



The Prevention of Electronic Crimes Act, 2016: Balancing Cybercrime Control and Freedom of Online Expression in Pakistan

Muhammad Tauheed Ahmad¹, Rao Imran Habib²

¹ L.L.B. Graduate, Faculty of Law, The Islamia University of Bahawalpur, Pakistan. Email: mrtauheeed@gmail.com

² Dean, Faculty of Law, The Islamia University of Bahawalpur, Pakistan. Email: imran.habib@iub.edu.pk

ARTICLE INFO

Article History:

Received: February 28, 2026

Revised: March 28, 2026

Accepted: March 29, 2026

Available Online: March 30, 2026

Keywords:

PECA 2016

Freedom of Expression

Digital Rights

Cyber Security

Fundamental Rights

Political Dissent

Doctrinal Legal Research

Funding:

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

To properly manage the burgeoning digital world and cybercrime activities, the Prevention of Electronic Crimes Act, 2016 (PECA) was enacted in Pakistan. Its primary role was to address serious online offences like cyber harassment, hacking, identity theft, online fraud, hate speech and the misuse of electronic communication. A law like this was needed to safeguard citizens and ensure order in the online world, especially in a nation where the internet is growing in significance. But the use of PECA has caused deep concern particularly in terms of freedom of expression. While the law was intended to protect from real cybercrime, many of its provisions are deemed to be too vague, too broad and lacking in clear boundaries. Given this uncertainty, PECA has been criticized in many cases to be applied to journalists, media personnel, political activists, and people voicing opposing views. This can create the danger that legislation designed to protect becomes a means of abridging free expression and stifling criticism. This paper looks at PECA through the lens of the law and reviews the interpretation and application of PECA in Pakistan. It also explores the attitude of judiciary and underlines the lack of consistency in protection of fundamental rights especially the right to freedom of speech provided under the Constitution of Pakistan. The study also investigates if PECA has instilled fear in citizens to voice their opinions online. It is conducted by doctrinal legal research, which involves careful attention paid to the statute, cases, judicial rulings and scholarly writing. It aims to understand its impact on the internet in Pakistan, and to assess if the law has a good balance between cyber security and constitutional freedoms. The paper ends by suggesting for legal changes to clarify PECA and provide fairer and better protection under the Law.

© 2026 The Authors, Published by iRASD. This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License

Corresponding Author's Email: mrtauheeed@gmail.com

1. Introduction

1. Legal Framework of PECA 2016

The legal framework under PECA offers a robust legal framework to govern various cyber activities such as unauthorized access, cyber stalking, misuse of identity, electronic fraud and hate

speech on the internet, to ensure a safe cyber environment for users (PECA, 2016). It provides a framework for regulating, monitoring, investigating and prosecuting cyber crimes, which is a reflection of the growing demand for legal regulation in the digital era. It places important roles on regulatory bodies like the Federal Investigation Agency (FIA) and the Pakistan Telecommunication Authority (PTA), which are responsible for enforcement, monitoring of online content, and implementation of national cyber legislation (PTA, 2021). It also aims to strike a balance between freedom and control in cyberspace. However, it is argued that Section 37 of the Act provides too much discretion to authorities, which could result in over-censorship, curbing of freedom of speech, and abuse of power (HRCP, 2018). It also poses important issues concerning how cyber law is understood under the Constitution, especially in the context of the fundamental rights such as freedom of speech, privacy etc.

The Prevention of Electronic Crimes Act, 2016 (PECA) is a comprehensive legislation to prevent, investigate and prosecute the electronic crimes in Pakistan. It defines specifically as offences (criminal offences) the following acts: unauthorized access to information systems, cyber stalking, online harassment, electronic fraud, and dissemination of unlawful information on the Internet. Federal Investigation Agency (FIA) is mainly responsible to implement PECA and Pakistan Telecommunication Authority (PTA) is the regulatory body under the PECA. The Human Rights Commission of Pakistan (HRCP) has though expressed concerns that the new Section 37 can allow for undue limitations on online expression. This paragraph also discusses comparative analysis, doctrinal reasoning and statutory interpretation (Rehman, 2019, Khan, 2020). The main monitoring and policing institutions that assist to implement and enforce this framework are key regulatory institutions like National Cyber Crimes Investigation Agency (NCCIA) and Pakistan Telecommunication Authority (PTA) which have a vital role in monitoring and controlling digital spaces (PTA, 2021). However, the law has been criticized, especially in respect of the provisions in section 37 that has been said to give excessive powers of censorship to the authorities, where in concerns freedom of expression (HRCP, 2018). In addition, the interpretation of PECA law is an interpretative analysis, comparative legal evaluation and doctrinal reasoning based on the principles of legal research as taught in the law school (A. Khan, 2020; S. Rehman, 2019).

1.1. Unauthorized Access and the Scope of State Regulation

The Act includes provisions as to Section 7 that make it illegal to gentile into computer systems and secure computer infrastructure. However, there is the need to distinguish between intentional and unintentional access (Ali, 2021). Proportionality in enforcement is stressed by the courts. Legal interpretation, comparison and doctrinal reasoning can also be expanded upon in this paragraph, following academic standards (A. Khan, 2020; T. Rehman, 2019). Section 7 of the Prevention of Electronic Crimes Act 2016 (PECA) makes it illegal to use any computer system or other computer-related data without authorization or to gain unauthorized access to any computer system or other computer-related property, and makes it the duty of the government and consumers to protect and secure critical national electronic systems, electronic devices, and other computer-related property from cyber attacks, hacking and other compromise or intrusion in or into computer systems. The paper demonstrates the need to have more explicit protection and accountability mechanisms in digital rights by comparing international standards in this field. The increased importance of cyber security in an increasingly digitized world where government and private organizations are increasingly heavily dependent on electronic communication, electronic storage and electronic information processing. In this context, the law is not only a remedial but also a preventative measure to protect computer systems from misuse, abuse and other malicious interference. Critically, the law differentiates between intentional and unintentional access to computers and the Internet in committing a cyber offence, thereby offering a welcome protection against unwarranted criminalization and inaction without the element of intent (Ali, 2021). This is especially important in intricate technological environments where access to systems can happen through technical glitches, inadvertence or even unintentional interaction with protected systems.

Moreover, courts have consistently stressed the need for proportionality in the implementation of cyber laws, ensuring that the punishment imposed under cyber crime provisions is fair, reasonable and commensurate with the gravity of the offence. This approach from the judiciary helps strike a balance between rigorous cyber law enforcement and respect for human rights,

particularly in cases of minor and non-malicious offences. It also demonstrates an attempt to avoid over-enforcement of penalties which could have a chilling effect on legitimate online activity and innovation. Further, this section is analyzed in a wider academic and legal debate that encompasses law interpretation, comparative law, and doctrinal approaches to law. This understanding is crucial to appreciate the regulatory approaches to comparable cyber offences in other countries, trends in international cyber law, and national law's compatibility with international cyber security norms. Finally, this section underlines the interaction between technological innovation and legal perspectives, and the importance of a fair, reasonable and dynamic legal framework in the digital era (A. Khan, 2020; T. Rehman, 2019). Section 7 prohibits unauthorized access to systems and safeguards digital infrastructure. Nevertheless, it is essential to make a distinction between intentional and unintentional access (Ali, 2021). Proportionality in enforcement is stressed by courts. In this paragraph, the interpretation of the law, comparative analysis, and reasoning based on the doctrine are further elaborated according to academic standards (A. Khan, 2020; T. Rehman, 2019). Section 7 makes it a crime to access an information system or data without proper permission. This is to ensure confidentiality, integrity and security of the digital system and to prevent unauthorized intrusion. It thus offers legal protection for the digital infrastructure, such as judicial information systems, from illegal access. But there must still be a difference between intentional and unintentional access so as to have proportionate enforcement (Ali, 2021).

1.2. Cyber Stalking: Protection of Privacy versus Misuse of Law

Section 21 of the concerned law gives protection to harassment, especially to women and tries to guarantee the security of people both online and in social spheres. In terms of doctrine, the provision needs to be read with a keen eye of legal interpretation, whereas comparative legal analysis shows the existence of comparable protection systems in other jurisdictions that underline more effective implementation systems. Nevertheless, it mainly relies on a strong and effective institutional response, which is also a crucial problem in enforcement (Ahmed, 2020). The scholarly literature also confirms that the lack of enforcement undermines the effectiveness of such provisions, thus restricting the access to effective remedies (Khan, 2021; S. Rehman, 2019). To this end, there is high normative intent in Section 21, albeit the effectiveness of its operation depends on institutional capacity, procedural effectiveness, and legal uniformity.

1.3. Data Protection and Digital Security Concerns

The problem of the misuse and unauthorized treatment of personal information is considered in the section 8 of the corresponding law, and it is important to note that the problem of data protection in Pakistan on the Internet is becoming more and more topical. Without extensive and autonomous laws on data protection, the nation continues to be highly dependent on the conditions of the PECA framework to govern such issues (Digital Rights Foundation, 2022). This legal loophole leaves a significant gap when it comes to ensuring enough security of personal data, and adherence to privacy rights. On the doctrinal side Section 8 needs special attention to the law in the context of the constitutional protection of privacy, while comparative law has developed data protection provisions in the majority of jurisdictions to address issues like these. From the scholarly literature, it is also recommended that with the absence of the comprehensive data governance framework in the absence of the cybercrime law, there would be limited number of protections available for individuals to gain from (A. Khan, 2020; S. Rehman, 2019). In that sense it will be a vital but in many ways incomplete law to address the new challenge of misuse of personal data.

1.4. Hate Speech Regulation and Its Impact on Online Expression

The Internet courted hate speech in section 11 is prohibited by the relevant legislation, which unfortunately is not clear and specific enough in terms of definitions of such hateful speech, causing ambiguity to its implementation in practice (Iqbal, 2019). The absence of clarity in the definition spells trouble for legal security and can lead to differing interpretations and applications across the board. The doctrinally, the provision needs to be interpreted with care by judges to balance freedom of expression with limitations to harmful speech and comparative legal analysis demonstrates that most jurisdictions have introduced narrower statutory definitions to inform application. The scholarly discussion also emphasizes that ambiguous terminology in cyber laws might result in both over- and under-enforcement, thus interfering with the basic rights and legal certainty (A. Khan, 2020; S.

Rehman, 2019). In line with this, Section 11 represents a required yet poorly-defined control measure of hate speech on the internet.

2. Self-Censorship

Self-censorship by both journalists and citizens may occur due to fear of legal action and thus, creates a chilling effect on the freedom of expression (Kaye, 2019). This is an indication of a wider regulatory effect in which the very existence of a strict or unclear legal rule affects behaviour without necessarily being enforced. Doctrinally, such consequences create issues about how much speech and expression should be regulated by the state and what the constitution contains in terms of constitutional guarantees. Comparative legal analysis also suggests that countries that have a higher degree of protection of the freedom of the press and more effective protection of procedures are less likely to suffer self-censorship. To this end, the scholarly discussion points to the fact that excessive criminalization or lack of clear regulatory frameworks can indirectly curb basic rights because they prompt people to be cautious and restrict open societal discourse (A. Khan, 2020; S. Rehman, 2019).

2.1. Chilling Effect

The chilling effects can considerably decrease the rate of democratic participation since they can deter people to freely express their views and participate in the discourse (UNESCO, 2020). When citizens and journalists foresee possible legal repercussions of expression, they tend to restrain their involvement in political and social discussions by themselves. Doctrinally, this poses serious questions on the safety of fundamental rights like freedom of expression and association which are critical to a working democracy. Comparative analysis also indicates that democratic societies that have greater protection of free speech and open legal systems are more likely to have a greater civic turnout. Thus, the scholarly literature highlights that the regulatory climate that creates chilling effects can undermine democratic institutions indirectly by restricting open participation and informed popular discourse (A. Khan, 2020; S. Rehman, 2019).

2.2. Online Activism Restrictions

Activists are often subject to legal investigation in accordance with the provisions of PECA, and it has already cast doubt on the possibility of using it against dissenting opinions (Amnesty International, 2021). This form of scrutiny can have a more extensive effect on civic space especially where legal provisions are used in a way that is seen to be aimed at activism or critical expression. This state of affairs casts doubts on the proportionality of the enforcement of cybercrime and how it is related to constitutional guarantees of basic rights. The comparative legal study goes on to show that in jurisdictions which have better protections of civil liberties, the law is structured in such a way that it presents a clear difference between justified security and peaceful activism. Based on this, the scholarly literature posits that unclear or widely-implemented cybercrime clauses can jeopardize the democratic process through uncertainty and intimidation of activists (A. Khan, 2020; S. Rehman, 2019).

2.3. State Surveillance under PECA: Privacy, Expression, and Legal Safeguards

The issue of surveillance by the state is a major concern with respect to the right to privacy, especially in the digital era where personal communication, online activity and electronic data can be easily monitored as opposed to the earlier days. The state may need some powers to prevent cybercrime, terrorism, fraud and threats to the nation's security, but the powers should always be within constitutional and legal boundaries. Surveillance that is overly general, vague, or unsupervised can result in misuse of power and an undue encroachment on citizen privacy. The importance of the issue becomes more when the context of the Prevention of Electronic Crimes Act, 2016 is taken in as PECA empowers the authorities to investigate and regulate online behaviors. These powers need to be closely considered to understand if they are to benefit citizens or instill fear among citizens on digital platforms. There is a strong connection between privacy and freedom of expression, as individuals may be less likely to express their views online if they perceive that their actions are being monitored at all times. This may lead to self-censorship by people who are reluctant to exercise their right to free expression for fear of being investigated, harassed, or prosecuted (A. Khan, 2020; S. Rehman, 2019). Hence, the state surveillance by PECA should be read and studied from the perspective of doctrinal analysis, comparison with other legal standards, constitutional principles, and legal interpretation as well as case law analysis. Such an analysis is helpful for establishing if

the law is balanced between cyber security and fundamental rights. A democratic legal system should guarantee that there is no unlimited and arbitrary and politically motivated surveillance. These safeguards would otherwise diminish privacy, curtail free internet expression and impact the overall protection of digital rights in Pakistan.

2.4. The Impact of Prevention of Electronic Crimes Act PECA on Freedom of Expression

The Prevention of Electronic Crimes Act, 2016 (PECA) is the first major law in Pakistan to govern cybercrime and digital behavior. PECA was enacted to fight against crimes including internet terrorism, internet harassment, and identity theft but by doing so, it has a great impact on the exercise of freedom of expression online. Although the law is meant to guarantee national security and order among the people, it has created a lot of controversy to the meaning of the law as far as the fundamental rights are concerned especially on the right to freedom of speech as enshrined in Article 19 of the Constitution of Pakistan. The conflict between control and freedom is at the core of this discussion (Freedom Network, 2022; Human Rights Commission of Pakistan, 2021).

2.4.1. Legal Framework of PECA and Freedom of Expression

PECA provides a wide legal framework of cyber crimes, with some of its provisions criminalizing sharing of information that could be considered harmful to national security or even civil order. Nevertheless, the law collides with the constitutional rights of freedom of speech that necessitates any limitation to be reasonable, and adequate. Opponents state that PECA is not clear and gives broad discretionary authority to the authorities that could lead to a violation of the right to legitimate expression (Digital Rights Foundation, 2021; M. Khan, & Ahmad, R. , 2020).

2.4.2. Vague and Overbroad Provisions

A key issue of PECA is that ambiguous and ambiguous language is used in a number of the provisions, such as the provisions concerning fake information and defamation. This is because such ambiguous terms can be subjectively interpreted by the law enforcement agencies and this creates confusion among citizens. Such ambiguity is a chilling effect that prevents people to voice their opinions in a free way, particularly when it comes to political issues (Article 19, 2020; S. Rehman, 2019).

2.4.3. Impact on Journalists and Media Professionals

PECA has had a major impact on journalists and media professionals due to the fact that investigative reporting and criticism of public institutions can be subjected to the provisions of PECA. Arrests and prosecutions of journalists under PECA have caused a lot of concern regarding freedom of the press in Pakistan. This state of affairs discredits the media as a watchdog and makes the democratic accountability weak (Freedom Network, 2022; International Commission of Jurists, 2020).

2.4.4. Role of the Federal Investigation Agency (FIA) and National Cyber Crimes Investigation Agency (NCCIA)

PECA is administered by the Federal Investigation Agency (FIA) now it's special wing called National Cyber Crimes Investigation Agency (NCCIA) which investigates and prosecutes. There are however concerns that have been raised over the wide powers accorded to the agency with no enough checks and balances. There are also some claims of selective enforcement and abuse of power, which imply that the law may be applied to the target of political opponents and dissenting voices (Human Rights Commission of Pakistan, 2021; International Commission of Jurists, 2020).

2.4.5. Regulation of Social Media and Digital Platforms

PECA is now applied to social media platforms as well, which means that the government can block or delete content that it considers illegal. Regulation is needed to curb detrimental online behavior, however, over-regulation may impede free discussion and curtail different opinions. Critics say that the regulation of content by PECA is often not transparent and without due process, and expresses their concerns on arbitrary censorship (Access Now, 2022; Digital Rights Foundation, 2021).

2.4.6. Effect on Public Discourse

The overall effect of PECA provisions has resulted in a chilling effect on the discourse of the people. Self-censorship may be used by citizens, activists and bloggers in order to escape legal penalties. This atmosphere does not encourage the freedom of dialogue and sharing of ideas that are the key aspects of a democratic society. This is made even worse by the fear of surveillance and prosecution (Article 19, 2020; S. Rehman, 2019).

2.5. Need for Reforms and Safeguards

2.5.1. Legal Clarity and Safeguards

The rules of PECA, especially those that deal with content regulation, must be explicitly stated to prevent ambiguity. Certain safeguards should be put in place to guard against misuse of powers. This will strike a balance between regulation and human rights.

2.5.2. Judicial Oversight Mechanism

An effective judicial review mechanism should be put in place to review regulatory actions. This would promote less arbitrariness of censorship and aid in accountability. It will also help to enhance public trust in Cyber-governance.

2.5.3. Institutional Capacity Building

Technical training and support should be provided to law enforcement agencies such as NCCIA and PTA. This will help in investigation and enforcement of cyber laws. Ongoing training is needed in the digital era.

2.5.4. Raising Awareness and Digital Literacy

Public awareness campaigns should be conducted to create awareness on cyber laws and digital rights. Good online behavior and prevention of cyber crime can be achieved through enhanced digital literacy. It is essential that it is successful with the public.

2.5.5. Regular Review and Amendment of Law

Periodic review of PECA is needed to keep pace with technology and global trends. Reforms should consider issues like AI and privacy. Adapting laws for sustainability.

2.5. The Impact of the Prevention of Electronic Crimes Act (PECA) on Freedom of Expression and National Security in Pakistan

Digital technologies have revolutionized how people voice their opinions, seek information and engage in public debate. In parallel, the volume of cybercrimes like online fraud, identity theft, cyber terrorism, hate speech and digital harassment has surged, leading to the creation of specific cybercrime laws by the governments. The Prevention of Electronic Crimes Act (PECA), 2016, was passed in Pakistan to combat cyber related offences and enhance national security in the digital world. The law has strengthened the powers of the State in investigating and prosecuting cybercrimes, but it has also sparked a lot of discussion about the impact it may have on freedom of expression and the basic rights enshrined in the Constitution of Pakistan. One of the most difficult legal questions in the cyber governance structure of Pakistan is the balance between national security protection and democracy. Learned from the Government of Pakistan (2016); United Nations Office on Drugs and Crime (2013).

2.5.1. Legislative Objectives and Scope of PECA

The Prevention of Electronic Crimes Act (PECA), 2016 has been enacted to come up with a comprehensive legal framework for the prevention of cybercrime in Pakistan. The Act makes certain offences, including online dissemination of hate speech and online harassment, unauthorized access to information systems, cyber terrorism, electronic fraud and identity theft of criminal offences. It enables the law enforcement agencies, especially the Federal Investigation Agency (FIA), to investigate and prosecute electronic crimes and offers ways to collect digital evidence. The main purpose of PECA is to ensure cyber security and protection of the national interests in the digital society. Yet, there are a number of provisions that are drafted in a broad way, raising concerns about their interpretation and implementation in relation to online speech and criticism of public institutions (Government of Pakistan, 2016; United Nations Office on Drugs and Crime, 2013).

2.5.2. PECA and Freedom of Expression

The Constitution of Pakistan guarantees freedom of expression under Article 19, which has been limited by reasonable restrictions as necessary for the preservation of national security, public order, morality and the integrity of the state. Some of the provisions of PECA, especially those relating to illegal online content, cyber terrorism and offences against the dignity of persons or institutions, could have a chilling effect on journalists, civil society organizations and social media users. Scholars and critics argue that fears of criminal prosecution for online expression may lead to self-censorship and, in turn, restrict democratic debate and public accountability. Proponents of the Act, on the other hand, argue that there is a need for responsible regulation of platforms to address issues of misinformation, hate speech and online incitement without abridging the right to freedom of expression (International Commission of Jurists, 2019; Khan, 2021).

2.5.3. PECA as a Tool for National Security

National security is one of the main grounds for the introduction and implementation of PECA. The Act grants legal powers to investigate cyber terrorism, extremist propaganda, cyber espionage, attacks on critical information infrastructure and other offences endangering national stability. It also supports collaboration between investigative authorities and digital service operators in collecting evidence and in the prevention of cybercrime. By enhancing Pakistan's capabilities in addressing emerging cyber security threats, PECA has made a significant contribution to the country's cyber defenses. Legal advisers, however, point out that any national security measures must be taken with constitutional safeguards and in compliance with international human rights standards to avoid misuse of the power of the state (Government of Pakistan, 2016; United Nations Office on Drugs and Crime, 2013).

2.5.4. Judicial Interpretation and Human Rights Concerns

The courts of Pakistan have also been instrumental in understanding the terms of PECA and upholding it in accordance with the constitutional values. Amidst the criticisms from the judiciary, the emphasis has been laid on the importance of proportionality, fairness in procedure and against arbitrary encroachments on fundamental rights. The human rights record of the government has been criticized for its investigative powers, its ability to remove content from social media, and its potential for misuse against political opponents, journalists and activists. Courts have increasingly stressed the necessity and proportionality requirements in the constitutional context of limitations on online expression. Judicial oversight is thus an essential tool for balancing cyber security goals and civil liberties, and is a major factor in the protection of civil liberties (Human Rights Commission of Pakistan, 2022; International Commission of Jurists, 2020).

2.5.5. Need for a Rights-Based Approach to Cyber Security under PECA

The success of PECA is reliant on maintaining a balance between national security and the safeguarding of fundamental freedoms over the long-term. Legislation in the field of cyber security should focus on the real threat of cyberspace and include clear processes, judicial oversight, accountability mechanisms and protection against arbitrary enforcement. Confidence in the implementation of PECA can be enhanced through legislative change, definition of key concepts in the law, creation of independent oversight bodies and strengthening of procedural safeguards. With the digital economy and online presence in Pakistan steadily growing, it is crucial that a rights-based cyber security framework is developed to enhance the country's national security and democratic governance (Human Rights Commission of Pakistan, 2022; Khan, 2021).

3. Conclusion

All the major laws passed by Pakistan in response to the growing cybercrime problems in the increasingly digitized society were the first foray in this direction with the Prevention of Electronic Crimes Act, 2016. But the use of PECA has caused deep concern particularly in terms of freedom of expression. While the law was intended to protect from real cybercrime, many of its provisions are deemed to be too vague, too broad and lacking in clear boundaries. Given this uncertainty, PECA has been criticized in many cases to be applied to journalists, media personnel, political activists, and people voicing opposing views. This can create the danger that legislation designed to protect becomes a means of abridging free expression and stifling criticism. The Act establishes a legal

framework to address cybercrimes like cyber harassment and data breach, and online fraud, but has raised plenty of questions about its effects on freedom of expression over the Internet. The paper has shown that the Act, although with noble intentions, presents massive chances of curbing freedom of lawful speech due to its expansive and unclear language. The review indicates that some parts of the legislation are not well defined and can be interpreted broadly, thus allowing them to be abused by law enforcers. The paper has presented a critical analysis on the PECA 2016, in its recently amended form, has a very difficult time grappling with digital speech in Pakistan. The paper highlights some of the most important clauses of the Act particularly the provision of freedom of speech with reasonable restrictions as provided in Article 19 of the Constitution of Pakistan. This has resulted journalists, activists and even the common people to not be able to express their views online because of the fear of being charged with a lawful action. In addition, the lack of uniformity in judicial interpretation and the lack of effective procedural protection have been a factor in these problems, raising questions about the respect for constitutional guarantees, such as the right to freedom of expression. But, the significance of cyberspace control can never be overemphasized, particularly in the wake of increasing cybercrimes. Thus, a delicate balance has to be maintained between the protection of security and the fundamental rights. The paper ends that the reforms are essential to make them more clear, to introduce more effective protections against their misuse, and to ensure proportional enforcement.

References

- Access Now, A. (2022). Pakistan: Concerns over digital censorship and PECA amendments. .
- Cyber harassment laws in Pakistan, (2020).
- Cybercrime frameworks, (2021).
- Amnesty International, A. (2021). Digital rights report.
- Article 19, A. (2020). Pakistan: Freedom of expression and regulation of online content. Article 19 Organization.
- Digital Rights Foundation, D. (2021). Analysis of PECA and its implications on digital rights in Pakistan. Digital Rights Foundation.
- Digital Rights Foundation, D. (2022). Data protection report.
- Freedom Network, f. (2022). Freedom of expression and media safety report Pakistan. Freedom Network.
- Government of Pakistan, G. (2016). Prevention of Electronic Crimes Act, 2016 (Act XL of 2016). Government of Pakistan.
- HRCP. (2018). Human rights report.
- Human Rights Commission of Pakistan, H. (2021). State of human rights in Pakistan 2021. HRCP.
- Human Rights Commission of Pakistan, H. (2022). State of human rights in 2022. Human Rights Commission of Pakistan.
- International Commission of Jurists, I. (2019). Pakistan: The Prevention of Electronic Crimes Act and freedom of expression. International Commission of Jurists.
- International Commission of Jurists, I. (2020). Cybercrime legislation and human rights in Pakistan. ICJ.
- Iqbal, M. (2019). Hate speech laws.
- Kaye, D. (2019). Speech police.
- Khan, A. (2020). Cyber law analysis.
- Khan, A. A. (2021). Cyber laws and freedom of expression in Pakistan: Challenges of balancing security and civil liberties. *Journal of Law and Society*, 52(52), 95–114.
- Khan, M., & Ahmad, R. . (2020). Cyber laws and freedom of expression in Pakistan: A critical analysis of PECA. *Pakistan Law Review*, 12(2), 45–60.
- PECA. (2016). Prevention of Electronic Crimes Act.
- PTA. (2021). Content regulation.
- Rehman, S. (2019). Legal challenges to freedom of speech under cybercrime laws in Pakistan. *Journal of South Asian Studies*, 34(1), 89–102.
- Rehman, T. (2019). Constitutional law.
- UNESCO. (2020). Freedom of expression.
- United Nations Office on Drugs and Crime, U. (2013). Comprehensive study on cybercrime. United Nations.