Journal of Pakistan Administration | 45(2): December (2024) | 66–91 | ISSN: 1027-1023

A Critical Analysis of Efficacy of the Prevention of Electronic Crimes Act, 2016:

Irritants and Remedies

Syed Khizar Ali Shah[1]

Suggested Citation:

Shah, S. K. A. (2024). A Critical Analysis of Efficacy of the Prevention of Electronic Crimes Act, 2016: Irritants and Remedies. *Journal of Pakistan Administration. 45*(2). 66–91.

Received: August 6, 2024/ Accepted: November 21, 2024/ Published: December 30, 2024.

Abstract

Cyber technologies are rapidly proliferating in Pakistan manifesting their pros and cons on the Pakistani governance system and society necessitating a new social contract between the state and citizenry. Prevention of Electronic Crimes Act (PECA, 2016) is an attempt to define the contours of this new state-citizen relationship in the cyberworld. However, PECA's purported relevance has been submerged under the civil society's backlash at the controversial enforcement of PECA, 2016 and the unabated deluge of cybercrimes. A comparative analysis of India's response mechanisms against the ever-evolving challenge of cybercrimes can help policy makers in Pakistan to tackle the issue effectively. Moving forward, Pakistan may have to rectify its policy orientation from being security centric to citizen centric by introducing humane amendments in PECA, 2016 and make prudent investments in capacity building of its citizens and state agencies.

Keywords: *PECA, 2016, cybercrimes, digital rights.*

[1] Information Group, Government of Pakistan
e-mail: skhizars@gmail.com

1. Introduction

Regulation of cyberspace is a hotly contested and debated topic around the world mainly because of the empowering effect of cyberspace on the masses in terms of expressing their voice and the ensuing freedom to criticize the performance of the government and state institutions (Khan, 2018; Rakha, 2023). Civil society and human rights activists want to zealously guard this newly acquired freedom of expression and, therefore, any legislative or coercive measures to regulate cyberspace are deeply scrutinized and sometimes vehemently opposed (Khan et al., 2019; Leghari et al., 2024; Rafiq, 2019). Whereas governments and state institutions want to combat fake news and maligning of government figures and state institutions (Rubsamen, 2023).

The concerns of civil society notwithstanding, it is an established fact that illegal use of cyberspace and cyber or digital crimes are proliferating at a breakneck rate (MacDermott et al., 2020). "Since 2001, the victim count has increased from 6 victims per hour to 97, a 1517% increase over 20 years" (Griffith, 2024). Even the developed countries with high literacy rates and digitization are struggling to contain cybercrimes like hacking, identity theft, harassment, and many others. In this context, the need for effective legislative and enforcement mechanisms cannot be denied. India is one of those countries which has made noticeable progress in the regulatory framework of cyberspace over the past twenty years (Singh, 2023). The interpretation and judgments of India courts have helped in strengthening of cyber legal framework in India (Singh, 2023).

However, given the secretive traditions and human rights record of many less developed countries, cybercrimes laws can be perceived to be double edged swords which in addition to curbing cybercrimes can also be used to curb freedom of expression (Najib et al., 2024; Runa, 2019; Young, 2004). Pakistan is one such country witnessing an intense debate amongst the supporters and naysayers of the cyber regulation (Abbas et al., 2023). In regulating cyberspace, Pakistan is at a crossroads between strict enforcement of law and regulations or using an empowering approach towards its citizens (Iftikhar et al., 2024). There is one opinion that PECA, 2016 filled a long standing vacuum in the regulation of cyberspace in Pakistan by positively contributing to the apprehension of cyber criminals (Yongmei & Afzal, 2023). However, there are equally vociferous voices over the use of PECA, 2016 suppress open debate and freedom of speech (Abbas et al., 2023). Hence, exploring the right balance between restrictions and freedoms allowed under cybercrime laws can be an interesting and relevant area of research in the context of overall governance framework.

1.1. Statement of the Problem

The terms electronic crimes, digital crimes or cybercrimes are used to describe the crimes committed by using any gadgets or technologies collectively described as Information Technology. Cybercrimes have registered a sharp uptick globally since the heralding of new millennium, Pakistan being no exception. The rapid digitization of governance, economy and social relations (by social media) has been accompanied with a simultaneous proliferation of cybercrimes in Pakistan.

Prevention of Electronic Crimes Act, 2016 (PECA, 2016) was enacted with the purported objective of identifying and curbing crimes committed through electronic or digital means. However, since its inception, PECA, 2016 has been the subject of intense debate and controversy. Human rights advocates and legal experts have criticized the PECA, 2016 for being flawed in terms of its language, scope and enforcement mechanism. On 8th April, 2022, Islamabad High Court struck down some provision of PECA Amendment Ordinance 2022, further clouding the common perceptions about the law. Moreover, the data indicates that cybercrimes have exponentially increased since the enactment of PECA 2016 raising serious questions about the efficacy of the law. This scenario necessitates an in-depth and methodical research about the efficacy of PECA, 2016.

1.2. Research Questions

The overarching research question is "How can the Prevention of Electronic Crimes Act, 2016 become an effective legislative tool to combat cybercrimes in Pakistan?"

1.2.1. Sub-questions:

i. How is expanding digitalization of service delivery and proliferation of social media linked to empowerment and freedom of speech in Pakistan?

ii. How and why incidence of cybercrimes is increasing in Pakistan?

iii. Why PECA, 2016 has been subjected to so much criticism and controversy and how can the controversy and irritants in implementation of PECA, 2016 be removed?

2. Review of the Literature

The nature and complexity of cybercrimes is a daunting research challenge, as motivations for such crimes range from "destructive entrepreneurship" of unemployed IT experts (Kshetri, 2016; Naudé, 2024) to the poor mental health

issues marauding trolls (March , 2022). Another striking feature of cybercrime literature is that due to "inherently free" nature of Internet, scholars have been particularly cautious and tentative in developing a discourse about cybercrimes laws lest they infringe upon new freedoms assured by cyberspace (Abbas et al., 2023; Flor, 2012). Literature about cybercrime laws in Pakistan and PECA, 2016 indicates an overwhelming consensus about the inadequacy of the cybercrime legislation and enforcement mechanisms in Pakistan in terms of protection of digital rights (Aleem et al., 2021; Arshad Khan, 2018; Haq & Atta, 2019; Usman, 2017; Zahoor & Razi, 2020). Like elsewhere, researchers in Pakistan are also apparently preoccupied with the potential threat to civil liberties and freedom of speech posed by cybercrime legislation and enforcement (Iftikhar et al., 2024; Khan, 2018; Khan et al., 2019). One of the major concern and criticism of the PECA, 2016 recurring in literature is the apparent contradiction of PECA, 2016 with certain provisions of ICCPR (Khan & Tehrani, 2018). The violent acts such murder of Mashal Khan has further intensified the feeling among human rights activists that Pakistan's cybercrime laws are vulnerable to devious manipulation and mala fide intent (Dad & Chaudhri, 2017; Khan & Tehrani, 2018; Saleem et al., 2023). PECA, 2016 has been further criticized for ambiguous language, arbitrary powers granted to PTA and FIA leading to arbitrary enforcement (Anjum, 2020; Khan et al., 2021; Zahoor & Razi, 2020). A major gap appearing in the scholarship on cybercrimes is about the seemingly dialectical relationship of digital empowerment and proliferation of cybercrimes. Secondly, in the context of Pakistan, literature on PECA, 2016 fails to critique the law within the framework of a robust theoretical framework of cybercrimes. Authors such as Munir & Shabir (2018), Kamran, Arafeen, & Shaikh, (2019), Jamshed et al. (2022) and Zahoor & Razi (2020) lack any theoretical grounding in their critique of PECA, 2016. A good theoretical reference point in understanding the genesis of cybercrimes is Jaishankar's (2007) Space Transition Theory (STT) of Cybercrimes which suggests that cybercrimes reflect a repressed criminal behaviour in physical space because of the anonymity of cyberspace, bandwagon effect on cybercriminals, high prevalence of cybercrimes in closed societies and conflict of sociocultural values with the values of cyberspace (Assarut et al., 2019). Since the publication of STT, it has been recognized as the landmark theory of cybercrimes applicable in various contexts and Jaishankar (2008) has been acknowledged as the "Founding Father of Cyber criminology" (Holt et al., 2016; Kethineni et al., 2018; Ndubueze, 2021).

3. Methodology

This research was carried out using exploratory qualitative methodology. The data collection was mainly done through secondary sources including research

articles and newspaper reports. Secondary data was supplemented and triangulated with qualitative thematic analysis of semi-structured interviews. A convenience sample of 10 respondents was planned for this purpose, however, only 7 respondents eventually agreed to give interviews. The respondents included 2 officers of FIA, 3 lawyers, 1 CEO of digital rights organization and 1 academician with background in digital rights. 3 officers of FIA eventually declined to give interviews despite initial confirmation. Convenience sampling allowed the researcher to access the most number of respondents within the constraints of time, money and security. The respondents had a diverse range of experiences and skills in the fields of digital rights, prosecution and policing of cybercrimes. The methodology for this research emerged from the literature review on digitalization, cybercrimes, PECA, 2016 and digital rights. The literature review established that there are two major schools of thought on PECA, 2016, one consists of civil society and digital rights activists and the other consists of government functionaries particularly FIA officials. Hence, respondents were selected to secure views of the two divergent clusters of opinions on PECA, 2016. The interview transcripts were codified and analyzed according to the manual of Qualitative Coding by Saldana (2021).

4. Digitalization, Empowerment and Cybercrimes in Pakistan

4.1. Digitalization and Empowerment

The digital era with the internet-connected world is creating new venues for social and economic development (Okeleke, 2018) and Pakistan is not an exception. At the World Economic Forum in 2017, Ebay's chief executive, Devin Wenig, highlighted Pakistan as one of the fastest growing e-commerce markets in the world (Majid, 2018). Mobile technology is at the heart of digital transformation in Pakistan providing fast, reliable and affordable connectivity. After the onset of Covid-19, the Internet Banking users increased by 26.3% and Mobile Phone Banking users increased by 27.5%. Similarly, the number of registered e-Commerce Merchants also increased by 62.79% (SBP, 2021) and digital connectivity rose in the country to over 50 percent in 2021. The country currently has 116 million mobile internet subscribers and 119 million broadband subscribers (PTA, 2022).

In line with the current potential of digital technologies, Pakistan has modified its policy framework for facilitating the digitization processes for socioeconomic empowerment. The policy has been designed with the presumable intent of empowering citizens through participation, efficiency, transparency, and accountability in different sectors of society (Khan, 2021). Similarly, Digital Pakistan Policy, has been launched by Ministry of IT

ostensibly to positively influence socioeconomic welfare through affordable and reliable IT infrastructure.

The different aspects of empowerment under digitalization are discussed as under:

4.1.1. Freedom of Speech

The advent of smartphones and social media apps gave a fresh impetus to freedom of speech (Liaquat et al., 2016). Events like Arab spring helped nurture a new crop of digital rights activists in Pakistan who have showed their determination to jealously guard the newly found avenue to voice their opinions (Yusuf et al., 2013). Mobile technology is also enabling the application of the Internet of Things (IoT) across areas including agriculture, clean energy and safe water solutions (Okeleke, 2018). Despite significant digital deprivation in large swathes of the country, social media is thriving in Pakistan's urban and peri urban centers. Nevertheless, digital freedoms remain a contentious issue as the government tries to balance the need for fostering a conducive digital economy while at the same time satiating its need for control over speech and narratives in online spaces. Pakistan was ranked as "Not Free" in the Freedom on the Net Report published by Freedom House, a ranking it has had the dubious honour of retaining for a number of years (Freedom House, 2022). Other watchdogs have raised alarm regarding the increasing use of laws to silence critics and journalists in online spaces as marking a decline in online freedoms (Khan, 2021).

4.2. Financial Empowerment

Evidence emerging from various sectors seems to favour the assertion that digitalization has an empowering effect over various marginalized groups who have been provided cash support through digital services like Easy-paisa and JazzCash. BISP's operations show that that rapid expansion of digital payments can generate immense dividends by ensuring efficient disbursement of cash based digital payments (Batool et al., 2021). One study indicates even informal training of social media has helped women in Pakistan in strengthening their social networks, managing daily affairs regarding their personal life and most significantly being engaged in entrepreneurship from digital forums (Anzak & Sultana, 2020). Nevertheless, fintech can be used to improve the accessibility of common citizens to banking services as Pakistan has a high teledensity of 85% with 181 million mobile subscribers (Ali, 2022). Fintech is not just about giving people financial tools to better manage their finances.

4.3. Digitalization and Cybercrimes

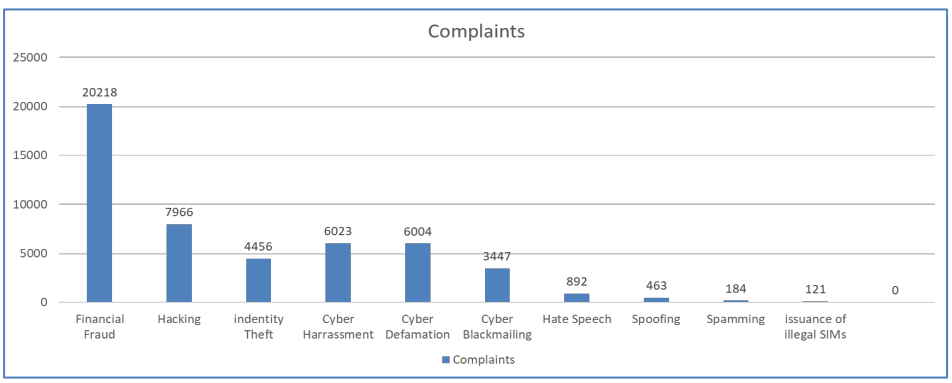
Cybercrime can be defined as "Offences that are committed against individuals

or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" (Akhlaq, 2021). Major reasons for the increase in cybercrimes in Pakistan can be identified as lack of awareness about cybersecurity, lack of FIA's enforcement capacity and unemployment amongst educated youth has created fertile ground for cyber criminal to exploit the digital medium (Hameed & Naqvi, 2021).

Cybercrime in Pakistan has increased by 83pc in the past three years with financial frauds at social platforms at the top. FIA received a total of 102,356 complaints related to cybercrime in the year 2021 underscoring an astounding surge increase in cybercrimes reported under the PECA, 2016 (Khilji, 2022). Financial frauds, harassments, fake profiles, defamation and hacking are the fastest growing cybercrimes in Pakistan (Abbasi, 2021). According to the data obtained from FIA reflected in Figure: 1, financial fraud is the cybercrime with the highest frequency followed by hacking, harassment, defamation, identity theft and blackmailing.

Figure 1.

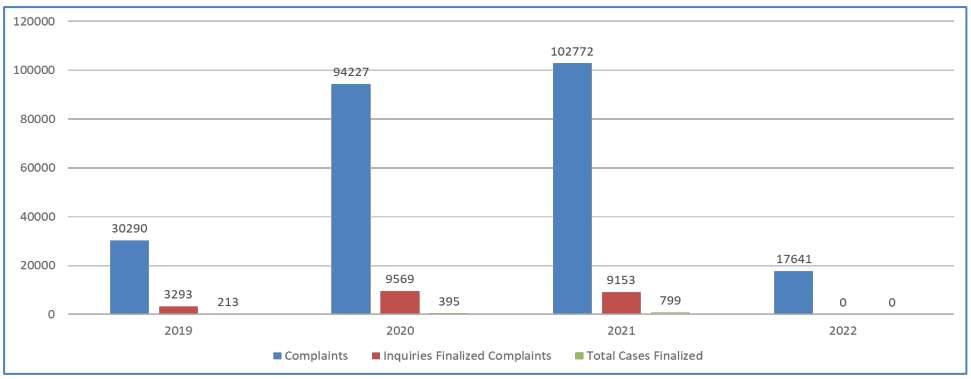
Complaints Type



Source: FIA, Cyber wing

The data given in Figure 2 indicates that pendency of unresolved inquiries is piling up due to a shortage of financial, human and infrastructural constraints of FIA.

Figure: 2



Source: FIA, Cyber wing

5. Critical Analysis of PECA, 2016

The absence of a law dealing with digital and cybercrimes was a much-lamented fact in Pakistan for the first decade and a half of the new millennium. In this context, the enactment of PECA, 2016 was much anticipated and awaited to fill a major legal and regulatory vacuum. Nevertheless, controversy marred the promulgation of PECA as it was alleged that PML-N government bulldozed the controversial PECA, 2016 bill despite the opposition's protests against the sweeping powers granted to executive that threatened freedom of expression in the country (Arshad Khan, 2018; Naseer, 2022). On the contrary, government insisted that PECA, 2016 was enacted after a thorough process of discussions with the concerned stakeholders and civil society (Khan, 2017). The then Minister for IT, Anusha Rehman, said that "Cyber Crime Law has been weakened and not remains even 40 percent of the original draft, after some NGOs [who had vested interest] raised the issue while quoting attack on freedom of expression" (Khan, 2017).

During the six years of its existence, PECA, 2016 has been the subject of controversy and intense debate for various reasons discussed below:

5.1. Ambiguity of Language

There are various provisions of the law which have not been clearly defined or explained in the law and therefore, the law becomes vulnerable to misuse and misinterpretation (Arshad Khan, 2018; Hamdani, 2016). For example, the word "act" has only been described as a "series of acts". Secondly, the words "create hatred" have been included but not explained in the definition of "dishonest intention". It has been argued by critics that "cyberterrorism" has been defined too broadly in the law by inclusion of "inter-faith, sectarian or ethnic hate" as

a qualifier for cyber-terrorism (Arshad Khan, 2018).

5.2. Discretionary Powers of PTA

Section 37 of PECA, 2016 gives draconian powers to PTA to block or censor any online content without the orders or interventions of the court. This power is in apparent violation of the Article 19 of the constitution as the restrictions provided in Article 19 can only be interpreted by the courts and not by any executive agency. Moreover, **Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021**, framed under Section 37 of PECA, 2016, allow PTA to block any website or platform on the directives of court and federal government or under any law (Shahzad, 2020). However, the history of PTA's regulatory actions is so controversial that such arbitrary powers are bound to create further distrust and uneasiness in the society (Freedom House, 2022).

5.3. Threats to Privacy

The Constitution of Pakistan enshrines the right to privacy as a fundamental right under Article 14(1). Moreover, Article 17 of the ICCPR, to which Pakistan is a signatory, states that "no one shall be subject to arbitrary or unlawful interference with his privacy, family or correspondence" (Privacy International, 2019). However, several sections of PECA, 2016 threaten the right to privacy because of the sweeping powers granted to FIA and PTA (Privacy International, 2019). Section 31 of PECA is particularly problematic as it does away with the requirement of a warrant for gaining access to an individual's data if deemed appropriate by the investigation officer. Similarly, under Section 32 of PECA, PTA can retain data about any individual from service providers up to a period of one year. Section 42 of PECA, 2016 poses another alarming threat to privacy as it empowers the government to share any data with any international government on the pretext of cooperation against cybercrimes (Rice, 2016).

5.4. Freedom of Speech

Civil society and rights activists and political parties have persistently criticized PECA, 2016 as a tool for clamping down freedom of speech and political opposition. These actions of the government were immediately termed as a blow to freedom of expression, resulting in self-censorship, arrests and detentions of workers and social media activists of opposition parties (Reporters sans frontiers, 2022). Section 26 of PECA, 2016 was a particular bone of contention as it criminalized "spoofing" which is normally considered to be ordinary political satire acknowledged and appreciated in every society (Zahra-Malik, 2016). One indicator of the perception of decreasing freedom of

expression is Pakistan's ranking on press freedom index which has dropped from 145 in 2020 to 157 in 2022 (Reporters sans frontiers, 2022).

6. Role of FIA

FIA came into the limelight after the passage of PECA, 2016 as the premier LEA responsible for combatting cybercrime. Nevertheless, powers granted to FIA under the law have been termed as draconian, arbitrary and vulnerable to abuse. For instance, Section 33 of PECA, 2016 empowers Federal Investigation Agency to access any digital device that may be required for the purpose of investigating a crime or offence. This provision of PECA, 2016 has been vehemently contested by rights activists as tool to violate privacy and to target political opponents.

In order to control cybercrimes, the government has established cybercrime wing in FIA. The wing has six zones and 15 circle offices throughout the Pakistan (Azeem, 2018). The government has also established 15 forensics laboratories for the forensics of digital devices. Upon the directions of the current government the two billion budgets have recently been issued to the cyber wing of federal investigation agency (Ahmed, 2022). The cybercrime wing has recently purchased the 5 GSM locater which will help the investigation officers to pin point the exact location of accused. Furthermore, the cybercrime of FIA has recently purchased the high end digital forensic workstations for audio video forensic analysis. The FIA cybercrime wing has also established storage area network (SAN) that is connected with forensic workstation through fibre optical used for data storage.

Despite the above-mentioned steps, FIA still suffers from following capacity issues:

6.1. Lack of Infrastructure

FIA's presence limited to the largest cities of Pakistan means that organization has a small enforcement footprint across the landscape of Pakistan. Some complainants have to suffer the hardship of travelling for hundreds of miles to lodge a complaint with FIA. Similarly limited cybercrime courts, cause people of far-flung areas the unnecessary hassle of travelling long distances to pursue the trial of their cases.

6.2. Attitude Problems

FIA's staff is still struggling to come to terms with the sensitivities of victims of cybercrimes. The low "complaints to cases" ratio indicates that FIA's staff is not very forthcoming on vigorous pursuit of the complaints registered under PECA. Marginalized groups like women and minorities are more likely to be

discouraged by FIA to pursue their cybercrime cases. There have been reports of victim-blaming by FIA officials in some cases causing further distress to the complainants.

6.3. Political Manipulation

Successive democratic regimes over the past decade have involved FIA in high profile cases of political opponents which has tarnished FIA's image as an independent law enforcement agency. Islamabad High Court has repeatedly admonished FIA for frivolous summons on flimsy accusations based on online speech. The Section 20 of PECA, 2016 has particularly become infamous for its invocation by FIA for alleged defamation by politicians, journalists and civil society representatives (Naseer, 2022). Most of these enquiries have been quashed by the courts after being termed as fabricated with mala fide intent.

6.4. Lack of Capacity

Serious questions have been raised on the existing capacity of FIA to effectively handle cybercrimes. FIA's lack of investigative skills and faulty case preparation has repeatedly come under the spotlight because of low conviction rate in cybercrimes. The investigation and case preparation is often delayed frustrating the court, adding to the duress of the complainants and earning a bad name for FIA (Kamran, 2021).

6.5. Lack of International Cooperation

FIA is still to develop institutional capacity to effectively solicit the cooperation of social media and cyber technology platforms in cybercrime cases. Legal instruments like Mutual Legal Assistance Treaty (MLAT) with United States, Convention on Cybercrime (Budapest Convention), OECD's Model Reporting Rules for Digital Platforms can enable FIA and other agencies of Pakistan to secure valuable record from international data centers and expeditiously tackle cybercrimes. By signing these legal instruments Pakistan can convince social media companies that their data will not be used to curb freedom of speech and right to privacy.

7. Comparative analysis of India's cybercrime legislation

India is an emerging giant in the field of Information Technology with IT related exports with IT exports worth 149.1 billion U.S. billion dollars (Sun, 2022). The development of cyber technologies and digitization has provided a much-needed impetus to India's economy (Maiti & Kayal, 2017). Indian government is cognizant of that fact in spite of all the recent progress, the digital literacy in India is just 6.5% and the internet penetration is 20.83 per 100 people. Enhancing digital literacy with the help of high mobile and internet

penetration can stimulate robust socioeconomic activity and propel the country in the league of developed countries (Chakraborty & Biswas, 2019). The question of cyber security has propped up inevitably as a natural outcome of the incessant digitization and Indian digital ecosystem is striving hard to cope with the issue of cybersecurity (Garg et al., 2021).

7.1. Cybercrime legislation and enforcement in India

Taking its inspiration from the United Nations Model Law on Electronic Commerce (UNCITRAL), 1996, the Indian Parliament enacted the Information Technology Act, 2000. This law was intended to deal with the digital crimes or cybercrimes and electronic commerce (Jain & Gupta, 2020). However, along with all the positive indicators of digitization, the menace of cybercrimes continued on an upward trajectory in India threatening to undo socioeconomic dividend of digitization (Karali et al., 2015). Like other developing countries, India also struggled with accurate reporting and registration of cybercrimes during the initial years of digitization boom. By 2010 estimates of reported cybercrimes were at 10% and about 2 % were actually registered. The conviction rate was estimated at as low as 2% (Karali et al., 2015). The phenomenon of highly skilled and IT literate people committing cybercrimes has also been termed as "destructive entrepreneurship" (Kshetri, 2016). Baumol (1990) as cited by Kshetri (2016) has propounded the theory that destructive entrepreneurs emerge as consequence of the inequitable payoffs offered for productive skills by developing economies. Low literacy levels, high unemployment, large informal sector and exploitative labour market are some characteristics of developing economies associated with the rise in cybercrimes in India.

In addition to other weaknesses of the enforcement mechanism, India's judicial system lacked the necessary paraphernalia to properly adjudicate the cybercrimes. Cyber appellate tribunal of India established in 2006 did not adjudicate a single case from 2011 to 2014 due to non-availability of the chairperson and judicial members. Moreover, the general approach and attitude of the police department towards cybercrimes was persistently observed to be nonprofessional and nonscientific. Victims often alleged that police followed routine and archaic investigation procedures which were completely useless in cybercrime cases and inevitably led to low conviction rate of cybercriminals (Kshetri, 2016). To overcome the deficiencies of Information Technology Act, 2000; the law was amended on 23rd December, 2008, renaming the Act as the Information Technology (Amendment) Act, 2008 and was referred to as ITAA, 2008. This act added eight new offences in the list of cybercrimes including voyeurism, child pornography, receiving stolen information, identity theft, cyber stalking, sharing sexually explicit content,

phishing and cyber terrorism (Kapila, n.d).

Apart from the above-mentioned Sections under ITAA, 2008, *Cybercrime cells* were set up in states for reporting and investigation of Cybercrime cases. The Government under the IT Act, 2000 set up *Cyber Forensic and Training Labs* in states of Kerala, Assam, Mumbai, Mizoram, Manipur, Nagaland, Arunachal Pradesh, etc., for awareness creation and training against Cybercrimes. Various programs were conducted by the Government of India to generate awareness about Cybercrimes for Judicial officers and Police officers (Kapila, n.d). "In 2015, in a watershed moment for free speech online, the Indian Supreme Court struck down section 66-A of the Information Technology Act 2000 on the grounds of violation of freedom of speech, guaranteed under Article 19(1)(a) of the Constitution of India. It was held that the section did not meet the criterion of 'reasonable restriction'" (Nazneen, 2020)

Despite the above mentioned reforms, in recent years there has been an astronomical increase in cybercrime cases in India. India reported 0.2 million cases in 2018; 0.39 million cases in 2019; 1.15 million cases in 2020; 1.44 million cases in 2021; and 0.2 million incidents in the first two months of 2022 (Basu, 2022). The seven times increase from 2018 to 2021 reflects the enormous magnitude of the problem and the data of first two months of 2022 indicates an unrelenting epidemic of cybercrimes (Bhalerao, 2022). Financial fraud has been identified as the major motive for cybercrimes and accounted for 30,142 out of the total 50,035 cases (60.02 per cent). This was followed by sexual exploitation (6.6 per cent) and extortion 4.9 per cent (Basu, 2022; Bhalerao, 2022). As the cybercrimes are being committed unabated, Indian Government has recently announced some new initiatives for curbing cybercrimes with special focus on capacity building in fields of information security and mass awareness campaign for cybersecurity (Basu, 2022; Bhalerao, 2022). Indian government has recently launched a twitter handle "Cyber dost" to share videos and tutorials on how to avoid cyber fraud (India.com, 2022). "States/Union Territories (UTs) have set up 169 cyber police stations across the country to combat ever rising cybercrimes in the country as per a latest report titled 'Data on Police Organizations for 2020' released by the Bureau of Police Research and Development (BPR&D)" (Siddiqui, 2022). It can be deduced from the preceding analysis that India is struggling to control the menace of cybercrimes despite introducing several legal and administrative reforms over the past decade. In realization of this reality, Indian government is putting emphasis on education and awareness of the masses which may turn out to be the only sustainable solution to stopping cybercrimes in the long run.

8. Discussion on Qualitative Thematic Analysis of Semi-structured Interviews

After the organization of codes and subcodes derived from the interview transcripts (Annex – I to V), the next step was combining different related codes to develop themes for analysis (Annex – VI). The determination of logical connectivity of ideas eventually led to the combining of the codes of "Empowerment", "Cybercrimes" and "Weak Enforcement" under the theme of "Dialectical Relationship of Empowerment and Cybercrimes". The rationale of the theme is established from the literature review and from analysis of the interview transcripts. From a researcher's point of view, it is fascinating to observe that the digitalization and AI revolution (also dubbed as 4th Industrial revolution) has globally triggered positive and negative forces of almost equal quantum i.e., digital empowerment and cybercrimes respectively. This dialectical equation is likely be a relevant theme of research in near future, considering the seemingly irreversible extension of digital technologies in modern societies. Respondents in this research pointed out that digitalization is a double-edged sword as on the one hand it empowers the citizens to voice their opinions without any fear or restrictions, however, digitalization is also providing a relatively less risky and convenient means of criminal activities. These views resonate well with the findings of literature review which categorically establishes a global epidemic of cybercrimes. Respondents also asserted that the new found empowerment is manifesting itself in development of bipolar personalities where people suddenly become aggressive or antisocial while hiding behind a mobile phone or a laptop. Covid-19 has further exacerbated this trend as isolation period of pandemic has led to internalization of the habits of online interactions, shopping and commercial transactions. This online and digital mode of life is providing opportunities to deviant and criminal minds to commit cybercrimes. In Pakistan's context situation is further complicated by weak enforcement capacity of state agencies. Participants of this research were clear in their opinions about grave deficiencies of FIA and PTA in regulating cyberspace effectively. The poverty of resources and capacity afflicting FIA is an open invitation to cybercriminals. It is also a sad reflection on FIA that despite repeated requests by this researcher only 2 of the 5 FIA officers agreed to respond to the interview questions.

The second theme emerging from the coding analysis is the "Polarization between government and civil society on cyberlaws". This theme is derived by combining the codes "Weakness of cyberlaws", "State policy" and "Remedial measures". Participants echoed the misgivings and frustrations of civil society reverberating in Pakistan since the enactment of PECA, 2016. Respondents strongly asserted that state's cyber policies are security centric and completely

insulated from the concerns of civil society. The interviewees were also deeply concerned about the deepening digital divide in the country as a consequence of apathy of state agencies and security centric policies. It emerged from the interview responses that the sharp polarization between the state and civil society germinates from the clandestine nature of PECA's enactment. There was an overwhelming rebuttal by the respondents of any notion of consultation on PECA claimed by the government. The subsequent victimization and targeting of specific individuals under PECA, 2016 by successive governments have categorically established malicious intentions behind the law, claimed the respondents from the civil society. Regarding improving the efficacy of PECA, 2016, participants vociferously supported a fundamental change in the policy direction of the federal government so that the equitable protection of digital rights of the masses is ensured and criticism of state institutions is not construed as a threat to national integrity.

9. Conclusion

PECA, 2016 will go down in Pakistan's legislative history as one of the most controversial and maligned pieces of legislation. The stigma associated with the law has been compounded by the recent sorry saga regarding PECA Amendment Ordinance eventually struck down by Islamabad High Court. Given this context, it is quite natural that any research on PECA, 2016 may start with a slight bias against the impugned law. However, to guard against any such bias, this research setout to explore two fundamental questions before analyzing the efficacy of PECA, 2016. The first question about the impact of digitalization on socioeconomic empowerment in Pakistan needed to be answered to determine the context in which PECA, 2016 is being operationalized. This research found that Pakistan's socioeconomic systems have been profoundly impacted by the forces of change unleashed by digitalization, e-governance, e-commerce, social media and other IT applications. The idea of freedom of speech previously relegated to books of constitutional law has now been weaponized for all and sundry through the unshackled and unregulated cyber technologies. Having determined this much, the second fundamental question confronting this research was the proliferation of cybercrimes in Pakistan and the apparent absence of this disturbing fact from the narrative of civil society against PECA, 2016. Subsequently, this research revealed that the cybercrime epidemic in Pakistan is apparently linked to the overarching systemic malaises such as illiteracy, cultural degradation, intolerance, political & religious polarization, unemployment, Covid-19 induced factors, neglect of FIA and other civilian LEAs. This diverse range of drivers of cybercrimes has convinced the detractors of PECA, 2016 that curbing cybercrimes is far beyond the scope of a law riddled

with definitional ambiguities, procedural intricacies and drafting gaffes. The research proceeded further with the critical analysis of PECA, 2016 with the help of both secondary and primary data and it was concluded that PECA's genesis remains deeply mired in controversy. Civil society and independent experts are adamant in their stance that last minute clandestine changes were made to the draft bill of PECA, 2016 ensuring its present draconian nature. The indiscriminate crackdown on political dissenters and rights activists in the immediate aftermath of the PECA's enactment seems to substantiate the allegations on the intent of the law. Moreover, the section-by-section analysis of the law reveals gaping holes in the drafting left either deliberately or unwittingly giving sweeping powers to PTA and FIA to interpret and enforce the law. PTA's powers to define objectionable material liable to be censored and FIA's powers to access and confiscate any data on the suspicion of being linked to a cybercrime are some of the grey areas giving PECA its present low standing. The most damning indictment of PECA, 2016 comes from undeniable statistics about the unmitigated escalation of cybercrimes, unabated arbitrary actions of FIA being persistently thrashed by judiciary and unbridgeable digital divide in certain areas of the country nullifying the tall claims associated with enactment of PECA, 2016. The comparison with the cyber law regime of India reveals that India is also in an unenviable position with respect to the magnitude of cybercrimes and protection of online freedoms. However, India's online security protocols and enforcement capacity are gradually evolving and therein lie some of the lessons replicable in Pakistan. It is also noticeable that Indian academicians have secured worldwide acclaim for theory development on cybercrimes which is likely to contribute to the effective legal and policy measures against cybercrimes. It can be safely concluded that PECA's transformation into an effective legal instrument will have to be preceded by paradigm shifts in state's approach towards digital rights and online freedoms. This is likely to bridge the much-needed trust deficit between the state and civil society and create grounds for the wide-ranging socioeconomic reforms needed to curb cybercrimes.

10. Recommendations

10.1. Short term

1. **Consultations with Stakeholders**: Government should immediately start consultation sessions with all the stakeholders regarding the contentious issues of PECA, 2016. This is a low-hanging fruit because minimal finances will be involved and dividends will be immediate in terms of positive feedback from civil society and media.

Responsibility: The concerned Standing Committee of National Assembly can be assigned this responsibility of meaningfully engaging with all the stakeholders of IT industry with a special focus on ensuring the transparency of dialogues. This will create an atmosphere of trust and optimism and provide government with expert insight on the required corrections and amendments in PECA, 2016.

2. **Mass Awareness Campaign:** A recurring finding of this research was the lack of mass awareness about cybercrimes and its legal regime in Pakistan. Prompt and effective actions in this regard are possible considering the existing training resources available in public and private sector of Pakistan which can be mobilized immediately with minimal any financial implications.

Responsibility: Ministry of Information & Broadcasting has a Cyber wing and its own training academy which can design and launch a media campaign across all broadcasting platforms but specially on social media applications to apprise the masses about the rapidly evolving nature of cybercrimes. Further collaboration with PTA and commercial banks can be initiated about how best to sensitize the masses as these organizations are already engaged with their customers through text messages about different threats posed by cybercriminals.

3. **Capacity building of FIA and PTA**: FIA and PTA are the face of government when it comes to enforcement of PECA, 2016 and their immediate capacity building is required to understand the shortcomings of the existing cyber law, exercise prudence while implementing it and hence, drastically improve the enforcement of PECA, 2016.

Responsibility: There are several independent thinktanks and digital rights organizations in Pakistan who can be approached to develop partnerships with FIA and PTA regarding mutual capacity building sessions. These collaborations can serve multiple purposes of trust building, sensitivity training and a hotline of timely communication.

10.2. Medium to Long-term

1. **Research on Cybercrimes**: Government needs to encourage academicians, researchers and universities to proactively carry out research on cybercrimes which can add value to legislative and policy discussions. The Space Transition Theory of Jaishankar (2008) should serve as an inspiration to Pakistani researchers.

2. **Shift in Policy Paradigm**: The ineffectiveness and misuse of PECA, 2016

has been invariable associated with the security-centered policy orientation of the state. The backlash received by state actions under PECA, 2016 from the civil society and judiciary should be an eyeopener for the state institutions. In medium to long-term state may gradually shift its policy paradigm from security centric to citizen – centric. This is a doable target considering that "Digital Pakistan" policy and the e-commerce policy of 2019 are already in the field promising a variety of digital rights to the citizenry. The concerned agencies need to evolve a robust coordination mechanism so that PECA, 2016 is not used to nullify the intended objectives of the above cited policies.

Responsibility: Transforming a decades old policy narrative may prove to be a herculean task, however, with the collective will and actions of the parliament and security establishment a gradual process of transformation can be initiated.

3. **Bridging the Digital Divide**: It is imperative that no segment of Pakistan's population be deprived of their digital rights on any genuine or false pretense. Currently just above 30% population of Pakistan has access to Internet and if the internet coverage is not expanded quickly then a large population will remain vulnerable to cybercrimes.

4. **Amendments in PECA, 2016**: Extensive evidence is now available from the enforcement of a flawed law that certain basic amendments to PECA, 2016 are urgently required. These amendments must be aimed at safeguarding the dignity and privacy of people against any whimsical, arbitrary or mala fide action. Adequate privacy protection provisions are needed to be introduced to the law in addition to the clear definition of "reasonably required" in case of confiscation of data for investigation by FIA.

5. **Utilization of IT Incubators**: The IT incubators setup in the country under Digital Pakistan policy can be given research projects to design security protocols for government websites and social media applications.

11. References

Abbasi, K. (2021, August 28). Cybercrime increases by 83PC in three years. thenews. Retrieved July 15, 2022, from https://www.thenews.com.pk/print/884453-cybercrime-increases-by-83pc-in-three-years

Abbas, Z., Khan, R., Khan, M. Z., & Imran, M. (2023). Cyber Laws and Media Censorship in Pakistan: An Investigation of Governmental Tactics to Curtail Freedom of Expression and Right to Privacy. *Journal of Creative Communications*, 09732586231206913.

Akhlaq, M. (2021). CYBERCRIME IN PAKISTAN: A STUDY OF THE LAW DEALING WITH CYBERCRIMES IN PAKISTAN.

Aleem, Y., Asif, M., & Ashraf, M. U. (2021). The Prevention of Electronic Crimes Act 2016 And Shrinking Space for Online Expression in Pakistan. *Ilkogretim Online*, *20*(2).

Anjum, U. (2020). Cyber crime in Pakistan; detection and punishment mechanism. *Časopis o društvenom i tehnološkom razvoju*, *2*(2).

Anzak, S., & Sultana, A. (2020). Social and economic empowerment of women in the age of digital literacy: A case study of Pakistan, Islamabad, Rawalpindi. *Global Social Sciences Review*, *1*, 102-111.

Arshad Khan, E. (2018). The Prevention of Electronic Crimes Act 2016: An Analysis. *LUMS LJ*, *5*, 117.

Assarut, N., Bunaramrueang, P., & Kowpatanakit, P. (2019). Clustering Cyberspace Population and the tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory. *International Journal of Cyber Criminology*, *13*(1).

Batool, S., Gill, S. A., Javaid, S., & Khan, A. J. (2021). Good Governance via E-Governance: Moving towards Digitalization for a Digital Economy. *Review of Applied Management and Social Sciences*, *4*(4), 823-836.

Dad, N., & Chaudhri, A. (2017). Pakistan's Blasphemy Law: Using Hate Speech Laws to Limit Rights Online and Offline. *Harmful Speech Online*, 21.

Flor, R. (2012). Perspective for New Types of Technologica Investigation and Protection of Fundamental Rights in the Era of Internet the So-Called Cyberterrorism as a Prime Example, Between Problems of Definition and the Fight Against Terrorism and Cybercrime. *Perspective for New Types of Technologica Investigation and Protection of Fundamental Rights in the Era of Internet the So-Called Cyberterrorism as a Prime Example, Between Problems of Definition and the Fight Against Terrorism and Cybercrime*, 51-76.

Garg, A., Popli, R., & Sarao, B. (2021). Growth of digitization and its impact on big data analytics. IOP Conference Series: Materials Science and Engineering,

Hameed, I., & Naqvi, S. A. A. (2021). An Analysis of the factors affecting Cybercrime against individuals in Pakistan. 2021 15th International Conference on Open Source Systems and Technologies (ICOSST),

Haq, U., & Atta, Q. (2019). Cyber Security and Analysis of Cyber-Crime Laws

to Restrict Cyber Crime in Pakistan. *International Journal of Computer Network & Information Security*, *11*(1).

Holt, T. J., Fitzgerald, S., Bossler, A. M., Chee, G., & Ng, E. (2016). Assessing the risk factors of cyber and mobile phone bullying victimization in a nationally representative sample of Singapore youth. *International journal of offender therapy and comparative criminology*, *60*(5), 598-615.

Iftikhar, I., Sultana, I., & Paracha, S. A. (2024). Balancing Act: Pakistan's Quest for Responsible Social Media Regulation. *PAKISTAN JOURNAL OF LAW, ANALYSIS AND WISDOM*, *3*(2), 216-231.

Jain, A., & Gupta, N. (2020). Cyber crime. *National Journal of Cyber Security Law*, *2*(2), 152-158.

Karali, Y., Panda, S., & Panda, C. (2015). Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. *International Journal of Engineering and Management Research Page Number,(5)*, 43-48.

Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes. *American journal of criminal justice*, *43*(2), 141-157.

Khan, A., Mubarik, M. S., & Naghavi, N. (2021). What matters for financial inclusions? Evidence from emerging economy. *International Journal of Finance & Economics*.

Khan, E. A. (2018). The Prevention of Electronic Crimes Act 2016: An Analysis. *LUMS Journal of Lan.* Retrieved from https://sahsol.lums.edu.pk/law-journal/pre-vention-electronic-crimes-act-2016-analysis.

Khan, S., & Tehrani, P. M. (2018). Cyber Law and Practice of Freedom of Speech on Internet: Pakistan Perspective. *The Journal of Social Sciences Research*, 519-530: 512.

Khan, S., Tehrani, P. M., & Iftikhar, M. (2019). Impact of PECA-2016 Provisions on Freedom of Speech: A Case of Pakistan. *Journal of Management Info*, *6*(2), 7-11.

Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, *66*(3), 313-338.

Leghari, M. A., Wasiq, M. F., Younes, J., & Hassan, B. (2024). Global Legislation Muzzling Freedom of Speech in the Guise of Cyber Security. In *Cybersecurity and Artificial Intelligence: Transformational Strategies and*

Disruptive Innovation (pp. 263-279). Springer.

Liaquat, S., Qaisrani, A., & Khokhar, E. N. (2016). Freedom of Expression in Pakistan: A myth or a reality.

MacDermott, Á., Baker, T., Buck, P., Iqbal, F., & Shi, Q. (2020). The Internet of Things: Challenges and considerations for cybercrime investigations and digital forensics. *International Journal of Digital Crime and Forensics (IJDCF)*, *12*(1), 1-13.

Maiti, M., & Kayal, P. (2017). Digitization: Its impact on economic development & trade. *Asian Economic and Financial Review*, *7*(6), 541-549.

Najib, A., Umar, U., Bhakti, A., Fatikasari, P., & Zawawi, A. N. K. B. (2024). Regulation on Freedom of Expression on Social Media in Indonesia and Malaysia. *Journal of Indonesian Constitutional Law*, *1*(1), 46-60.

Naudé, W. (2024). Destructive digital entrepreneurship. In *Handbook of Research on Entrepreneurship and Conflict* (pp. 292-328). Edward Elgar Publishing.

Ndubueze, P. N. (2021). History, Evolution and Challenges of Cyber Criminological Scholarship. *International Journal of Cyber Criminology*, *15*(1), 65-78.

Rafiq, A. (2019). Challenges of securitising cyberspace in Pakistan. *Strategic Studies*, *39*(1), 90-101.

Rakha, N. A. (2023). Cyber Law: Safeguarding Digital Spaces in Uzbekistan. *International Journal of Cyber Law*, *1*(5).

Rubsamen, B. M. (2023). A Fake Future: The Threat of Foreign Disinformation on the US and its Allies. *Global Tides*, *17*(1), 8.

Runa, S. J. (2019). The Challenges of Freedom of Expression and the Digital Security Act 2018. *BiLD Law Journal*, *4*(2), 75-92.

Saleem, M. S., Malhooz, F., & Fatima, T. (2023). From Cyber-crimes to Cyber-Security: Exploring Legal Minefield of Artificial Intelligence in Pakistan. *Pakistan Research Journal of Social Sciences*, *2*(3).

Singh, A. R. (2023). The Evolution of Metaverse and Cyberspace Regulation Vis-A-Vis Indian and International Legal Issues. *ILE Multidisciplinary Journal*, *I*(I), 39-46. Iledu.in

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

Yongmei, C., & Afzal, J. (2023). Impact of enactment of 'the prevention of

electronic crimes act, 2016'as legal support in Pakistan. *Academy of Education and Social Sciences Review*, *3*(2), 203-212.

Young, J. M. (2004). Surfing while Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation-A Critical Analysis of the Council of Europe Convention on Cybercrime and the Canadian L Lawful Access Proposal. *Yale JL & Tech.*, *7*, 346.

Yusuf, H., Dragomir, M., Thompson, M., Watts, G., Chan, Y.-Y., & Nissen, C. S. (2013). *Mapping digital media: Pakistan*. Open Society Foundations.

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.

Annexure - I

Open coding from responses to Question 2: How and why incidence of cybercrimes is increasing in Pakistan?

- Financial frauds, harassments, fake profiles, defamation and hacking are the fastest growing cybercrimes in Pakistan
- Proliferation of social media apps
- Lack of prosecution and punishment
- Weaknesses of online security protocols on government websites
- Lack of education
- Deterioration of culture and values
- Weak law enforcement capacity
- Lack of education
- Deterioration of social, moral and cultural values
- Professional trolls
- Smear campaigns
- Lack of regulation
- Irresponsible use
- Social intolerance
- Manipulation of religious and political groups
- Social acceptance of violence
- Dating culture on social media
- Blackmailing
- FIA is poorly resourced

Annexure – II

Open Coding from responses to Question 1: What is the Impact of digitalization on empowerment and freedom of speech?

- Access to information
- Media as a pressure group
- Fight for media ratings
- Media misusing freedom of speech
- Culture of abuse, violence and immoral values
- Financial influence on media
- Political influence on media
- Media's exploitation by different pressure groups
- Ambiguity in constitutional provision on freedom of speech
- Awareness about freedom of expression
- Risks and costs of empowerment
- Empowerment and hate speech
- Public platform to raise "voice"
- Importance of education
- Clash of uneducated titans
- Regulation can lead to true empowerment
- Covid 19 and expanding digitalization
- Social media and enhanced freedom of speech
- Control and garb of national security
- Definition of "reasonable restrictions" is problematic
- Arbitrary rules and regulations
- Lack of citizen centric approach
- Inequitable access to internet
- Regulations and qualified freedoms
- Protection of fundamental rights
- Shrinking social and digital space
- Cyber armies
- Security cantered policies
- Knee jerk reactions of authorities
- friction with civil society
- lack of education
- attitude when sitting behind screens
- Service delivery is being increasing linked internet
- Pakistan is regressing in terms of freedom of expression
- dictatorship of information
- hate speech and blasphemy

Annexure - III

Open coding from response to Question 3: Why PECA, 2016 has been subjected to so much criticism and controversy?

- Criminalization of government's criticism
- Disconnect with civil society and stakeholders
- Violation of fundamental rights
- Ambiguity of "reasonability" of restrictions
- Dormant courts
- Targeting of specific people
- Suppression of voices
- Control of narratives
- Clandestine drafting of law
- Lack of data protection provisions
- Arbitrary powers of FIA
- Suppression of opposition
- Control the voice
- Sweeping powers to government agencies
- Curtailing political dissent
- Lack of protections in PECA
- Assault on online discourse
- Deepening of digital divide
- Lack of consultation with civil society
- Digital rights considered a security risk
- Operational space to ISI
- Draconian law

Annexure-IV

Open Coding from responses to Question 4: How can Pakistan learn from the best practices of India to improve PECA, 2016?

- Spread awareness
- Capacity building/training of LEAs and Judiciary
- Cyber forensic facilities
- Cyber crime coordination centre
- National Critical Information Infrastructure Protection Centre (NCIIPC
- Botnet Cleaning and Malware Analysis Centre
- Chief Information Security Officers (CISOs
- audit of the government websites and applications
- cyber security mock drills
- India should not be an example for Pakistan
- India is violating digital rights of minorities

Annexure-V

Open coding from responses to Question 5: How can the controversy and irritants in implementation of PECA, 2016 be removed?

- Consultation with parliamentarians
- Public survey on PECA
- Promulgation of Data Protection Law
- Regular consultative process with stake holders
- Change of policy formulation approach
- Curtailment of excessive powers to government agencies
- Accountability of leas
- Education of masses
- Training of leas
- Change of security centric approach
- Protection of privacy
- Change of policies

Annexure -VI

Code	**Empowerment**					
Subcodes	Having access to information	Covid 19 and expanding digitalization	Public "Voice" platform	Social media and enhanced freedom of speech	Service delivery and internet	Fundamental rights

Annexure -VII

Code	**Cybercrime**					
Subcodes	Culture of abuse	Misuse of freedom of speech	Exploitation of pressure groups	Risks & costs of empowerment	Empowerment and hate speech	Clash of uneducated titans
	Attitude behind screens	Hate speech & blasphemy	Cyber armies	Professional trolls	Irresponsible use of social media	Online Dating culture & blackmailing

Annexure -VIII

Code	**Weak enforcement**				
Subcodes	Lack of prosecution & convictions	Weakness of cybersecurity protocols	Lack of capacity of concerned agencies	Lack of resources with FIA	Arbitrary powers of FIA

Annexure-IX

Code	**State policy**				
Subcodes	Control in the garb of national security	Lack of citizen centric approach	Inequitable access to internet	Shrinking social and digital space	Security centered policies
	Knee jerk	Regressing	Dictatorshi	Criminalizatio	Disconnec

Code	State policy				
	reactions of state agencies	freedoms	p of information	n of government's criticism	t with civil society
	Suppressio n of opposition	Controllin g the "voice"	Targeting of specific individuals	Deepening digital divide	Digital rights as security risks

Annexure-X

Code	Weakness of Cyber Law in Pakistan				
Subcodes	Ambiguity in Constitution regarding "reasonable restrictions"	Arbitrary rules and regulations	Definition of "reasonable restrictions"	Sweeping powers to government agencies	Clandestine drafting of PECA, 2016
	Lack of data protection provisions in PECA, 2016	Disconnect with civil society			

Annexure-XI

Code	Remedial Measures				
Subcode s	Citizen centric approach to policy making	Public survey of PECA, 2016	Promulgatio n of Data Protection laws	Regular consultative process with stakeholders	Change of policy formulatio n approach
	Curtailme nt of excessive powers to governme nt agencies	Accountabili ty of LEAs	Education and awareness of masses	Capacity building of LEAs/agenci es	Curtailme nt of excessive powers of agencies