IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

Policy Brief

PECA 2025: A Dispassionate Analysis

Maham Naweed
Khadija Almus Khanum

February 2025

Chair International Law

Executive Summary

The Prevention of Electronic Crimes Act (PECA) 2016 was Pakistan's initial effort to combat cybercrime. Recently, it has been updated through the 2025 amendment to address the rapidly evolving digital landscape. This amendment aims to modernize the legal framework, equipping the state to tackle emerging cyber threats and ensure digital security. However, the PECA amendments have ignited considerable debate and criticism, primarily centered on their potential impact on freedom of expression and the risk of abuse by state authorities. Key recommendations include refining vague definitions, ensuring independent oversight for due process, promoting transparency through regular reporting, and enhancing capacity-building initiatives for law enforcement and public awareness on digital rights. Implementing these measures can help foster a balanced digital regulatory framework that safeguards both national security and individual freedoms.

Policy Recommendations

- **Narrow and Clarify Definitions:** The Act could benefit from clear and precise definitions of terms such as "disinformation", "hate speech", "fake and/or false" along with any other terms requiring clearer definitions.
- **Strengthen Due Process:** All content takedown requests need clear legal justifications, and it should be made clear in the Act that the Social Media Protection Tribunal will function as an independent body.
- **Promote Transparency and Accountability:** The Digital Rights Protection Authority ("DRPA") and Social Media Protection and Regulatory Authority ("SMPRA") could publish regular reports detailing their activities, including the number of content takedown requests, the legal basis for such requests, and their outcomes.
- **Emphasize Capacity Building and Awareness:** Investing in training programs for law enforcement and regulatory personnel on freedom of expression, digital rights, and international human rights standards is essential. Public awareness campaigns can also educate citizens about their rights and responsibilities in the digital space.

BACKGROUND

The National Assembly of Pakistan enacted the Prevention of Electronic Crimes Act ("PECA") 2016 on 19 August 2016. PECA was enacted to provide a comprehensive legal framework for combating cybercrime.

The 2025 amendment seeks to update and refine PECA in response to rapid technological changes. This amendment aims to modernize the legal framework to address the evolving challenges posed by digital technologies and cyber threats. The amendment was passed by the National Assembly and received presidential assent on 30 January 2025. These amendments have sparked intense debate and criticism, primarily over their implications for right of freedom of expression and the potential for abuse by state authorities. Critics argue that the amendments contain vague language, granting law enforcement agencies broad discretion in interpreting the law.[1] Additionally, they contend that the amendments undermine Articles 19 and 19A of the Constitution of Pakistan, which guarantee freedom of expression and the right to information.[2] The amendments are also seen as an attempt to tighten control over digital and internet freedoms, posing a threat to journalists, activists, and political opponents.[3]

While freedom of speech is a fundamental right recognized in both international and domestic law, it is not absolute. Digital platforms, which have become a key medium of expression, are subject to regulations aimed at preventing hate speech, violent content, and any form of expression that could potentially harm or defame individuals or groups within society and pose a risk to national security.

FREEDOM OF EXPRESSION IN INTERNATIONAL LAW

In several international human rights instruments, the right to freedom of opinion and expression is enshrined and protected. Article 19 of the Universal Declaration of Human Rights ("UDHR") underscores the importance of freedom of expression as a fundamental human right, allowing individuals to express their thoughts freely and access information without

[1] Dawn Report, PECA stifles free speech, doesn't curb disinformation (Dawn, 12 February 2025) https://www.dawn.com/news/1891428 accessed 12 February 2025.
[2] Ibid.
[3] International Federation of Journalists, Pakistan: PECA amendments further tighten government grip on digital expression (*IFJ*, 29 January 2025) https://www.ifj.org/media-centre/news/detail/category/press-releases/article/pakistan-peca-amendments-further-tighten-government-grip-on-digital-expression accessed 12 February 2025.

censorship.[4] Similarly, Article 19 of the International Covenant on Civil and Political Rights ("ICCPR") reaffirms the principles laid out in the UDHR, emphasizing that every individual has the right to freedom of expression. However, this right carries certain duties and responsibilities and may therefore be subject to necessary restrictions by law to safeguard the rights and respect of others, as well as national security and public order.[5] Article 10 of the European Convention on Human Rights ("ECHR") acknowledges that while freedom of expression is protected, it may be limited by laws that are necessary in a democratic society.[6] Other international instruments, such as the African Charter on Human and Peoples' Rights[7] and the American Convention on Human Rights[8], also recognize the importance of free expression while emphasizing that it must be exercised within legal boundaries.

FREEDOM OF EXPRESSION IN PAKISTAN'S CONSTITUTION

Article 19 and Article 19A of the Constitution of Pakistan address fundamental rights related to freedom of speech and access to information.

Article 19 states:

> *"Every citizen shall have the right to freedom of speech and expression, and there shall be freedom of the press, subject to any reasonable restrictions imposed by law in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, commission of or incitement to an offence."*

A breakdown of this right highlights three key facets of its scope:

---

[4] United Nations, Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III), art 19 https://www.un.org/en/about-us/universal-declaration-of-human-rights accessed 7 February 2025.
[5] United Nations, *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 19 https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights accessed 7 February 2025.
[6] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms* (European Convention on Human Rights, as amended) art 10 https://www.echr.coe.int/documents/d/echr/convention_ENG accessed 7 February 2025.
[7] African Union, *African Charter on Human and Peoples' Rights* (adopted 01 June 1981, entered into force 21 October 1986) art 9 https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf accessed 7 February 2025.
[8] Organization of American States (OAS), *American Convention on Human Rights* (adopted 22 November 1969, entered into force 18 July 1978) art 13 https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights.pdf accessed 7 February 2025.

i. Every citizen has the right to express their thoughts and opinions freely.
ii. The press has the right to operate without undue interference.
iii. This right is subject to restrictions aimed at protecting national interests, public order, and morality.

Article 19A states:

> *"Every citizen shall have the right to have access to information in all matters of public importance subject to regulation and reasonable restrictions imposed by law."*

The two primary aspects of this right are:

i. Citizens have the right to obtain information related to matters of public importance.
ii. The exercise of this right is subject to regulations and reasonable restrictions imposed by law.

In 2016, the Supreme Court of Pakistan, in the case of **Pakistan Broadcasters Association v. Pakistan Electronic Media Regulatory Authority**, held that,

> "*State could regulate the right to speech when it came into conflict with the rights of other individuals or other societal interests.*"[9]

The apex court further held:

> *"In a civilized and democratic society, restrictions and duties co-existed in order to protect and preserve the right to speech. It was thus inevitable to maintain equilibrium by placing reasonable restriction on freedom of expression in the maintenance of public order."*[10]

INTERNATIONAL FRAMEWORKS ON CYBERCRIME AND DIGITAL REGULATION

Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime, formally known as the Convention on Cybercrime of the Council of Europe is recognized as the first international treaty addressing

[9] PLD 2016 SC 692.
[10] Ibid.

crimes committed via the internet and other computer networks. This Convention aims to harmonize national laws, enhance international cooperation, and improve the effectiveness of investigations and prosecutions of cybercrime. It establishes a framework for mutual assistance among countries, enabling them to share information and resources during cybercrime investigations.[11]

Tallinn manual on the international law applicable to cyber warfare

The Tallinn Manual on Cyber Warfare is a comprehensive guide developed by experts in international law regarding the application of existing legal frameworks to cyber operations during armed conflict. It analyzes how established international legal norms apply to this "new" form of warfare and emphasizes that international humanitarian law is applicable to cyber warfare, thereby establishing principles for state conduct in cyberspace during military operations. While its primary aim is to address cyber threats during armed conflict, the manual also underscores the broader significance of regulating the digital domain, highlighting how the vulnerabilities of cyberspace can pose serious challenges to national security, critical infrastructure, and global stability if left unchecked.[12]

United Nations' Efforts

The United Nations ("UN") has been actively engaged in promoting digital rights and cybersecurity through various resolutions and initiatives. Resolutions such as A/RES/70/125 highlight the importance of enhancing global cooperation in combating cybercrime while respecting human rights online. The UN General Assembly has called upon member states to develop comprehensive national strategies that align with international norms.[13] In 2007, the International Telecommunication Union ("ITU"), the UN's specialized agency for information and communication technologies ("ICTs"), launched the Global Cybersecurity Agenda, which

[11] Council of Europe, *Convention on Cybercrime* (Budapest Convention, adopted 8 November 2001, entered into force 1 July 2004) https://www.coe.int/en/web/cybercrime/the-budapest-convention accessed 8 February 2025.
[12] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013).
[13] United Nations General Assembly, *Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society* (16 December 2015) UNGA Res 70/125 https://unctad.org/system/files/official-document/ares70d125_en.pdf accessed 8 February 2025.

focuses on building a global framework for cybersecurity through capacity building, international cooperation, and public-private partnerships.[14]

COMPARATIVE ANALYSIS OF CYBERCRIME LAWS

Regulation of electronic crimes or cybercrimes might be relatively new to Pakistan's legal framework, but many states have enacted cybercrime legislation to address the increase in online activity and ensure proper policing and enforcement.

United States

In 1986, the United States passed the Computer Fraud and Abuse Act ("CFAA"), a key piece of legislation aimed at addressing cybercrime. Over the years, through amendments and several Supreme Court rulings, the CFAA's scope has broadened. The Act prohibits unauthorized access to protected computers and networks, as well as exceeding authorized access. It covers a wide range of computer-related offenses and imposes both civil and criminal penalties. The CFAA addresses issues such as trespassing, threats, damage, espionage, and the use of computers as instruments of fraud. It is also often referred to as an anti-hacking law.[15]

United Kingdom

The United Kingdom's Online Safety Act 2023 aims to regulate online content and ensure user safety on the internet. This Act includes specific provisions to address illegal and harmful content, with particular emphasis on protecting children online. It requires service providers to take action against illegal content and activity, including controlling or coercive behavior, sexual violence, fraud, racially or religiously aggravated public order offenses, inciting violence, intimate image abuse, selling illegal drugs or weapons, terrorism, and other related activities. New offenses introduced by the Act include encouraging or assisting serious self-harm, cyberflashing, sending false information intended to cause non-trivial harm, threatening communications, and intimate image abuse.[16]

---

[14] International Telecommunication Union (ITU), *Global Cybersecurity Agenda (GCA)* https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx accessed 8 February 2025.
[15] National Association of Criminal Defense Lawyers (NACDL), *Computer Fraud and Abuse Act (CFAA)* https://www.nacdl.org/Landing/ComputerFraudandAbuseAct accessed 8 February 2025.
[16] UK Government, *Online Safety Act 2023: Explainer* (2023) https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer; *Online Safety Act 2023* (UK Public General Acts, 2023 c.50) https://www.legislation.gov.uk/ukpga/2023/50 accessed 8 February 2025.

The United Kingdom's Computer Misuse Act 1990 makes it illegal to access computer systems without authorization, aiming to protect computer systems from hacking and other cyber offenses. It prohibits activities such as gaining unauthorized access to computer data or systems and performing actions that could impair system functionality. The Act was later amended to introduce harsher punishments for cybercrime and to address emerging types of cyber offenses.[17]

European Union

The General Data Protection Regulation ("GDPR"), drafted and passed by the European Union (EU), is a comprehensive data protection law applicable to all organizations operating within the EU or processing the personal data of EU residents. It imposes stringent security requirements for data processing and mandates businesses to safeguard personal data from breaches and unauthorized access. Organizations that fail to comply with the GDPR can face hefty fines.[18]

The Digital Services Act (DSA) is another comprehensive framework for regulating online platforms and digital services in the European Union. The DSA includes measures to tackle illegal content, ensure transparency in online advertising, and protect users' fundamental rights online.[19]

India

The Information Technology Act 2000 is the primary legislation governing cybercrime and electronic commerce in India. It provides a legal framework for addressing cyber offenses, data protection, and the responsibilities of internet intermediaries. Hacking, data theft, and cyberterrorism are among the numerous areas covered by the Act. The 2008 amendment strengthened its provisions, broadened its scope, and introduced new offenses to keep pace with the evolving nature of cybercrime.[20]

---

[17] United Kingdom, *Computer Misuse Act 1990* (UK Public General Acts, 1990 c.18) https://www.legislation.gov.uk/ukpga/1990/18/contents accessed 8 February 2025.
[18] European Union, What is GDPR, the EU's new data protection law?? https://gdpr.eu/what-is-gdpr/ and, General Data Protection Regulation (GDPR) https://gdpr-info.eu/ both accessed 8 February 2025.
[19] European Commission, *Digital Services Act* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en accessed 8 February 2025.
[20] Government of India, *Information Technology Act 2000 (as amended)* https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf accessed 8 February 2025.

China

China's Cybersecurity Law, which came into effect in 2017, aims to strengthen data protection, localize data, and enhance cybersecurity to safeguard national security. The law establishes the principle of cyberspace sovereignty and mandates that critical information infrastructure operators implement stringent security measures, comply with data localization requirements, and cooperate with cybersecurity authorities. It addresses various cyber activities deemed to threaten national security and social stability, including hacking, data theft, and the dissemination of prohibited information. Additionally, the law provides clear regulations on legal liability, prescribing penalties such as fines and revocation of permits and business licenses for violations.[21]

OVERVIEW OF THE PECA ACT (2016)

In 2016, Pakistan enacted PECA to address the evolving digital landscape and the growing need for legal frameworks to combat cybercrime and ensure digital security. This controversial legislation laid the foundation for regulating online activities, protecting citizens from digital threats, and providing mechanisms for prosecuting electronic crimes. PECA applies across Pakistan and extends to all citizens, regardless of their location, with the objective of combating cybercrimes such as unauthorized access to computer systems, electronic fraud, cyberbullying, and online harassment. It outlines various offenses and corresponding punishments, including hate speech, electronic forgery and fraud, unauthorized use of identity information, and related offenses.[22]

The passage of PECA 2016 was met with significant criticism from various stakeholders, including human rights organizations, legal experts, and civil society. Critics argued that PECA severely restricts citizens' rights to free speech and expression, with many of its provisions being vague and open to interpretation. Concerns were also raised that the law could enable excessive surveillance without proper oversight or a clear data protection framework.

---

[21] *Cybersecurity Law of the People's Republic of China* (effective 1 June 2017) (translated by DigiChina, Stanford University) https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ accessed 8 February 2025.

[22] Government of Pakistan, *Prevention of Electronic Crimes Act 2016* https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj accessed 9 February 2025.

In 2022, the Islamabad High Court ("IHC") declared the PECA amendment unconstitutional, which sought to expand the scope of Section 20 (criminal defamation) to include institutions. The IHC also struck down parts of Section 20 that criminalized defamation, ruling that it violated constitutional protections for free speech.[23] While the Supreme Court has reviewed cases involving PECA and requested briefings on its compatibility with fundamental rights, it has never rendered a definitive judgment criticizing or invalidating its provisions.

Although PECA 2016 faced significant criticism at the time of its enactment, it has been applied in several cases, demonstrating its role in addressing cybercrimes in Pakistan. *In State vs. Sarmad Liaquat*, the accused was convicted under Sections 20, 21, and 24 of PECA for offenses related to the dignity of a person and cyberstalking. The court found sufficient evidence to establish the charges, sentencing the accused to three years' imprisonment under Section 21, along with additional penalties under Section 24 for cyberstalking.[24] Another notable instance occurred in Peshawar, where an individual was convicted under Section 21 of PECA, receiving two years' rigorous imprisonment and a fine. This case underscored the law's role in prosecuting offenses against individual modesty and online harassment, reinforcing legal mechanisms for protecting victims of cybercrimes.[25]

PECA 2025 Amendment

In January 2025, Pakistan's Parliament passed the Prevention of Electronic Crimes (Amendment) Act 2025, introducing significant changes to the cybercrime legislation.[26] The amendment aims to enhance regulatory oversight of online content and impose stricter penalties for disseminating disinformation. It also proposes the creation of the Digital Rights Protection Authority ("DRPA"), empowered to regulate unlawful content, including

[23] The Express Tribune, 'IHC strikes down PECA ordinance' (*The Express Tribune*, 8 April 2022) https://tribune.com.pk/story/2351529/ihc-strikes-down-peca-ordinance accessed 9 February 2025.
[24] Digital Rights Foundation, *State vs Sarmad Liaquat* https://digitalrightsfoundation.pk/state-vs-sarmad-liaquat/ accessed 9 February 2025.
[25] Peshawar High Court, *Quashment Petition No. 50-P of 2022* https://peshawarhighcourt.gov.pk/PHCCMS/judgments/QP50-2022---FFFRRR.pdf accessed 9 February 2025.
[26] National Assembly of Pakistan, *Act No. II of 2025: An Act further to amend the Prevention of Electronic Crimes Act, 2016* https://www.na.gov.pk/uploads/documents/679b243193585_457.pdf accessed 10February 2025.

blasphemy, hate speech, incitement to violence, obscenity, defamation, and material against the defense or security of Pakistan.[27]

The amendment broadens the definition of "social media platforms" to include websites, applications, and tools facilitating digital communication, encompassing any individual or entity operating such platforms within Pakistan. Social media platforms may be required to register with the government, establish local offices, and appoint representatives in Pakistan. Additionally, the Social Media Protection and Regulatory Authority ("SMPRA") has been established to regulate social media platforms, ensure online safety, and address unlawful content.[28]

Similar to the original PECA 2016, the 2025 amendment has faced widespread criticism from media, human rights groups, and political entities within Pakistan. Critics argue that the amendments further tighten governmental control over digital expression and internet freedom, criminalizing dissent and suppressing free speech due to vague and broad language that could be misused against media professionals, journalists, political activists, and human rights defenders.

Appeals against the 2025 amendments have been filed in the IHC, notably by the Pakistan Federal Union of Journalists ("PFUJ")[29] and several television anchors[30], raising concerns about infringements on press freedoms and civil liberties. While the PECA amendments await judicial review, it is essential to recognize that these changes aim to address critical challenges in the digital landscape and align Pakistan's legislative framework with global trends in combating cybercrimes.

The amendments penalize the dissemination of false or misleading information that could cause fear, panic, or unrest, an essential measure in an era of rapid misinformation spread. Regulating harmful content like hate speech and obscenity seeks to create a safer online environment, especially for vulnerable groups such as women and minorities often targeted by cyber harassment. The establishment of regulatory bodies ensures better oversight of online

[27] Ibid.
[28] Ibid.
[29] PFUJ challenges PECA amendments in IHC (*The Express Tribune*, 6 February 2025) https://tribune.com.pk/story/2526928/pfuj-challenges-peca-amendments-in-ihc accessed 10 February 2025.
[30] Anchorpersons challenge Peca tweaks in IHC (*Dawn*, 8 February 2025) https://www.dawn.com/news/1890552 accessed 10 February 2025.

content, while the emphasis on digital ethics mandates compliance with national laws and introduces penalties for non-compliance, ensuring safer and more respectful online spaces.

Provisions to combat content against Pakistan's defense or security are crucial for protecting national interests from malicious actors exploiting digital platforms for anti-state propaganda or incitement, similar to measures taken by countries like the US and China.

While it remains to be seen whether these amendments will be upheld or quashed, balancing the protection of individual freedoms with the need for regulations is essential for safeguarding collective societal rights and fostering a just and fair society.

POLICY RECOMMENDATIONS

- **Narrow and Clarify Definitions:** The Act could benefit from clear and precise definitions of terms such as "disinformation", "hate speech", "fake and/or false" along with any other terms requiring clearer definitions. The current language is broad and vague, potentially leading to arbitrary enforcement and suppression of legitimate speech. Redefining these terms with greater precision, in line with international human rights standards and jurisprudence, ensures that only speech posing a direct and imminent threat to public safety or order is targeted.
- **Strengthen Due Process:** Concerns exist that the DRPA and SMPRA could act without sufficient oversight. All content takedown requests need clear legal justifications, and it should be made clear in the Act that the Social Media Protection Tribunal will function as an independent body, free from any influence, to ensure fair hearings and protect the rights of all parties involved.
- **Promote Transparency and Accountability:** The lack of transparency in the operations of regulatory bodies and potential for government overreach requires attention. The DRPA and SMPRA could publish regular reports detailing their activities, including the number of content takedown requests, the legal basis for such requests, and their outcomes.
- **Emphasize Capacity Building and Awareness:** Investing in training programs for law enforcement and regulatory personnel on freedom of expression, digital rights, and international human rights standards is essential. Public awareness campaigns can also educate citizens about their rights and responsibilities in the digital space.

Action Matrix				
Options for Pakistan				
Option	**Pathways to Solution**	**Implementation of Solution**	**Actors Responsible**	**Implementation Timelines**
Narrow and Clarify Definitions	Review and revise definitions of "disinformation", "hate speech", "fake and/or false", along with any other terms requiring clearer definitions, in consultation with legal experts and human rights organizations.	Draft amendments to include precise definitions aligned with international standards.	• Ministry of Law and Justice • National Assembly of Pakistan	6 - 12 months
Strengthen Due Process	Establish clear legal frameworks for content takedown requests with mandatory legal justifications. Ensure the Social Media Protection Tribunal operates independently.	Develop procedural guidelines for content moderation and tribunal operations. Provide training to tribunal members.	• Ministry of Information Technology and Telecommunication • SMPRA	6 - 12 months
Promote Transparency and Accountability	Mandate DRPA and SMPRA to publish periodic reports on content takedowns, legal bases, and outcomes.	Design and implement a reporting framework. Publish quarterly and annual reports.	• Ministry of Information & Broadcasting • DPRA • SMPRA	Continuous, starting within 3 months
Emphasize Capacity Building and Awareness	Develop training modules for law enforcement on digital rights and freedom of expression. Launch public awareness campaigns on digital rights.	Roll out training programs nationally. Design and execute awareness campaigns through digital and traditional media.	• Ministry of Information Technology and Telecommunication • Ministry of Human Rights • Civil Society Organizations	12-18 months