Online ISSN Print ISSN

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

The Legislative Framework for Cybercrime in Pakistan: A Critical Analysis of PECA 2016

[1*]Fatima Rida Suddle, [2]Aden Khan, [3]Sehar Nawaz

Article Details

Keywords: Cybercrime, Cyber legislation, Pakistan, PECA 2016, Social Media

Fatima Rida Suddle
Lecturer: Department of law, University of the Sialkot, Sialkot, Pakistan. Corresponding Author Email: suddlefatima@gmail.com
Aden Khan
LL.M. Scholar, University of the Lahore, Lahore, Pakistan
Email: adenkhan45@gmail.com
Sehar Nawaz
Lecturer: Department of law, University of the Sialkot, Sialkot, Pakistan
Email: seharwarraich15@gmail.com

ABSTRACT

The rapid growth of digital tools and social networking sites in Pakistan has resulted in an alarming increase in the number of cybercrimes that represent a huge threat to the personal safety and social tranquility. This paper provides a critical analysis of how well the Prevention of Electronic Crimes Act (PECA) 2016 works in the counteraction of offence that is related to social media in Pakistan. The research paper puts forward structural weaknesses at the foundation of the legislation such as inconsistency with the constitutional rights, absence of specific comprehensive implementation mechanisms and the inappropriateness of punitive measures. Through the analysis, it is clear that even with the enactment of PECA, the reported cases of cybercrimes have increased tremendously to the level that was not experienced before the enactment of the Act which implies that it has failed to attain the deterrent effect of the Act. The study also highlights how the enforcement agencies, including the Federal Investigation Agency (FIA) and Pakistan Telecommunication Authority (PTA), fail to effectively regulate the sharing of offensive and other harmful content in the digital systems within the parameters of the current law. These results demonstrate the necessity of a legislative change that would maintain the balance between the security of fundamental rights and implementing effective measures against social media exploitation.The study concludes by highlighting the importance of adapting the legal framework to evolving technological and social conditions to develop an inclusive, secure, and just digital environment in Pakistan.

INTRODUCTION

Pakistan is making efforts to enhance development in both the public and private sectors through the adoption of the internet, 3G/4G services, and information and communication technologies (ICTs). The swift evolution of technology presents considerable challenges for governments—especially those in developing countries—in protecting individuals, institutions, and national security from cyber threats. Unfortunately, Pakistan continues to be vulnerable to cybercriminal activities. In fact, occurrences of cybercrimes are rising rapidly and becoming more common within Pakistani society. As technology continues to advance, the need for comprehensive regulations to monitor and control cyber activities becomes increasingly critical. Cyber law constitutes a vital component of legal systems intended to deter cybercrimes and regulate online behavior involving the use of digital technologies. The term cyber legislation denotes the body of laws formulated to control and respond to unlawful conduct committed through the internet, in cyberspace, or by means of computing devices (Zahoor & Razi, 2020). The development of cyber law in Pakistan remains at a nascent stage. Although enforcement authorities are attempting to tackle the issue, the overall situation continues to worsen. As a former British colony until 1947, Pakistan inherited the entirety of British legal frameworks. The 1973 Constitution of Pakistan reflects the nation's gradual approach toward legislative reform. Similarly, laws concerning cybercrime have yet to be revised and structured in alignment with the evolving demands of the digital age. In Pakistan, cybercrime remained a low-priority issue until recently, largely due to limited public awareness. Lack of special laws pertaining to cybercrime used to exist until few years back; but the recent rise in cybercrime has brought to the fore the importance of special laws. Pakistan government has introduced major interventions through promulgation of necessary laws to take on the issues confronting cyber dimensions with a view of protecting citizens who are involved in virtual activities. The following section presents the information on the cyber laws and regulatory actions that have been established in Pakistan as of now.

TELEGRAPH ACT 1885

Act of 1885 was the very first law in the country which had to regulate the practices of message surveillance and so forth. It gave the government the power to eavesdrop on communications. Though the provisions of the Act still take shape in upholding the authority of the federal and the provincial governments in violating the privacy of individuals, it has become weak in meeting the challenges that have been posed by the intricacies brought by the technological changes in the world today. Owing to the claims of acting in the public interest, the government has had its way uncritically with no checks or balances by the courts. The government is authorized to seize

telegraphic systems in those situations or cases when there are national emergencies or when there is the need to maintain the safety of the whole community. Also, under the Act, in Section 23, unauthorized entry into telegraph offices and the interference with telegraph messages is made a criminal act with legal penalty to the offence.

THE ACT, PAKISTAN TELECOMMUNICATION (RE-ORGANIZATION) ACT, 1996

The PTA was launched to look after the development, regulation and operation of telecommunication networks, provision of telecom services. The PTRA 1996 was also drafted to increase the internet monitoring and surveillance power of a state. The work of PTA does not just include the process of control of the communication sector in Pakistan. It is also used in protecting the interests of consumers in any telecom related transactions. The authority is charged with the role to receive complaints made by citizens and organizations and has the mandate to act accordingly. Moreover, the fact that the Act bestows the duty on the Frequency Allocation Board or the Telecommunication Authority to inform the judiciary about any form of unlawful telecommunication activities. The courts in such instances can use their authority to issue warrants on suspected crimes. The acts also give the law enforcers the right to seize the gear involved in the unlawful activities and investigate intensively.

NATIONAL I.T. POLICY 2000

In 2000, the Government of Pakistan came up with an information technology policy, which had an intention of developing laws on how to deal with cybercrime. The formulation of this policy was done by doing a comparison of the legal systems of other civil and common law jurisdictions, and also the UNCITRAL Model Laws. Although the strategic initiatives of several nations were discussed, the policy was mainly coded on the basis of the so called International Consensus Principles on Electronic Authentication developed by the Internet Law and Policy Forum. The main goal of such a move was to make electronic commerce more secure and enhance protection of people data. This action has been quite a milestone towards protection of cyberspace.

ELECTRONIC TRANSACTIONS ORDINANCE, 2002

Pakistan has seen the rise of cyber laws slowly. ETO 2002 was the former legislation in the country that dealt with cybercrime, but its area of focus was limited to a few offenses only. The main aim of the Ordinance was to enable and coordinate information, records, documents and the transactions undertaken electronically and was to also set up the means of recognizing registered service providers. This Ordinance actually focused on electronic commerce bodies and online transactions in the bid to fight cybercrime. It was the first case in which Pakistani government tried to address the issues in the cyberspace and develop legal provisions related to them as the

ETO 2002 occurred. Before it was instituted, matters concerning cybercrime were carried out on the Telegraph and Telephone acts and the regular courts used to administer the complaints. This law assists the corporate sector by the companies that offer these services, consumers and individuals who have utilized the services with regards to settling disputes that occur in the cyberspace due to cybercrime.

This Ordinance was promulgated by the National assembly of Pakistan in September 2002. The foremost aim of the law was to give legal status to the different transactions done in the cyberspace. Using this Act, the legal validity of electronic signatures and records was provided. Also, the regulation suggested that the Federal Government set standards related to data protection and the privacy of users (Zahoor & Razi, 2020). Electronic documents were not actually recognised or legally accredited before the establishment of the ETO 2002. Cybercrime also found its way to the ETO 2002 through criminalizing access by unauthorized persons into, and destruction of information systems. However, the law had a number of uncertainties. It omitted some of the crimes previously covered by the law of cybercrimes of other nations. Despite that it was one of the first steps and shaped the framework of further cyber laws, the Act was rather limited and did not imply a great variety of cybercrimes. The increased civilization in the use of digital media has also raised new legal issues, whereby, there is the need to come up with elaborate legal applications and legal structures, as well as the more specific laws of cybercrime in order to protect the digital rights of individuals.

ELECTRONIC CRIMES ACT, 2004

This was a legislation enacted as per the stipulations put forth by the ETO 2002 facilitated by the Ministry of Information Technology. The law defined a set of crimes that occurred in the cyberspace and put them under the group of cybercrimes. The Electronic Crimes Act (ECA) defines cybercrime as the use of techniques of unauthorized communication, otherwise known as, interception, spoofing, spamming, cyberstalking, and unauthorized access. It also deals with more sinister crimes such as system destruction, electronic forgery, electronic fraud, and cyber-terrorism. Moreover, abuse of telecommunication gadgets and encryption together with the use of viruses is also identified as one among the typologies of cybercrime. This law however, did not provide any particular enforcement agency. Moreover, the crimes that were described in the legislation were not very specifically defined. The descriptions were wide and general and hence hard to understand. The absence of enforcement procedures and definition of cybercrimes as offenses that are not clearly defined violated the effectiveness of this legislation.

PREVENTION OF ELECTRONIC CRIMES ORDINANCE, 2007

The increasing rate of cybercrime in the country ultimately gave rise to a very urgent need to deal with such a situation through special legislation. Consequently, the former President General Pervez Musharraf issued the PECO in 2007 (Munir, 2020). This legal step covered a small spectrum of electronic crimes that were in the field and this made it an early form of cyber law. Presidential orders were made to implement the Ordinance three times namely on May 2008, February 2009, and lastly on July 4, 2009. These endeavours, however, failed to see the Ordinance be raised to the parliamentary agenda in any formal manner and it eventually expired under constitutional powers.

CYBER SECURITY COUNCIL BILL, 2014

The bill is the Cyber Security Council Bill (CSCB) presented by Senator Syed Mushahid Hussain on April 14, 2014. The bill proposed the establishment of a council to address cybersecurity challenges both domestically and internationally, along with the formulation of a comprehensive cybersecurity strategy extending over a period of ten to twenty years, supported by relevant regulations. However, the government has not yet approved the CSCB.

PREVENTION OF ELECTRONIC CRIMES ACT, 2016

The PECO 2007 was replaced by the PECA 2016, which now serves as the primary legal framework for prosecuting cybercrimes in Pakistan.

BACKGROUND

The new cybercrime legislation started as a debate in the year 2014, after a terrorist attack on the Army Public School (APS) in Peshawar wherein more than 150 students and teachers had lost their lives. In response to the incident, Pakistan formulated a National Action Plan comprising twenty measures aimed at countering extremism. A draft bill was proposed for parliamentary consideration in February 2015. The National Assembly approved the bill in April 2016. Subsequently, in July 2016, the Senate unanimously passed the bill after introducing fifty amendments to the original version. These amendments were then referred back to the National Assembly for further review, and the legislation was officially enacted in August 2016. The President granted approval to the PECA 2016 in the same month, thereby bringing a formal anti-cybercrime law into effect in Pakistan.

OVERVIEW OF PECA, 2016

The PECA serves as an extension of Pakistan's penal code, addressing both procedural and substantive aspects of cybercrime. The Act encompasses a broad range of offenses, including unauthorized access to data or devices, unlawful interference with data or information systems,

phishing, spoofing, and digital piracy—all classified as serious cybercrimes subject to legal penalties. It further includes cyberstalking, electronic fraud, electronic forgery, cyberbullying, identity theft, and cyberterrorism as major offenses under its scope. The primary objective of the legislation is to prevent the dissemination of hate speech, incitement to violence, and terrorism through electronic means, while also responding to the increasing incidence of cyber-related offenses. The justification for this law stemmed from the inadequacy of previous electronic crime statutes in addressing newly emerging cyber threats. It was maintained that PECA would mitigate cyber-related misconduct, protect individuals from cyberattacks, enhance national security, and foster a secure environment for the growth of the information technology sector.

CRITICAL ANALYSIS OF PECA

The PECA seeks to address cybercrime through electronic means; however, the legislation is poorly structured. In criminal law, statutes that impose legal liability must be clear and precise. PECA, however, contains multiple ambiguous provisions. For example, (Akhlaq, 2021)

i. Section 3 penalizes unauthorized access to data or information systems carried out with "dishonest" or "fraudulent" intent. The problem lies in the absence of a defined legal standard for what constitutes dishonesty. The Act fails to specify the threshold for dishonest intent or clarify its scope. This raises questions regarding individuals who can prove the absence of dishonest or deceptive intent—does this exemption validate their unauthorized access to private data?

The legal doctrine of "void for vagueness" applies to statutes with unclear terminology. Laws, particularly those that criminalize conduct, must articulate prohibited behavior in straightforward terms comprehensible to the public. Individuals should not be left uncertain about the nature of criminal acts. The U.S. Supreme Court (SC), in *Connally v. General Construction Co.*, declared that vague laws—those requiring individuals to interpret their meaning—are unconstitutional. Consequently, several PECA provisions may be considered unconstitutional due to their vagueness, as they may violate Article 10-A of the 1973 Constitution, which ensures the right to a fair trial and due process. Under this principle, individuals must be made aware of the charges against them and the specific acts for which they are being prosecuted.

ii. Critics contend that PECA grants excessive authority to law enforcement agencies, undermining due process and increasing the potential for misuse. The legislation gives authorities full discretion in interpreting the accused's dishonest intent, which is a key element in several offenses under the Act. Similarly, there are no defined standards for assessing the "intent to cause harm" or the "intent for wrongful gain," leaving these determinations entirely at the discretion of the investigating authorities. As a result, the PTA is afforded unchecked power

under the Act.

iii. The definition of cyberterrorism under PECA is another point of concern. It includes any offense listed in Sections 6 to 9, committed with the intention of spreading fear, panic, or insecurity among the public. This definition is excessively broad and susceptible to misuse. It allows non-terrorism cases to be prosecuted under terrorism laws at the discretion of the executive, resulting in disproportionately severe penalties. Historical misuse of anti-terrorism laws highlights the risks of such broad definitions. Research by a non-profit organization examining Pakistan's prison system revealed that 80% of those convicted under terrorism laws had no connection to terrorism, with only 20% fitting the conventional understanding of the term (Justice Project Pakistan & Reprieve, 2014).

iv. PECA differentiates between cognizable and non-cognizable offenses. Under the Act, only a few crimes—such as the use of sexual images for blackmail, child pornography, and cyberterrorism—are classified as cognizable, meaning that law enforcement officers may arrest suspects without prior court approval. All other cybercrimes are deemed non-cognizable, requiring a court-issued warrant for arrest or investigation. Sections 30 and 31 of the Act permit courts to issue search warrants upon receiving a request from an investigating officer. However, the use of the word "may" in these provisions introduces discretionary language, allowing courts to reject warrant applications if they are not convinced. These procedural requirements hinder effective cybercrime investigations, especially given the limitations in staff and resources already acknowledged by Mr. Waqar Ahmed Chauhan, Director of the FIA's Cyber Crime Wing.

v. Despite the classification of most PECA offenses as non-cognizable, a review of First Information Reports (FIRs) reveals that the Federal Investigation Agency (FIA) frequently includes cognizable offenses from the Penal Code, PECA, and anti-terrorism statutes to justify arrests and conduct investigations. This practice represents a misuse of legal provisions. Instead of relying on such measures, the law should be revised to equip authorities with appropriate powers specific to their jurisdiction.

vi. A further deficiency in PECA lies in its inability to regulate international internet corporations operating in Pakistan's digital space. The law lacks jurisdiction over these entities, creating a legal void that obstructs the monitoring and regulation of content distributed by global digital platforms.

vii. Notably, Pakistan has no specific legislation dedicated to data protection. Currently, PECA serves as the only legal instrument that partially addresses data-related concerns. Though, data protection is not a primary focus of the Act and is only minimally covered. Inspired

by the European Union's General Data Protection Regulation (GDPR), The Personal Data Protection Bill 2021 has been proposed under the name Bill titled Personal Data Protection Bill 2021, and is yet to pass. Therefore, PECA is the presumed framework that is applied in data protection, although the flaw of this framework in this regard is undisputed.

viii. PECA enables the real time data collection when a court order is acquired also. This becomes a great cause of concern because this clause can lead to invasive surveillance frameworks that can either target people on an individual basis or widespread. This is the contradictory side of the legislation with reference to the monitoring regulations in the Fair Trial Act, thus giving rise to more legal and ethical concerns.

ix. The PECA also mandates Internet Service Providers (ISPs) to store traffic data of their users over a one-year period and to hand it over in case an investigation takes place, as such, in response to a request by the PTA. This is a significantly longer retention period as compared to the 90 days retention that existed previously. This kind of prolonged data retention goes against the international privacy standards. Further, the Act does not provide clear guidelines on how data should be stored and thus increases the chances of data losses. Without any system of effective privacy and data protection laws and legislation, user data storage and retention represents significant harms to individual privacy, the data can be misapplied, spied on, or even targeted.

x. Increase in Cases of Child pornography in Pakistan over the last few years. According to the section 19(3) of PECA, any individual who produces, posts, distributes, transmits, acquires, or possesses sexually explicit content of a minor may be fined up to five million rupees, jailed up to seven years or be fined and sent to jail. But case studies show that most of the people engaged in such crimes usually run into organized pornographic rings. The punitive performance of the existing penalties can be deemed as lacking when reached to criminals that are associated with larger criminal groups. Hence, there is a driving necessity to have clauses to the law that render more severe penalties on these organized groups.

xi. ECA has also been widely criticized for infringing on the fundamental right to freedom of expression as guaranteed under Article 19 of the Constitution of 1973. Several sections of the Act are used to curtail free speech in Pakistan. The vague language of the statute allows authorities to suppress dissent and control public discourse. PECA is particularly noted for its overregulation of online content and for granting sweeping censorship powers to regulatory bodies. Under Section 37, the PTA is authorized to block or remove online content deemed contrary to Islamic values, morality, national security, or public order. However, these criteria

are overly subjective and lack clearly defined standards. The discretion to decide what constitutes a violation rest solely with the PTA, allowing it to act unilaterally. Restrictions on free speech should be determined by the judiciary, not an administrative authority. As a constitutional right, freedom of expression must be safeguarded by the state. Historically, the PTA has exercised these powers to censor significant amounts of online content. According to a report by the Digital Rights Foundation, the PTA blocked approximately 1.4 million URLs in 2022. Additionally, in April 2023, the Senate was informed that actions had been taken against sectarian and harmful posts on social media, resulting in the blocking of 35,000 Facebook pages and 59,253 URLs (Digital Rights Foundation, 2023). While PECA is intended to address cybercrime, many of its provisions have been criticized for suppressing freedom of expression.

AN ANALYSIS OF PECA'S EFFECTIVENESS IN COMBATING CYBERCRIME IN PAKISTAN

The subsequent section outlines the various ways in which social media platforms are utilized for engaging in cybercriminal activities within Pakistan, along with an evaluation of the extent to which the PECA 2016 has been effective in curbing such misuse.

CYBER FRAUD

Internet-based financial fraud entails the use of digital platforms such as social media networks, email services, chat rooms, and online message boards to conduct deceptive transactions, mislead victims through fraudulent schemes, and channel illicitly obtained funds into bank accounts or to other individuals involved in the scheme (Haider, Ali, & Zubair, 2023). Social media platforms are often targeted by fraudsters due to the ease with which users can be contacted and personal information can be accessed. In *Sheraz Khan v. The State*, the accused defrauded the victim of an amount totaling 2,857,230 rupees through WhatsApp and Facebook. The Lahore High Court granted bail to the accused, holding that offences under general criminal law and the PECA 2016 could not be adjudicated concurrently.

Although social media was central to the fraudulent conduct in this case, the accused was able to exploit procedural gaps within PECA 2016. Specifically, Sections 28 and 44 of PECA 2016 permit the application of other legal frameworks, including the Pakistan Penal Code (PPC), the Code of Criminal Procedure (CrPC), and the Qanun-e-Shahadat Order (QSO), provided there is no conflict with the provisions of PECA. The inconsistencies and ambiguities between these criminal laws and PECA 2016 create opportunities for the accused to manipulate the legal process, particularly during bail hearings and trial proceedings.

CYBER DEFAMATION

Defamation refers to the dissemination of false information, whether through spoken or written means, including digital and social media platforms, with the intent to damage an individual's reputation, self-esteem, dignity, confidence, or other personal attributes in the eyes of the public (Haider, Ali, & Zubair, 2023). Social media users may, often without awareness of the implications, cause significant and lasting harm to others by sharing or posting defamatory content with ease. Cyber defamation falls within the ambit of Sections 20 and 21 of the PECA 2016, which pertain to offences against human dignity. In *Muhammad Daniyal Farrukh Ansari v. The State*, the accused was charged with multiple offences, including those infringing upon the complainant's dignity and modesty. However, the SC granted bail to the accused on the grounds that the alleged offences did not fall under the prohibitory clause. This outcome highlights a critical shortcoming in PECA 2016, namely that the penalties prescribed under the law do not adequately reflect the seriousness of such crimes. Defamation, particularly in its cyber form, constitutes a grave violation capable of inflicting permanent harm on the reputation of the victim or their family.

CYBER HARASSMENT

Online harassment entails the continuous imposition of psychological or emotional distress, and in some cases physical harm, upon an individual or group through digital communication channels or social media platforms. This form of abuse often includes actions intended to threaten, expose, or disgrace the victim publicly on the internet. Incidents of online harassment are frequently reported across widely used platforms such as Facebook, WhatsApp, Snapchat, Instagram, and TikTok. In *Waheed Dhehphal Chandio v. The State*, the perpetrator circulated explicit videos involving his former wife and sister-in-law following the dissolution of his marriage. These recordings, which had been made during the period of engagement and marriage, were subsequently disseminated to various family members of the victims via social media platforms. As a result, the accused faced charges under Sections 20, 21, and 24 of the PECA 2016.

UNLAWFUL CRITICISM OF GOVERNMENT BODIES

Individuals possess the freedom to express their views; however, this liberty is frequently misused on social media platforms. Users often direct unjust criticism toward state institutions, including the armed forces, judiciary, police, and local administrative bodies, thereby demoralizing government officials. In *Mirza Iftikhar Uddin v. The State*, the accused was charged with inciting violence by circulating videos targeting a judge of the SC. The Islamabad High

Court, in granting bail to the accused, determined that the alleged offences did not fall under the prohibitory clause.

Cybercrimes perpetrated through social media can produce far-reaching consequences for both individuals and public institutions. Although the PECA 2016 does not specifically categorize such acts, Sections 20 and 21 provide general penalties. Nonetheless, it is recommended that dedicated provisions be introduced in the legislation for offences against state institutions, accompanied by more stringent punishments.

SPREAD OF POLITICAL HATE

Political activists have established social media cells to advance the objectives of their respective parties. These entities primarily function to highlight their party's achievements while simultaneously criticizing opposing factions. They create political hostility and indeed have caused legal woes to political leaders. This subsequently has led to the development of a more intolerant and confrontational political debate. This situation has led to an increase in political hatred in the country. In an effort to ensure that the people do not indulge in or are exposed to these types of divisive behavior it is paramount that some strict rules are employed that ensure that those members of the political parties are not allowed to use social media to post incendiary material. Instead, releasing of such content ought to be under constraints by a form of regulatory body e.g. the censorship board.

SPREAD OF RELIGIOUS HATE

Social media has become one of the main sources of the spread of blasphemous and religiously provocative content. Critical contents aimed at different religious beliefs are posted by users, and this is very offensive to the followers of any religion and is a way of destroying harmony in the community. This kind of content is a source of increasing sectarian tensions causing a perturbation of peace and the maintenance of the order. A significant one was incident during the Faizabad sit-ins when various religious and political forces drove violence by giving some provocative speeches and using digital propaganda. This unrest sparked off the infringements of human rights where some people lost their lives and others their personal properties like vehicles and goods. In addition, the protests also led to obstruction of roads hence hindering the freedom of people.

The case of Muhammad Ayoub v. There were several Facebook accounts that were sharing blasphemous material in Federation of Pakistan. As an answer, the complainant filed a writ petition which was later accepted by the court. The courts ordered the PTA to censor offending material. The court, in giving other directions, advised the government to incorporate

the sentences in the Sections 295, 295-A to 295-C of the PPC as an additional sentence under Section 9 in the PECA 2016 as the offence is very serious. Although this is the order, so far no amendments have been gazetted to the legislation and there are quite a number of web sites which still post messages that stir up religious intolerance.

CONCLUSION

The advent of the internet and the popularity of the social media have transformed the sphere of the interpersonal communication and interaction making people connect and interact more effectively than previously. In Pakistan, major part of the population enthusiastically uses many social networking sites on a daily basis that has resulted in the development of remarkable changes in social behaviour, communication conventions and people discourse. Nonetheless, the digital growth has been coupled by mushrooming of cybercrimes, which remain to be one of the major threats to the security of individuals and tranquility within society. Such crimes as harassment or fraud, hate speech and invasion of privacy are already deeply incorporated on the general culture of the Internet, and are still not addressed by the current systems of the law.

Pakistan is a developing-country with less technological infrastructure and exposure to digital governance and hence, substantive challenges to manage the ill effects of the cybercrime complexity. Social media has been seen as a big problem especially because there is rampant abuse of this tool, with numerous categories of crime regularly being committed against citizens, society and the state. In the light of the growing number of such crimes, it becomes significant to refer to the adoption of the PECA in 2016 as a positive step in the legislative branch. The act was aimed at balancing and imposing a sentence on the illegal acts that were being carried out using electronic means and mostly referred to social media sites. However, adoption and success of PECA have received their share of critique due to under performance.

Even though PECA 2016 is a root effort to curb electronic crimes, it is not a complete law as it stands. The reported cases of cybercrimes in recent years have been at unprecedented levels and this is an indicator that the Act may not have delivered the intended sting of acting as a deterrence. Such inefficiency remains a continuous struggle that is coupled by structural weaknesses in the legislation itself. It has been found that there are definite discrepancies between the provisions of the PECA and the basic rights stipulated in the Constitution of Pakistan, and the binary of compatibility with democratic principles and civil liberties is therefore questionable. Besides, the absence of comprehensive implementation mechanisms, clear procedural guidelines and practical enforcement protocols coupled with the very nature of the multifaceted nature of cybercrime has further feebled its capacity to confront the challenges of

cybercrime.

The direction of penalties that are handed out under PECA is often considered to be insufficient to the magnitude and depth of crime that they deal with. The punishments, which are written in the prescriptions, do not match the psychological, reputational, or financial losses, which the victims undergo in most cases. In spite of the fact that organizations like the FIA and the PTA have been granted the power to allow them the ability to conduct surveillance and curb illegal online activities in a bid to protect and regulate specific wrong doings of the other users, they seem to lack compromise and effectiveness in their endeavors. Unusable and hurtful material remains very common in digital areas, and it is an indicator of the flaws in using the current formal apparatus as far as enforcement agencies are not able to contain the abuse as extensively as they need to consider the topic.

This fact brings into serious question the effectiveness of PECA in fighting crimes that occur through social media. Although any law will not be expected to operate in a flawless manner, there must be a range of revisions of the law, its time-to-time modifications in line with the emerging technological and social environments. Thus, the reformation of PECA should be made a legislative and administration priority. The ultimate objective of this process of reform should be to develop a very fine balance, on the one hand what the fundamental rights of individuals to free speech, privacy, and access to information are, and also ensuring in place are effective mechanisms to prevent other abuses created by the power of social media, whether by governments or by individuals. It is only by doing so that the Pakistani legal system can stand to come up with an inclusive secure and justice-related digital environment.

REFERENCES

1. Akhlaq, M. (2021). Cybercrime in Pakistan: A study of the law dealing with cybercrimes in Pakistan. PCL Student Journal of Law, 5(1), 1. LEAP Pakistan. https://leappakistan.com/pclsjl-vol-5-issue-1-2021/

2. Connally v. General Construction Co., 269 U.S. 385 (1926)

3. Cyber Security Council Bill, 2014

4. Digital Rights Foundation. (2023). DRF annual report 2023. https://digitalrightsfoundation.pk/wp-content/uploads/2024/04/DRF-Annual-Report-2023.pdf

5. Electronic Crimes Act, 2004

6. Electronic Transactions Ordinance, 2002

7. Haider, W., Ali, A., & Zubair, M. (2023). Prevention of Electronic Crime Act, 2016: An analysis of the Act's effectiveness in controlling misuse of social media in Pakistan. Journal of

Educational Research & Social Sciences Review. https://ojs.jerssr.org.pk/index.php/jerssr/article/view/197

8. Information Technology Policy and Action Plan, 2000

9. Justice Project Pakistan & Reprieve. (2014). Terror on death row: The abuse and overuse of Pakistan's anti-terrorism legislation. https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/AdvisoryCom/Terrorism/JusticeProjectPakistan_1.pdf

10. Mirza Iftikhar Uddin v. The State, Criminal Misc. No. 908-B/2020 (Islamabad High Court, August 20, 2020)

11. Muhammad Ayoub v. Federation of Pakistan, W.P. No. 3553/2017 (Lahore High Court, April 10, 2017)

12. Muhammad Daniyal Farrukh Ansari v. The State, Criminal Petition No. 1414 of 2020 (Supreme Court of Pakistan, January 18, 2021).

13. Munir, M. A. (2010). Electronic Crimes Ordinance: An overview of its preamble and extent. Pakistan Journal of Criminology, 2(1), 189–202. http://www.pjcriminology.com/wp-content/uploads/2019/01/14-5.pdf

14. Pakistan Telecommunication (Re-organization) Act, 1996

15. Prevention of Electronic Crimes Act, 2016

16. Prevention of Electronic Crimes Ordinance, 2007

17. Sheraz Khan v. The State, Crl. Misc. No. 44216-B/2021 (Lahore High Court, July 27, 2021).

18. Telegraph Act, 1885

19. The Constitution of the Islamic Republic of Pakistan, 1973

20. Waheed Dhehphal Chandio v. The State, Crl. B.A. No. S-180 (High Court of Sindh, Sukkur Bench, June 24, 2019).

21. 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. https://doi.org/10.51872/prjah.vol2.Iss2.43