging as a critical component. Pakistan's law enforcement agencies face numerous and complicated obstacles in countering cybercrime.

There needs to be more appropriate technological prowess for oversight, particularly about the surveillance by foreign spy organizations such as the National Security Agency of the United States (Qadeer, 2020). Furthermore, the nation is not impervious to viruses such as Peals, Skeeya, and Gamarue, which can infiltrate computer systems, install malicious software, and pilfer sensitive personal information. Additionally, distributed denial-of-service (DDOS) attacks, which occur surreptitiously and without user consent, pose yet another significant risk. The financial sector in Pakistan is unfortunately vulnerable to cyber-attacks, as evidenced by recent incidents such as the data theft from all Pakistani banks, which was announced by the Federal Investigation Agency's Cyber Crime Wing (Shakeel Qarar, 2020). As a result, there needs to be more confidence between customers and banks.

Furthermore, the presence of terrorist organizations complicates the cybersecurity picture, as there is a continual danger of critical government websites being hacked or stolen, such as strategic assets. Cyber propaganda is used by terrorist organizations like IS and TTP to promote their agenda and recruit members (Zia UL Islam et al., 2019). Terrorist attacks, such as the one that took place at Bacha Khan University in 2016, are a clear demonstration of the use of information and communication technology (ICT) by attackers who operate from abroad. However, despite this risk, there is still a general lack of awareness among the public about how to protect their sensitive information from unauthorized access, which can result in individuals becoming victims of identity theft and other forms of abuse.

It is evident that cybersecurity poses some significant challenges, including the widespread misrepresentation of the topic in the media. The media tends to oversimplify the issue and present it from a general perspective, which often leaves individuals with a superficial understanding of the matter. There needs to be an institutional framework to address this challenge and a broad spectrum of security arguments involving foreign dangers that frequently overlook cybersecurity issues confronting the country. Cybersecurity is a crucial aspect of national security, with equal importance to other areas like border security, nuclear assault, and terrorism. However, it has been overshadowed by the nation's conventional security culture, which has led to a lack of adequate attention to cybersecurity. One of the biggest challenges in developing a robust cybersecurity strategy is obtaining feedback from stakeholders. Without their input, policies can become overly technical or bureaucratic, rendering them less effective.

Despite being passed in 2016, Pakistan's cyber law has faced criticism due to some of its measures being labelled as 'draconian' (Raza Khan, 2016). However, it is important to note that such criticisms are common in developing countries like Pakistan, which are still working to strengthen their democratic structures. Critics argue that the law has bestowed great powers on the authorities, which they have occasionally abused (Vasudevan Sridharan, 2016). Data breaches are a persistent concern, but our system is equipped with the latest security measures to ensure adequate protection (Barrister Jannat Ali Kalyar, 2019). The legislation is also unable to distinguish between cybercrime, cyberwarfare, and cyberterrorism, resulting in overly harsh penalties that are insufficient for the nature of the offence (Jamshed et al., 2021).

Moreover, many experts assert that PECA is being used as a tool by the state to suppress free speech and expression while masquerading it under the pretext of "national security" and "anti-state" propaganda (Aziz, 2018). This criticism and weakness also refer to a difficulty in cybersecurity measure creation and implementation. Pakistan must rely on internal investment since private partners need more backing to help construct cybersecurity infrastructure. There are two prominent organizations tasked with cybersecurity maintenance: the National Response Centre for Cyber Crimes (NRC), which is part of the Federal Investigation Agency (the primary law enforcement agency), and the Pakistan Information Security Association (PISA), a non-governmental organization that collaborates with the private sector to mitigate commerce-related threats (Baker, 2014).

Overall, the state's cybersecurity posture remains weak. There appears to be a need for a proactive, comprehensive, and grass-roots security program since the existing cybersecurity measures appear reactive, focusing on 'putting out the fire.' The cybersecurity safeguards in place are shallow, with understaffed programs and most precautions being cosmetic. The approach to solving cybersecurity concerns is 'security box centric,' which condemns any 'out of the box solution,' emphasizing the former. Increased agreement among stakeholders, including risk, compliance, security, and IT audit, is necessary to address cybersecurity. This disagreement is damaging because it wastes time and money.

Lastly, data theft is a significant issue for our country. The National Database & Registration Authority (NADRA) is the only independent organization in the nation entrusted with the responsibility of maintaining government databases and citizen statistics, with utmost confidence and accuracy. The risk of data theft increases when data is linked and sent to defence organizations and numerous other government projects, such as the Punjab Safe Cities Authority, the Benazir Income Support Program, and others. Two years ago, the Punjab Information Technology Board suffered one of the worst data breaches in Pakistani history, which resulted in the leak of personal information belonging to millions of citizens (Barrister Jannat Ali Kalyar, 2019).

5. <u>Recommendations</u>

Attorneys and human rights activists agree that while legislation to combat cybercrime has been passed, timely implementation is necessary. As thoroughly discussed in previous sections of this study, the issue of increased cybercrime and PECA flaws cannot be ignored. This research presents practical recommendations and implementation guidelines to make PECA more realistic and implementable for the people of Pakistan. It is pertinent that the relevant authorities will recognize the difficulties raised and take necessary actions to address them.

5.1.Amendments in PECA, 2016:

Conducting a comprehensive evaluation of PECA 2016 that considers the conflicting legal provisions and the practical implementation challenges is imperative. To ensure a comprehensive review process, it is imperative that all relevant social stakeholders, including civil society members, legal experts, and especially technological professionals, are actively engaged and involved. Given that the PECA 2016 primarily deals with technology-related crimes, the participation of technical specialists is crucial to ensure a thorough and effective evaluation. The Government must take immediate action to review and rectify any provisions violating individuals' fundamental rights. Introducing favorable legislation that protects and promotes the values of free expression, privacy, and data is imperative. The Government must take immediate action to amend PECA 2016 to ensure that the act is more public-friendly and focused on generating maximum public benefits. The current version of PECA is biased towards certain sections and requires a more holistic approach to ensure fair and just outcomes for all. In PECA, content control and cyber offences must be dealt with as distinct concepts. To protect the fundamental right to freedom of expression, we must establish a separate framework for 'digital content moderation' or 'digital content regulation'. This approach will enable us to confidently safeguard the rights of individuals and maintain a fair and just digital environment. It is imperative that Section 37, which grants the PTA the authority to restrict online content, is revised immediately to define the boundaries and prerequisites for content removal clearly. This clause must be omitted from PECA and integrated into the new framework recommended in point three with utmost urgency.

5.2.Training of Law Enforcement Officials

The Government must prioritize the empowerment of law enforcement officials who deal with cybercrimes. Providing technical training to FIA officers that aligns with international standards is imperative. With the evolving nature of cybercrime, urgent measures must be taken to enhance the technical capabilities of the FIA. Furthermore, it is essential to establish judicial capacity in handling cybercrime cases. To achieve this, a technical judicial advisory council must be formed to ensure that honorable judges have a sound understanding of the complexities of cybercrime.

5.3.Establishment of Specialized Courts

Given the overwhelming number of criminal cases currently being heard in our courts, establishing dedicated Specialized Courts to address these specific cases is imperative. It would ensure that justice is served promptly and efficiently while alleviating the burden on our already overworked judicial system.

5.4.Mass Awareness

Launching a public awareness campaign to educate the general public about current cybercrime laws and how to report them is crucial. The FIA and PTA should begin broadcasting public service announcements on media platforms to educate more people about cybercrime. The FIA and PTA should make their domains and the types of cases they will be handling public.

5.5.Establishment of Hustle-free Helpline

The FIA must establish physical care facilities or 24-hour call centres to provide prompt assistance and input to the public on their issues. Additionally, incorporating more convenient features such as online chat and phone support into the FIA reporting website would significantly enhance its user-friendliness and efficacy. To properly handle cybercrime, the FIA requires additional competent human resources and nationwide cyber forensic labs should be developed.

6. Conclusion

It must be realized that amending PECA is an evolutionary process rather than a revolutionary one. Based on the debate in this article, it is clear that cybercrime is widespread in our society and has been mostly overlooked for a long time. PECA 2016 serves as the foundation for the country's proper cybercrime legislation. PECA's long-standing problems are its inconsistencies with existing constitution sections and a need for practical implementation instructions. Some laws have been noted to be exploited to help criminals rather than catch them. To ensure social harmony and maintain public order, it is imperative to enact laws. The protection of fundamental rights and the welfare of society at large should always take precedence. The state is committed to supporting and empowering its citizens, and implementing the above-mentioned recommendations will make PECA more effective and accessible to the general public. Moreover, amending PECA 2016 will foster greater public confidence and help curb the alarming rise in cybercrime.

Funding
This article was not supported by any funding from public, commercial, or not-for-profit sectors.

Conflict of Interest/ Disclosures
The authors have disclosed that there are no potential conflicts of interest concerning the research, authorship, and/or publication of this article.

References

Allia Bukhari. (2020, October 21). Silent Battles: How Pakistani Women Counter Harassment in Cyberspace. *The Diplomat*. https://thediplomat.com/2020/10/silent-battles-how-pakistani-women-counter-harassment-in-cyberspace/

Aziz, F. (2018). Pakistan's cybercrime law: Boon or bane. *Heirich Boll Stiftung, The Green Political Foundation and Perspective of Digital Asia*.

Baker, E. W. (2014). A model for the impact of cybersecurity infrastructure on economic development in emerging economies: Evaluating the contrasting cases of India and Pakistan. *Information Technology for Development*, *20*(2), 122–139.

Barrister Jannat Ali Kalyar. (2019, December 22). Cyber Insecurity. *The News*. https://www.thenews.com.pk/tns/detail/586618-cyber-insecurity

Forcepoint. (n.d.). *What is Spoofing?* https://www.forcepoint.com/cyber-edu/spoofing

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139–223.

Ingram, J. R. (2014). Digital piracy. *The Encyclopedia of Criminology and Criminal Justice*, 1–5.

Jamshed, J. (2021). Gender discrimination and sexual harassment in the legal profession: A perspective from patriarchal society. *Women & Criminal Justice*, 1-13.

Jamshed, J., Javed, M. W., Bukhari, S. W. R., & Safdar, A. (2020). Role of Police Investigation in the criminal justice system of Pakistan. *International Journal of Management Research and Emerging Sciences*, *10*(2).

Kundi, G. M., Nawaz, A., Akhtar, R., & MPhil Student, I. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications*, *4*(4), 61–71.

Kundi, G. M., & Shah, B. (2009). IT in Pakistan: Threats & opportunities for eBusiness. *The Electronic Journal of Information Systems in Developing Countries*, *36*(1), 1–31.

Mariam Sherwani. (2018). The Right to Privacy under International Law and Islamic Law: A Comparative Legal Analysis. *Kardan Journal of Social Sciences and Humanities*, *1*(1), 30–48.

McQuade III, S. C. (2008). *Encyclopedia of cybercrime*. Bloomsbury Publishing USA.

Mohiuddin, Z. (2006). Cyber Laws in Pakistan: A Situational analysis and Way Forward. *Ceericsson Pakistan*.

Munir, A., & Shabir, G. (2018). Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation. *Global Political Review (GPR)*, *3*, 84–97.

Mushtaque, K., Ahsan, K., Nadeem, A., & Umer, A. (2014). Critical Analysis for Data Privacy Protection in Context of Cyber Laws in Pakistan. *Journal of Basic and Applied Scientific Research*, *4*(10), 1–4.

Phishing.org. (n.d.). *What is Phishing?* https://www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,credit%20card%20details%2C%20and%20passwords.

Pollitt, M. (1997). *CyberTerrorism-Fact or Fancy? Retrieved January 23, 2010*.

Qadeer, M. A. (2020). The Cyber Threat Facing Pakistan. *The Diplomat*.

Raza Khan. (2016, August 11). Cyber crime bill passed by NA: 13 reasons Pakistanis should be worried. *Dawn*. https://www.dawn.com/news/1276662

Shakeel Qarar. (2020, December 29). *FIA arrests man accused of obtaining, distributing child pornography on social media*. https://www.dawn.com/news/1598523/fia-arrests-man-accused-of-obtaining-distributing-child-pornography-on-social-media

Sharma, I., & Alam, M. A. (2016). Privacy and freedom issues in cyberspace with reference to cyber law. *International Journal of Computer Applications*, *145*(3), 11–18.

Talha Khan. (2015, February 1). Cybercrimes: Pakistan lacks facilities to trace hackers. *The Express Tribune*. https://tribune.com.pk/story/831178/cybercrimes-pakistan-lacks-facilities-to-trace-hackers

Usman, M. (2017). cyber crime: Pakistani perspective. *Islamabad Law Review*, *1*(03), 18–40.

Vasudevan Sridharan. (2016, November 8). Pakistan passes “draconian” cybercrime law threatening civil liberties. *International Business Times*. https://www.ibtimes.co.uk/pakistan-passes-draconian-cybercrime-law-threatening-civil-liberties-1575530

Zia UL Islam, Khan, M. A., & Zubair, M. (2019). Cybercrime and Pakistan. *Global Political Review*, *IV*(II), 12–19. https://doi.org/10.31703/gpr.2019(IV-II).02