NATIONAL COMMISSION FOR HUMAN RIGHTS

Human Rights Implications of Pakistan's Cybercrime Law:

PECA and the 2025 Amendment Act

National Commission for Human Rights, Pakistan (NCHR)

Table of Contents

Acknowledgement

Author:
Jasmine Hoti Azeem

NCHR Oversight:
Ms Rabiya Javeri Agha, Chairperson NCHR

Design and Layout:
Aliza Aslam

The National Commission for Human Rights extends its sincere appreciation to its partner organisations Digital Rights Foundation (DRF), Media Matters for Democracy (MMfD), and Bolo Bhi for their invaluable support in collecting data and cross-verifying information throughout the course of this study. Their expertise and collaboration significantly strengthened the quality and credibility of the findings.

The Commission also expresses its gratitude to the **Ministry for Information** for taking the time to respond to queries raised by the NCHR and for engaging constructively on issues identified through consultations with relevant stakeholders.

Published Feb 2026

Foreword

The digital age has transformed how people connect, and hold power to account. But, it has also turned into a contested space where the lines between regulation and protection often blur. The Prevention of Electronic Crimes Act (PECA) was introduced to safeguard citizens from cybercrime, including hate speech and online harassment. However, its implementation and amendments have raised human rights concerns.

As Pakistan's independent human rights institution, the NCHR has a constitutional duty to review such laws through a human rights lens.This report examines the PECA Amendment Act 2025 and its impact on freedom of expression, privacy, and access to information which are rights guaranteed under Pakistan's Constitution and international human rights law.

Drawing on consultations with journalists, digital rights experts, legal practitioners, and civil society, the report aims not only to critique but to propose balanced reforms that protect digital rights while addressing national security concerns.

Findings show that while PECA includes provisions to address online abuse particularly for women and children, its broad and vague definitions have enabled overreach.

This report reaffirms NCHR's commitment to constructive engagement with the government, parliament, and civil society to build a fair digital governance framework grounded in transparency, accountability, and rights-based protection. Pakistan stands at a crossroads: laws like PECA must evolve to ensure digital security without silencing digital freedom, protect citizens without silencing them. This report is an invitation for reflection and reform, so that Pakistan's digital future remains open, safe, and rights-based.

Rabiya Javeri Agha
Chairperson
National Commission for Human Rights (NCHR)
Islamabad, Pakistan

NCHR Mandate

The National Commission for Human Rights (NCHR) is a statutory body established under the NCHR Act XVI of 2012. The Act stipulates a broad and overarching mandate for the promotion and protection of human rights, in line with Pakistan's Constitution, domestic laws and international treaties. NCHR was accredited as an A-status National Human Rights Institution (NHRI) by the Global Alliance of National Human Rights Institutions (GANHRI), a UN-linked body. As part of its statutory function, the Commission along with investigating human rights violations and providing relief to the victims, reviews existing and proposed legislations from a human rights perspective.

This report provides an analysis of the recent PECA Amendment Act passed by the government. The Commission has thoroughly examined national and international laws, key case laws, reports from reputable international organizations, and conducted extensive consultations with digital rights activists, journalists, and legal experts. Based on these findings, the report proposes several recommendations to prevent the misuse and misapplication of the PECA Amendment Act within Pakistan's digital landscape.

Executive Summary

The Prevention of Electronic Crimes (Amendment) Act 2025 marks a decisive moment in Pakistan's digital and democratic evolution. What began as an effort to protect citizens from online harassment, cyber fraud, and disinformation has transformed into a deeply contested instrument of control over digital expression. This report by NCHR examines the trajectory of Pakistan's digital governance. It traces its roots from informal censorship to the institutionalization of online regulation with a paricular lens on how the 2025 amendment has impacted fundamental rights, civic freedoms, and institutional independence.

Over the past two decades, the government's approach to regulating online spaces has shifted from sporadic content blocking to a formalized and expansive legal structure. The creation of the Social Media Protection and Regulatory Authority (SMPRA) under PECA 2025 consolidates unprecedented executive power to restrict and remove digital content under vague definitions of unlawful or offensive material. This centralization of control reflects a broader pattern in which regulatory measures intended for citizen protection are increasingly used to suppress dissent, limit media freedom, and political expression. The law expands the term aspersion to include criticism of state institutions such as the military, judiciary, and parliament. This change effectively revives the concept of criminal defamation. It undermines constitutional guarantees of free speech under Articles 19 and 19A and impacts Pakistan's obligations under the International Covenant on Civil and Political Rights (ICCPR).

The report highlights the cumulative impact of overlapping and ambiguous legal frameworks such as PECA, the PEMRA Ordinance, Defamation Ordinance, and Anti-Terrorism Act. Such legislations have created a punitive environment where expression is often treated as a threat to security. The establishment of new regulatory bodies and tribunals further undermines judicial independence and due process. By limiting appellate jurisdiction to the Supreme Court, PECA 2025 renders justice inaccessible for most citizens and weakens oversight mechanisms vital for accountability. The replacement of the FIA's Cybercrime Wing with the National Cyber Crime Investigation Agency (NCCIA) does little to address longstanding issues of inefficiency and privacy violations, instead expanding the government's surveillance capacity without adequate safeguards.

Equally concerning is the gendered impact of PECA's enforcement. While the law was envisioned to protect women and vulnerable groups from online violence, its implementation reveals systemic insensitivity and misuse. Data from the Digital Rights Foundation (DRF) shows that women make up 58% of harassment complainants, yet they continue to face stigma, intimidation, and secondary victimization during investigations. Sections of the law have even been used against

women journalists and survivors, reversing its protective intent. The transgender community faces further exclusion, with officials frequently dismissing or ridiculing their complaints—illustrating how patriarchal and discriminatory structures are embedded in enforcement mechanisms.

Beyond domestic implications, the PECA Amendment Act carries significant international and economic consequences. Its incompatibility with ICCPR standards particularly on freedom of expression, privacy, and fair trial has drawn scrutiny from international observers, including the European Union.[1]

Pakistan stands at a crossroads between digital security and digital freedom. It urges a fundamental recalibration of the country's approach to cyber governance—away from punitive regulation and toward a rights-based framework grounded in transparency, accountability, and inclusivity. NCHR advocates for reforms that decriminalize disinformation, strengthen judicial oversight, enact data protection laws, and integrate UNESCO's principles of digital governance, emphasizing transparency, diverse expertise, checks and balances, openness, and cultural inclusion.

Ultimately, this report calls for reflection and reform. Laws designed to safeguard citizens must not be used to silence them. True digital safety cannot be achieved through control—it requires trust, justice, and respect for human dignity. As Pakistan advances its digital governance framework, it must be guided by the objective of protecting democratic freedoms while ensuring a safe and rights-respecting digital environment.

[1] Absa Komal, "Don't take GSP+ for granted, says EU envoy," *Dawn News,* 30.Jan.2025 https://www.dawn.com/news/1888586 (accessed 28.Feb.2025)

Chapter 1

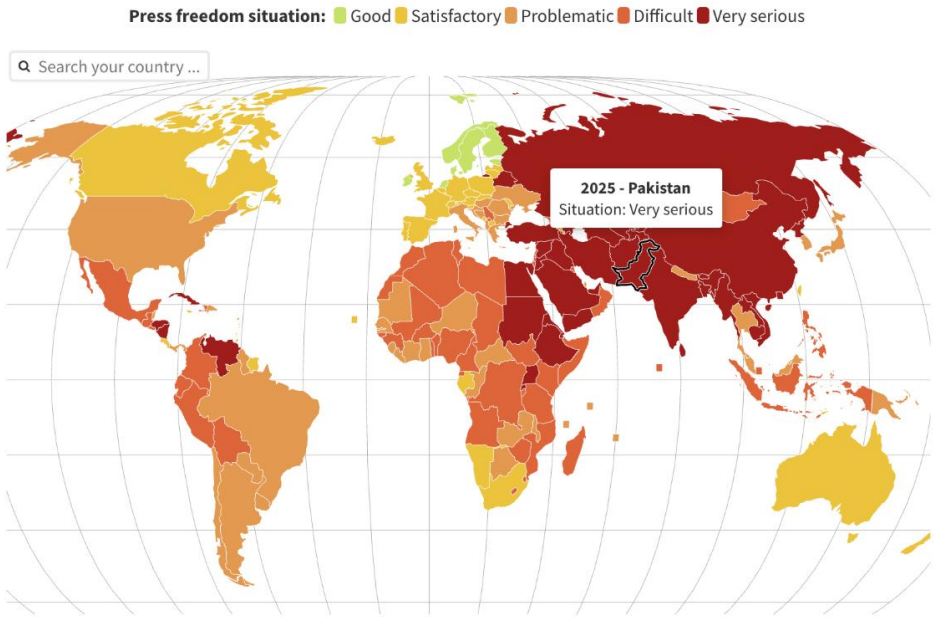
Introdcution

Every click leaves a trace, every regulation leaves an impact, between them lies the struggle to keep freedom alive in the digital age.

Introduction

The rise of the Information Age has introduced the growing challenge of cybercrime. Recognizing its impact, nearly 80% of countries have enacted cybercrime legislation to regulate digital threats[2] . One of the major components of cybercrime is the rapid spread of disinformation. As an emerging social phenomenon, it creates problems regarding trust in the news media, political polarization, manipulation of social media, the circulation of incorrect health information,online harrassment and hate speech. However, states regulatory responses have often been heavy-handed, leading to restrictions on democratic freedoms and human rights [3].

Pakistan faces similar challenges in balancing social and security concerns with fundamental rights of freedom of speech. Over the years the government has enacted several legislations to target disinformation, with the recent enactment of Prevention of Electronic Crimes Act (PECA) Amendment Act 2025. While the stated objectives of PECA include curbing online hate speech, terrorist content, and the harassment of women, serious concerns have been raised by stakeholders across the country. The law has frequently been invoked against dissidents and women who have spoken publicly about harassment—placing it in direct conflict with the Constitution of Pakistan and international human rights standards.



[2] "Global cyberlaw Tracker," *UN Trade and Development*, https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide (accessed from 25 Feb 2025)
[3] Irene Khan, "Disinformation and freedom of opinion and expression," *Human Rights Council 47th Session*, 21 June–9 July 2021 https://digitallibrary.un.org/record/3925306?v=pdf (accessed from 25 Feb 2025)

"According to the 2025 World Press Freedom Index by Reporters Without Borders (RSF), Pakistan fell to 158th place out of 180 nations, marking its lowest ranking in recent years. The drop underscores mounting pressures on the media through legal restrictions, digital censorship, economic coercion, and gendered harassment.[4]"

Objective of the Study:

The objective of this report is to simplify and explain the Prevention of Electronic Crimes Act (PECA) and its recent amendments in a way that is accessible to the general public. It aims to make the law understandable for non-legal readers while identifying the implementation challenges it has created for citizens, journalists, and institutions.

The report further seeks to engage key stakeholders which includes members of parliament, policymakers, journalists, digital rights experts, and civil society—to encourage informed dialogue on reforming the law. By presenting evidence-based analysis and recommendations, the study aspires to contribute to ongoing national discussions and promote a balanced, rights-based digital governance framework in Pakistan.

Structure of the Report:

The report is divided into several sections, each examining the *PECA Amendment Act* from a different perspective to provide a comprehensive understanding of its legal, social, gender, and economic implications. Below is a division of the different sections that make up the report:

Evolution of PECA traces the historical development of PECA, from early censorship mechanisms such as the Inter-Ministerial Committee for the Evaluation of Websites (IMCEW) to the formal establishment of PECA in 2016 and its 2025 amendment. It shows how informal content control evolved into a legal regime that institutionalized censorship over digital spaces.

Stakeholder Analysis summarizes reactions from key actors—journalists, the judiciary, civil society, and parliamentarians—regarding the 2025 PECA amendment. It captures widespread opposition from the media and rights groups, the judiciary's critical stance, and the government's justification that the amendments aim to curb misinformation.

Legal Analysis provides an in-depth review of the legal changes introduced by the PECA Amendment Act 2025. It discusses the new institutions created, broader definitions introduced, penalties increased, and reduced judicial oversight.

[4] Pakistan, *Reporters without borders (RSF)*, May 2025, https://rsf.org/en/czountry/pakistan

PECA Gender Analysis examines PECA through a gender and inclusion lens, analyzing its impact on women and transgender persons. It uses data from the Digital Rights Foundation (DRF) and real-life cases to highlight gendered patterns of online harassment, institutional failure in investigation, and misuse of laws.

National Legal Framework explores how PECA interacts with Pakistan's Constitution and overlapping laws such as PEMRA, the Defamation Ordinance, and the Anti-Terrorism Act. It explains how these overlapping provisions create a punitive legal environment

International Legal Framework assesses PECA's compatibility with Pakistan's international human rights obligations, particularly under the ICCPR. It identifies violations of key articles related to freedom of expression, due process, privacy, and assembly—supported by global case law and UN Human Rights Council precedents.

Economic Repercussions analyzes how PECA's human rights implications could affect Pakistan's trade relations, especially its GSP+ status with the European Union.

Conclusion section summarizes the report's findings, noting a deep divide between the government and rights groups over PECA's purpose and impact. It presents three possible pathways forward: repeal, reform through implementation frameworks, or targeted amendments aligning with global digital governance principles.

Recommendation section offers actionable steps categorized under UNESCO's five principles of digital governance—transparency, diverse expertise, checks and balances, openness, and cultural diversity. These recommendations aim to reform PECA into a law that protects citizens without curbing democratic freedoms.

Annexure provides a side-by-side comparison of PECA 2016 and PECA 2025, highlighting specific amendments, concerns, and commentary on problematic provisions. It serves as a technical reference for legal practitioners and policymakers.

Chapter 2

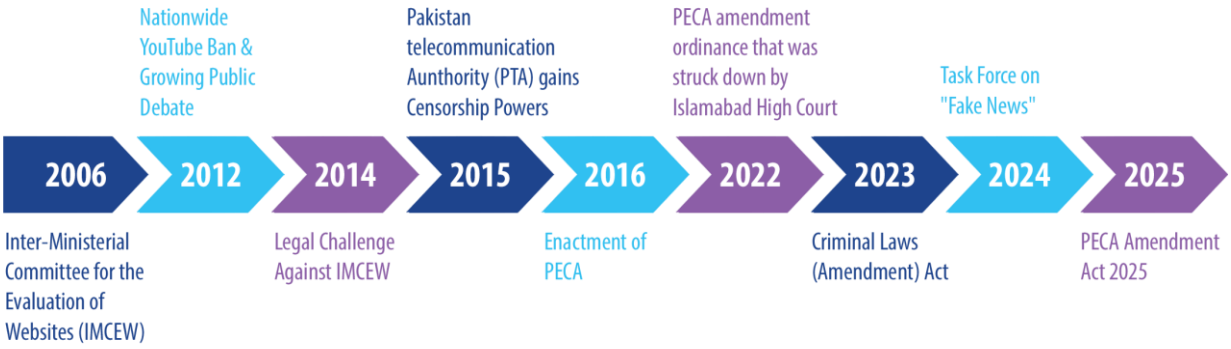
Evolution of PECA: The Rise of Digital Censorship in Pakistan

Censorship rarely begins with silence; it begins with control disguised as protection.

Evolution of PECA:
The Rise of Digital Censorship in Pakistan

The Prevention of Electronic Crimes Act (PECA) is the culmination of years of expanding government control over Pakistan's digital space, evolving from informal censorship mechanisms into a comprehensive legal framework for online regulation.

The roots of online censorship in Pakistan can be traced back to 2006, when the Inter-Ministerial Committee for the Evaluation of Websites (IMCEW) was established through an executive order to regulate online content[5]. Despite lacking legal backing, the IMCEW directed the PTA to block websites, initially targeting blasphemy and pornography, but later expanding it to political speech. In 2012, following the *Innocence of Muslims* controversy, the government imposed a nationwide YouTube ban[6], due to the absence of a legal framework for content takedown requests. This major incident sparked public and parliamentary debate on formalizing internet laws.



Following this, Bolo Bhi – a leading digital rights organization – challenged IMCEW's legitimacy in 2014, leading to a landmark Islamabad High Court (IHC) ruling that halted arbitrary censorship[7]. Under mounting legal pressure, the government dissolved IMCEW in 2015 but granted PTA new censorship powers under the Telecommunications Policy 2015[8], which was widely criticized as unconstitutional.

These developments led to the drafting and eventual enactment of the Prevention of Electronic Crimes Act (PECA) in 2016, legally empowering the Pakistan

[5] "Pakistan's Online Censorship Regime," *Bolo Bhi,* pg 7 https://bolobhi.org/wp-content/uploads/2020/07/Pakistan%E2%80%99s-Online-Censorship-Regime.pdf (accessed from 25 Feb 2025)

[6] "Pakistan blocks YouTube over anti-Islam video," *Al-Jazeera New,* 18.Sep.2012 https://www.aljazeera.com/news/2012/9/18/pakistan-blocks-youtube-over-anti-islam-video https://bolobhi.org/wp-content/uploads/2020/07/Pakistan%E2%80%99s-Online-Censorship-Regime.pdf (accessed from 25 Feb 2025)

[7] "Pakistan's Online Censorship Regime," *Bolo Bhi,* pg 8, https://bolobhi.org/wp-content/uploads/2020/07/Pakistan%E2%80%99s-Online-Censorship-Regime.pdf#:~:text=The%20IMCEW%20became%20a%20prime%20example%20of,constitutionality%20of%20the%20IMCEW%20and%20the%20powers

[8] Ibid

Telecommunication Authority (PTA) to block online content under broad categories such as national security, public morality, and religious sensitivities. This provision granted the PTA unilateral authority to determine what content was unlawful and to direct social media platforms to remove it[9]. This unchecked decision-making power was particularly concerning given that the law criminally punished disinformation.

While PECA originally contained broad provisions criminalizing defamation of "natural persons," the government expanded its scope in 2022 through an amendment ordinance, redefining "person" to include the military, judiciary, and state institutions, effectively criminalizing their criticism. The Islamabad High Court (IHC) however struck down the ordinance in April 2022, deeming it unconstitutional and a violation of free speech[10].

In 2023, PECA was amended once again through the Criminal Laws (Amendment) Act 2023, this time with the objective to extend comprehensive protection against online violence targeting children. The amendment introduced new criminal offences such as online grooming and child trafficking through the addition of Section 22A, thereby strengthening child protection mechanisms in digital spaces[11]. However, alongside these positive reforms, the amendment also expanded the definition of a complainant to include "any person who makes a complaint of any offence… and includes a victim, or an individual having substantial reasons to believe the offence is being committed or likely to be committed, and any authority referring the complaint for investigation."

Previously, only an aggrieved individual could file a complaint, but this expansion allowed any person to initiate complaints, including for defamation against public figures or government entities. This provision has been subsequently misused by investigative bodies.

Despite growing criticism, the government continued to tighten digital regulation. In 2024, it established a task force on "fake news" and anti-state propaganda, setting the stage for stricter controls on online expression[12].

From 2006 to 2025, Pakistan's internet governance transformed from informal government directives into a structured censorship system. PECA 2025 marks the peak of this evolution, turning government control over digital spaces into a

[9] "Prevention of Electronic Crimes Act, 2016," *The Gazette of Pakistan extraordinary published by Authority*, pg 762, Sec 37

[10] Tahir Naseer, " IHC strikes down PECA Ordinance, terms it 'unconstitutional'," Dawn News, 8 April 2022, https://www.dawn.com/news/1684032 (accessed on 25th Feb 2025)

[11] Imran, "PECA and children part 1," *RIPHAH information Portal,* 31 October 2023, https://iportal.riphah.edu.pk/newspaper/peca-and-children-part-i/

[12] "Government forms "fake news" Taskforce after PTI Protest March Deaths," *DRF Archives for Dec 2024*, 3 Dec 2024, https://digitalrightsfoundation.pk/2024/12/page/3/ (accessed on 25th Feb 2025)

formalized and systematic legal framework. Human rights groups warn that these regulations will silence dissent, control media, and limit public debate.

Chapter 3

Stakeholder Analysis

When laws are made without the voices they affect, the first casualty is trust, and the next is democracy.

Stakeholder Analysis

On January 29, 2025, the Government of Pakistan expedited the passage of controversial amendments to (PECA) 2016, bypassing standard legislative scrutiny. The bill was passed through both houses of Parliament -- the National Assembly and Senate -- and received presidential approval within just one week[13]. This rushed process has raised serious concerns about the lack of due diligence, stakeholder consultation, and deliberation in the legislative process.

Digital Rights organizations that sought engagement with the government were met with silence, as no draft of the bill was shared for review or feedback[14].This lack of a participatory approach suggests a potential disconnect between policymakers and the communities most affected by digital regulations.

Below is the reaction of key stakeholders impacted by the PECA Amendment Act 2025:

Journalist

The PECA Act has, for the first time, united the entire journalist community in Pakistan in a collective effort to repeal the law in its entirety. Journalists view the amendments as a direct assault on their profession, suppressing press freedom and free speech. The Joint Action Committee (JAC), comprising all major journalist associations, has unanimously rejected the amendments, labeling it a "black law" and announcing protest rallies nationwide[15].

[13] Nausheen Yousaf, "Peca amendment bill becomes law as president grants assent," The News, 29 Jan 2025, https://www.thenews.com.pk/latest/1277421-peca-amendment-bill-gets-presidents-assent (accessed 30 Jan 2025)

[14] Aziz, Farieha, "Journalists, activists rally against Peca amendment," *The News,* 29. Jan 2025, https://www.thenews.com.pk/print/1277311-journalists-activists-rally-against-peca-amendment (accessed 30 Jan 2025)

[15] Shazia Hasan, "Journalists, rights activists in Karachi reject PECA as black law," 14 feb 2025, https://www.dawn.com/news/1891769 (accessed 15 Feb 2025)

The protests gained momentum as the Pakistan Federal Union of Journalists (PFUJ) called for hunger strike camps across the country[16]. Journalists observed symbolic hunger strikes while people from various walks of life visited the camps to express their solidarity. This collective resistance reflects the deep concern within the media community over the growing restrictions on press freedom.

Reflecting on the decline in press freedom over the past several years, journalist

Arifa Noor stated, "State and private players have been able to tame mainstream media. It has pushed a considerable amount of commentary and reporting onto social media, and this is why they now want to go after social media.[17]"

The context of Noor's remarks is underscored by Pakistan's LOW ranking of 152 out of 180 countries on Reporters Without Borders'[18] mentioned above.

Despite the challenges, journalists remain committed to resisting the amendments, drawing hope from the successful repeal of the 2022 PECA ordinance, which the Islamabad High Court deemed unconstitutional. They believe that refraining from invoking the PECA law is essential to avoid granting it legitimacy. Instead, they advocate for relying on existing overlapping laws, such as the Defamation Ordinance and the Pakistan Electronic Media Regulatory Authority (PEMRA) regulations, to address issues without compromising fundamental rights.

Judiciary

The judiciary has emerged as a key ally in defending freedom of expression and standing in solidarity with journalists. The Islamabad High Court Bar Association (IHC Bar) described the PECA Amendment Act 2025 as a black law, asserting that it suppresses free speech and violates the Constitution[19]. The Bar passed a resolution demanding its repeal, citing contraventions of Articles 8 and 19 relating to fundamental rights[20]. Similarly, lawyers from the Lahore Bar Association protested outside the Lahore High Court, condemning the amendments as an infringement on media freedom and human rights.

[16] Kalbe Ali, " Journalists stage hunger strike to protest amendments to PECA," 13 Feb 2025, https://www.dawn.com/news/1891590 (accessed 15 Feb 2025)
[17] Sarah Zaman, "Pakistani Journalists fear amended cybercrime law will further curb freedoms," 30 Jan 2025, https://www.voanews.com/a/pakistani-journalists-fear-amended-cybercrime-law-will-further-curb-freedoms-/7952337.html (accessed 15 Feb 2025)
[18] Ibid
[19] "Lawyers, journalists unite against PECA," *The Express Tribune*, 31. Jan.2025, https://tribune.com.pk/story/2525644/lawyers-journalists-unite-against-peca?utm_source=chatgpt.com
[20] Ibid

In collaboration with the Pakistan Federal Union of Journalists (PFUJ)[21], several petitions were submitted by the Islamabad High Court Journalists Association (IHCJA)[22] and by prominent journalists, including Hamid Mir, Naseem Zahra, Adnan Haider, and Amir Abbas[23]. These petitions were filed through the IHC Bar Association President Riasat Ali Azad, Advocate Imran Shafiq, and Lawyer Adil Aziz Qazi, collectively challenging the legality of the 2025 amendments.

The Islamabad High Court, under Justice Inaam Ameen Minhas, has taken up the petitions challenging the PECA Amendment Act [24]. The court also summoned the Attorney General of Pakistan to assist in the proceedings. Several petitions remain pending before various high courts across the country, reflecting growing judicial engagement with the constitutional implications of the 2025 Amendment.

Legal experts have expressed frustration over the granular changes introduced through the amendments, which they believe are intended to reverse years of judicial checks aimed at preventing the misuse of the law's provisions.

The establishment of SMPRA tribunals under the amendment, are set to function as a parallel judiciary system, effectively undermining independent judiciary [25]"

Civil Society

The civil society stands firmly aligned with the journalist community in opposing (PECA) 2025, condemning it as a serious threat to freedom of expression and access to information. Human rights organizations and activists have widely criticized the law for its potential to harm fundamental rights and restrict digital freedoms.

Leading activists have consistently spoken out against the Act through major newspapers and institutional websites, with the Human Rights Commission of Pakistan (HRCP) and Bolo Bhi at the forefront of the campaign. Their efforts have

---

[21] Malik Asad, "Peca changes challenged in Islamabad High Court," *Dawn News* https://www.dawn.com/news/1890270 (accessed 3 March 2025)

[22] News Desk, "IHC Journalists Association challenges PECA amendments," *The Express Tribune*, 17.Feb.2025, https://tribune.com.pk/story/2529167/islamabad-high-court-journalists-association-challenges-peca-amendments (accessed 3 March 2025)

[23] Malik Asad, "Anchorpersons challenge PECA tweaks in IHC," *Dawn News* https://www.dawn.com/news/1890552 (accessed 3 March 2025)

[24] "IHC serves notices in another plea against PECA 2025," *Associated Press of Pakistan,* 5.Mar.2025, https://www.app.com.pk/domestic/ihc-serves-notices-in-another-plea-against-peca-2025/ (accessed 8 March 2025)

[25] Aamir Saeed, "'Over our bodies': Pakistani lawyers warn government against establishing 'parallel' judicial system," *Arab News, https://www.arabnews.pk/node/2571988/pakistan* (accessed 12 March 2025)

been amplified by strong statements from international organizations concerned about the impact of the amendments.

The Global Network Initiative (GNI) addressed an open letter to the Prime Minister of Pakistan, highlighting the economic and social consequences of tighter internet regulations. The letter stated:

"At a time when internet speeds have dropped by more than 30% in Pakistan and the country reportedly leads the world in financial losses suffered due to internet and social media outages, GNI urges the Pakistani government to act consistently with its international obligations and avoid creating disproportionate economic and social consequences by placing more stringent controls on the internet.[26]"

Similarly, Amnesty International has voiced grave concerns, warning that the latest amendment to the already draconian PECA law would further tighten the government's grip over Pakistan's heavily controlled digital landscape[27].

Parliamentarians

The PECA Act was first introduced in 2016, with the opposition at that time siding with civil society against the bill. Ironically, every sitting government has supported PECA while in power, while the opposition has consistently opposed it.

In an effort to address concerns, the National Commission for Human Rights (NCHR) consulted with civil society stakeholders and raised their grievances with senior members of the Government, including the Minister of Information. In response, the Minister assured that the PECA 2025 Amendment's primary objective was to combat misinformation and fake news, particularly to protect vulnerable populations such as women and minorities. He asserted that the existing Defamation Ordinance of 2002 was too weak to address heinous crimes committed through social media, necessitating stricter regulations. Critics however argue that the original PECA legislation already addressed issues related to misinformation and online abuse.

The minister also addressed concerns about the violation of due process by assuring that the establishment of tribunals is intended to expedite the trial process. He clarified that these tribunals are positioned at the level of High Courts, and any party

---

[26] "GNI Statement on Ongoing Digital Repression in Pakistan," *Global Network Initiative*, 8.Jan.2025 https://globalnetworkinitiative.org/gni-statement-on-ongoing-digital-repression-in-pakistan/ (accessed 3 March 2025)

[27] "Pakistan:Authorities pass bill with sweeping controls on social media," *Amnesty International*, 24.Jan.2025 https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/ (accessed 3 March 2025)

seeking to appeal can still do so under Article 199 of the Constitution[28], ensuring that the mainstream judicial route remains accessible. Furthermore, he emphasized that the government is willing to consult stakeholders when drafting the rules of various provisions.

The government's stance is that the amendments aim to protect mainstream media and licensed journalists from unregulated voices on social media. However, numerous stakeholders argue that the fundamental structure of the law is inherently flawed, allowing human rights violations within its framework. They assert that introducing new amendments does not address these core issues, but rather adds stricter provisions that further erode constitutional safeguards and diminish public trust in government institutions.

The rushed passage of the bill through Parliament, coupled with the risk of constitutional violations and regulatory overreach, has ignited intense public debate and heightened fears of increased control over free expression.

---

[28] The Constitution of Islamic Republic of Pakistan, (1973), Article 199, https://www.na.gov.pk/uploads/documents/1549886415_632.pdf (accessed 3 March 2025)

Chapter 4

Legal Analysis

A law's true power lies not in its words, but in how it is used—and misused—to shape the boundaries of freedom.[29]

[29] *Author's analysis, informed by principles of rule of law and legal implementation.*

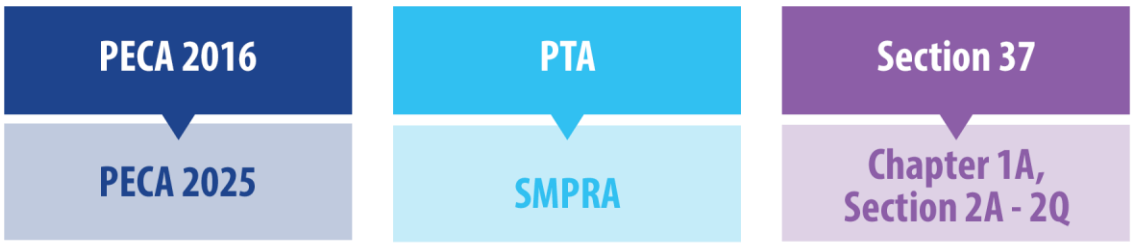
Legal Analysis

The Prevention of Electronic Crimes Act (PECA) has consistently generated legal debate due to concerns about how successive governments have applied it in addressing digital expression and misinformation. Its application in previous cases has raised serious concerns about freedom of expression, privacy, and due process. The PECA (Amendment) Act 2025 further intensifies the regulatory scope of the original 2016 law, introducing more stringent and expansive measures.

Below is an in-depth analysis of the major amendments introduced in various provisions of PECA, contextualized with examples from the implementation of PECA 2016:

Creation of a new Regulatory Authority (SMPRA)

A key change in the 2025 amendment is the creation of the Social Media Protection and Regulatory Authority (SMPRA), which replaces the Pakistan Telecommunication Authority (PTA) from PECA 2016. Under Section 37 of the original legislation, PTA had broad discretion to block or remove online content deemed unlawful[30]. SMPRA, introduced under Section 2A(1), further centralizes government control over digital content.The federal appointment of SMPRA leadership (Section 2D) and the government's ability to issue binding directives (Section 2O) undermines its regulatory independence. The SMPRA Chairperson can also make unilateral content-blocking decisions, subject only to retrospective approval within 48 hours (Section 2G).



Past enforcement practices illustrate these concerns. Satirical and political commentary disseminated through pseudonymous social media pages has, in several instances, been repeatedly restricted or taken down, often citing "local legal requirements" without detailed justification[31]. In other cases, short-video and

[30] " How not to regulate Disinformation: the 2024 general elections and the misregulation of disinformation," *Bolo Bhi*, 5 Feb 2024, https://bolobhi.org/how-not-to-regulate-disinformation-the-2024-general-elections-and-the-misregulation-of-disinformation/ (accessed 20th March 2025)

[31] Kunwar Khuldune Shahid,"Five years of PECA: The law that tried to silence Pakistan," *IFEX*, 9 May 2022, https://ifex.org/five-years-of-peca-the-law-that-tried-to-silence-pakistan/ (accessed 20th March 2025)

livestreaming platforms were subjected to nationwide bans and later restored only after agreeing to comply with content moderation conditions[32].

Digital rights advocates and satirists caution that the establishment of SMPRA risks formalising these practices. In particular, the proposed 48-hour content approval requirement is expected to further institutionalise censorship, significantly constraining spontaneous, critical, and satirical expression in Pakistan's digital space.

SMPRA's mandatory platform registration requirement (Section 2Q) reinforces the authority previously granted under the Removal and Blocking of Unlawful Online Content (RBOUC) Rules, which were introduced to operationalize section 37 of PECA but faced legal challenges. These rules were criticised for exceeding the scope of their parent legislation, as they required social media companies to take direct responsibility for user-generated content deemed unlawful. Under the RBOUC framework, the Pakistan Telecommunication Authority (PTA) was empowered to compel platforms to restrict content, with the threat of nationwide bans for non-compliance.

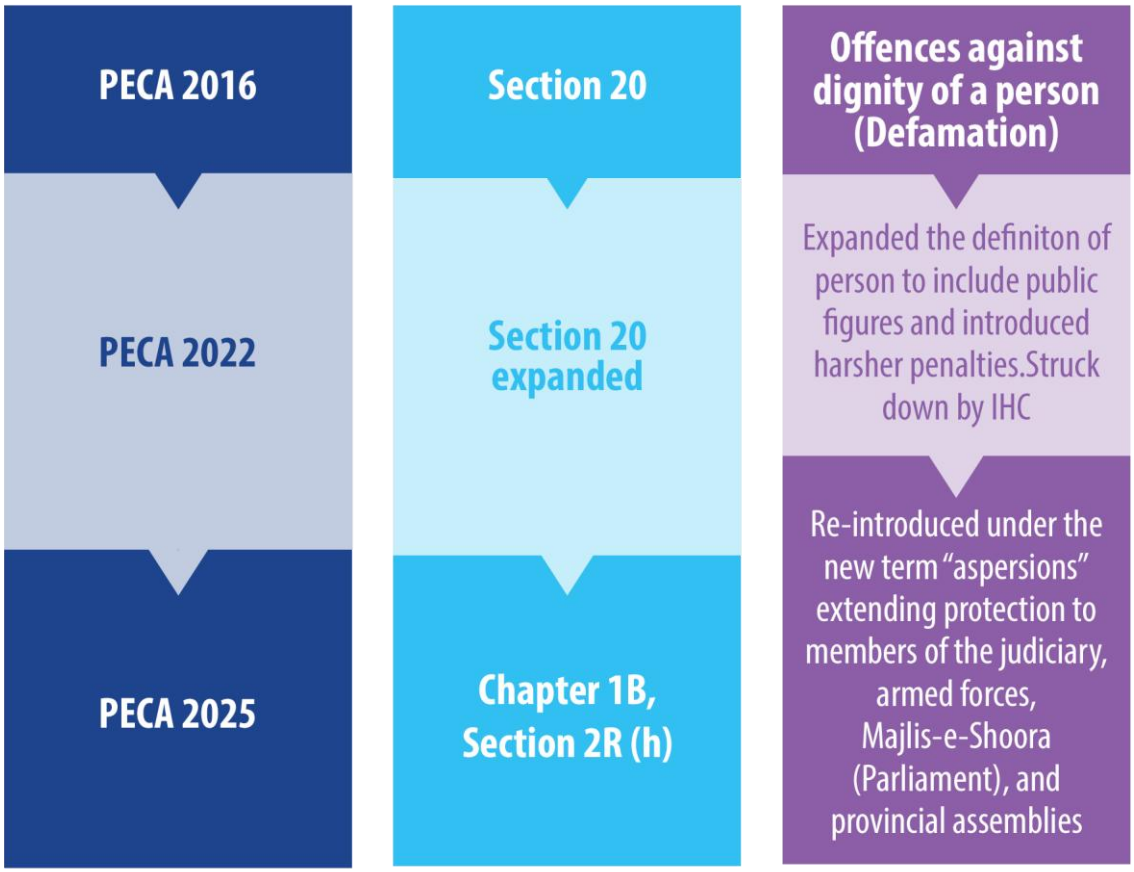
The blocking of X (formerly known as Twitter) was legally justified by the government under these same RBOUC Rules, despite ongoing constitutional challenges and public criticism over their vague and expansive scope [33].

Expansion of Legal Definitions and Broad Interpretation

The 2025 amendments to PECA effectively reintroduce defamation, which had been previously struck down in 2022 with the repeal of (Section 20) of PECA 2016 due to constitutional concerns[34]. This has been done through the introduction of a new term, "aspersion," broadly defined as the act of spreading "false and harmful information damaging an individual's reputation." Additionally, the amendments significantly expand the definition of "unlawful content" in (Section 2R) to include information that is considered false based on a "sufficient reason to believe it is false," and to encompass "aspersions against any person," including members of the judiciary, armed forces, Majlis-e-Shoora (Parliament), and provincial assemblies. These broad

[32] "Pakistan Telecommunication Authority (PTA) lifts ban on Bigo live," *PR Newswire,* 01.Aug.2020, https://en.prnasia.com/releases/apac/pakistan-telecommunication-authority-pta-lifts-ban-on-bigo-live-287008.shtml, (accessed 20th Feb 2025)
[33] Farieha Aziz, "The ministry of (dis)information and the ban on X," *Dawn News Prism,* 25.April.2024, https://www.dawn.com/news/1828972 (accessed 20th Feb 2025)
[34] Tahir Naseer, "IHC Strikes down PECA Ordinance, terms it 'unconstitutional'," *Dawn News,* 8 April 2022, https://www.dawn.com/news/1684032 (accessed 20th Feb 2025)

formulations further blur the line between legitimate criticism and punishable offense, deepening fears of overreach.



Journalists have previously been targeted for defamation under (Section 20), for commentary on public institutions. In one case the charges were dismissed after over a month of court hearings, public condemnation, and support from journalists and rights groups[35].

However, with the new amendments introducing broader definitions, the government now has legitimate legal authority to control voices that criticize it.

The 2025 amendments also expand the definition of a "complainant," in (Section 2(via)) allowing third parties without direct harm to file legal actions.

The expansion of the definition of complainant undermines previous rulings, like in the case of an Islamabad based journalist, who was accused of defamation by a private individual. The FIR was vague, and the case was dismissed due to lack of

[35] Shafi Baloch, " Case against journalist Shahzeb Jilani quashed due to lack of evidence," *Dawn News*, 18 May 2019, https://www.dawn.com/news/1483053 (accessed 20th March 2025)

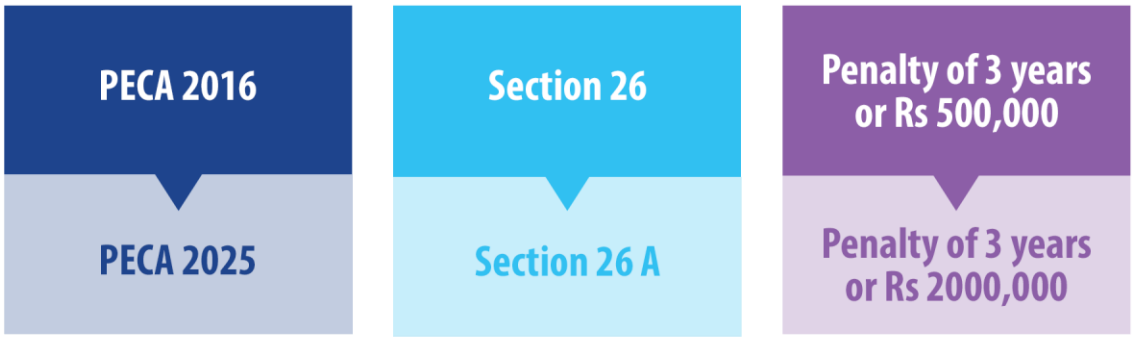
evidence[36]. However, the new amendments enable third parties to file complaints as proxies, potentially leading to politically motivated actions against journalists and activists.

Moreover, the amendments now includes a definition of social media platforms in (Section 2 (xxviiib)) which includes "communication channels" like VPNs under social media regulations, allowing the state to block VPNs used to access restricted platforms, such as X (formerly Twitter)[37]. This increases censorship and restrictions on digital access, further tightening control over online expression.

Standardizing the scope of Criminalization

A particularly contentious provision in PECA 2025 is Section 26(A), which introduces stringent penalties for the dissemination of false information that causes "panic or unrest." The punishments include up to three years of imprisonment, a fine of Rs. 2 million, or both. Such high penalties create a chilling effect [38] on free speech, discouraging individuals from exercising their fundamental right to express opinions due to fear of legal repercussions.The disproportionate nature of these punishments contradicts international best practices, where defamation and misinformation laws -unless they harm human life, are typically handled through civil remedies rather than criminal prosecution.

While PECA 2016 also prescribed penal measures—ranging from Section 3 (3 months' imprisonment or a Rs. 50,000 fine for unauthorized access to information) , to Section 11 (14 years' imprisonment or a Rs. 50 million fine for cyberterrorism) —these provisions have been used against many who criticised government institutions.



[36] "Section 20 of Pakistan's Prevention of Electronic Crimes Act:Urgent Reforms needed," *Trial Watch Fairness Report A Clooney Foundation for Justice Initiative*, Sep 2023, pg 10 https://cfj.org/wp-content/uploads/2023/10/Pakistan_PECA-Report_September-2023.pdf (accessed 20th March 2025)
[37] Farieha Aziz, " The ministry of (dis)information and the ban on X," *Dawn Prism*, 25 April 2024, https://www.dawn.com/news/1828972#:~:text=Local%20law%20and%20the%20rules%20don't%20apply&text=These%20rules%20were%20introduced%20by,for%20the%20restriction%20on%20X. (accessed 20th March 2025)
[38] In a legal context, a chilling effect is the inhibition or discouragement of the legitimate exercise of natural and legal rights by the threat of legal sanction.

Similarly, Sections 9 (glorification of an offence), 10 (cyberterrorism), and 11 (hate speech) have been invoked in cases against journalist Bilal Farooqi[39]. Many of these cases—either closed or still pending—were registered between 2019 and 2020. The threat of harsh penalties not only discourages free expression but also emboldens institutional impunity, making it harder for individuals to speak truth to power without facing serious personal risk.

A New Investigative Body: National Cyber Crime Investigation Agency (NCCIA)

Under Section 29 of the PECA Amendment Act 2025, the Federal Investigation Agency's cybercrime wing has been replaced by the National Cyber Crime Investigation Agency (NCCIA). While the creation of a specialised body suggests institutional reform, the amendment does not address the structural deficiencies that characterised cybercrime enforcement under the FIA, particularly concerning procedural safeguards, accountability, and respect for due process.

Concerns stem from documented instances involving journalists engaged in critical reporting, where cyber-related inquiries escalated into informal summons by federal authorities, including requests to appear before counter-terrorism units without written grounds at the initial stage. In at least one such instance, judicial intervention by a superior court was required to restrain further contact by the investigative authority. These incidents, documented by international press-freedom organisations, raised serious questions regarding intimidation, procedural overreach, and the misuse of investigative powers in matters involving expression.

With an absence of explicit safeguards and oversight mechanisms in the current amendment, there is a credible risk that the NCCIA may inherit and reproduce similar practices, including coercive investigation methods, lack of transparency, and violations of privacy and due-process rights. Detailed documentation of these patterns is available through publicly accessible reporting by international media watchdogs and human-rights organisations.

Furthermore, many journalists have raised concerns about FIA's inefficiency and lack of resources.

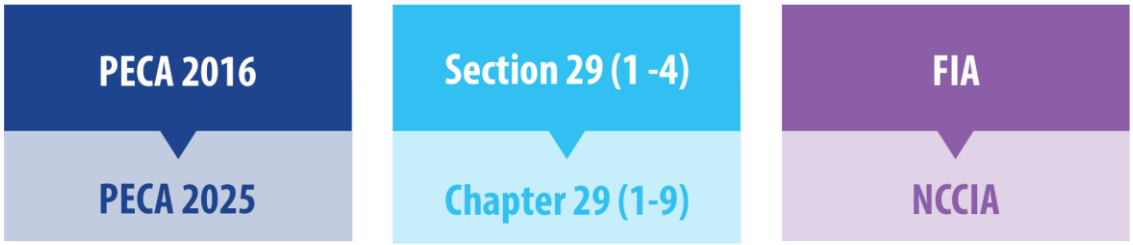
In one reported instance, a woman journalist filed a complaint with the Federal Investigation Agency in 2018 after experiencing sustained online harassment, including abusive messages, threats of sexual violence, and the non-consensual circulation of personal images. Despite repeated follow-ups through both online portals and in-person visits, no substantive action was taken by the authorities[40].

[39] Farieha Aziz, "Project PECA III: What goes around,comes around," *Dawn Prism,* 16. Dec 2022, https://www.dawn.com/news/1726162 (accessed 25 Feb 2025)

[40] Farieha Aziz, "Rethinking PECA: How cybercrime laws are weaponised against women," Human Rights Commission Pakistan, Jan 2022, pg 10 (accessed 20th Feb 2025)

Ultimately, the complainant withdrew the case, citing frustration and lack of institutional response [41].

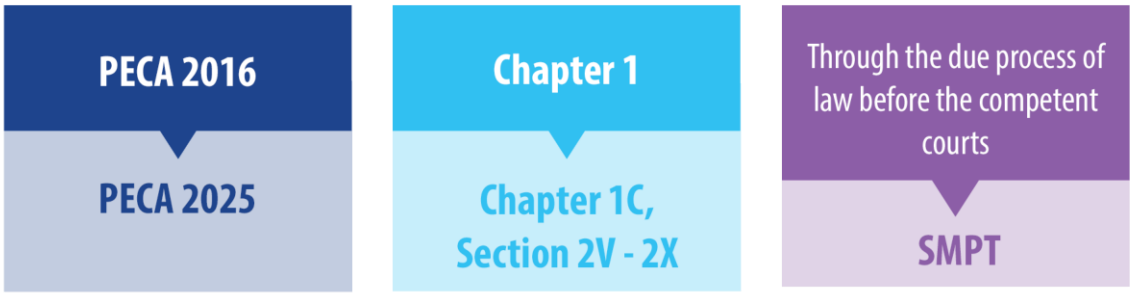
This highlights the systemic issues of inefficiency and neglect within the FIA, which raises doubts about whether the newly established NCCIA will effectively address these concerns.



Restricting Judicial Oversight and Due Process

PECA 2025 introduces significant restrictions on judicial oversight and due process by adding an entirely new Chapter 1C, which establishes Social Media Protection Tribunals. These tribunals now replace traditional judicial forums for appeals against content removal decisions, limiting the right of recourse to only the Supreme Court. This change substantially reduces access to judicial remedies, especially for individuals and smaller entities lacking the resources to pursue expensive litigation.

The introduction of SMPT undermines the principles of fundamental justice that were previously upheld through High Court interventions, particularly in cases challenging executive overreach and FIA intimidation under PECA 2016. By shifting adjudication to specialized tribunals with narrower jurisdiction and limited procedural safeguards, the amendment makes the legal process more complex and costly. As a result, access to fair and timely judicial recourse becomes increasingly difficult, diminishing the public's ability to challenge censorship or defend against unlawful content takedowns.



[41] Afra Fatima, "From screens to streets: women vloggers in Pakistan face harassment everywhere," 30.12.2025, https://digitalrightsmonitor.pk/from-screens-to-streets-women-vloggers-in-pakistan-face-harassment-everywhere/#:~:text=So%2C%20she%20decided%20to%20file,to%20shame%20his%20thinking%20publicly. (accessed 20th March 2025)

In 2020, journalist Arshad Sulehri's home was raided by the FIA. He challenged the illegal search in the Islamabad High Court, leading to a landmark ruling in *Arshad Sulehri v. Federation of Pakistan*. The court emphasized the need for special guidelines when acting against journalists, recognizing the profound impact on press freedom and independence. It also noted that creating fear of arrest undermines a journalist's independence and is unacceptable in a constitutionally governed society[42]. These examples highlight how an independent judiciary serves as a check on excessive power, offering citizens hope for justice. With the establishment of SMPRA, that hope is further diminished.

[42] Muhammad Aftab Aslam, " It's raining offences," The News on Sunday, 6 March 2022, https://www.thenews.com.pk/tns/detail/938563-its-raining-offences (accessed 20th March 2025)

Chapter 5

PECA Gender Analysis

Digital spaces mirror our society: where patriarchy thrives offline, it finds new weapons online.

PECA Gender Analysis

One objective of PECA was to protect women from cyber harassment and create a safer digital environment that encourages their participation in technology and online spaces. However, in practice, the implementation has exposed persistent gender gaps. This vulnerability is further exacerbated by deep-rooted patriarchal norms and widespread misogyny, which continue to shape both online and offline experiences of women in Pakistan.

This chapter analyses PECA through a gender lens, identifying where the law has successfully provided recourse to victims of online violence and where its misuse has resulted in further victimization. Drawing upon official data from the Digital Rights Foundation (DRF) Cyber Harassment Helpline, judicial precedents, and field reports from the Human Rights Commission of Pakistan (HRCP), the report presents findings and concrete policy recommendations to align PECA with Pakistan's constitutional protections and international human rights obligations.

Digital Gender Divide and Vulnerability

The 2024 Report of the United Nations Secretary-General identifies that one of the three emerging global challenges is a growing backlash against women's rights[43], warning that gender equality is increasingly being reversed across digital and public spaces. This global trend is mirrored in Pakistan, where women continue to face significant barriers to digital inclusion. Only about 33 percent of women have access to mobile broadband services, compared to 53 percent of men. This digital exclusion leaves many women unaware of the tools needed to protect themselves from online abuse in a society where patriarchal norms already constrain female agency.

Technology-facilitated gender-based violence (TFGBV) encompasses a broad range of abuses including cyberstalking, online sexual harassment, doxxing, defamation, and the non-consensual sharing of intimate images. The United Nations Population Fund (UNFPA) defines TFGBV as "an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated or amplified in part or fully by the use of information and communication technologies or digital media against a person on the basis of gender."

Data from the Digital Rights Foundation's Cyber Harassment Helpline (0800-39393) indicates that women consistently make up the majority of complainants. Out of approximately 20,000 recorded cases, 58 percent were filed by women, with most victims between 18 and 30 years of age. This demographic pattern suggests that

[43] "UNGA 79: Intensification of efforts to eliminate all forms of violence against women and girls," *UN Women,* 2024, https://www.unwomen.org/sites/default/files/2024-10/a-79-500-sg-report-ending-violence-against-women-and-girls-2024-infographic-and-recommendations-en.pdf

younger women who are more active online are both more exposed to harassment and more willing to report it. In Pakistan about one third of female students and nearly half of working women report harassment online[44]. Many are forced to consider leaving school or the workforce entirely.

Despite the creation of this legal framework, the experience of women and girls online remains precarious. Rather than serving as a shield, PECA has in several instances been transformed into a sword that is used to suppress expression, silence victims, and deter the reporting of harassment[45].

Provisions of PECA Relevant to Women

The sections below outline the key provisions relevant to women's protection under PECA and areas where further strengthening may be required:

Section 24 (cyberstalking):

Section 24 of PECA criminalizes sustained online harassment, intimidation, or surveillance. It covers behaviours such as repeated unwanted contact, coercive monitoring, and the unauthorized sharing of images or videos that cause distress. This provision directly addresses the most common forms of online abuse experienced by women such as stalking, sextortion, and non-consensual sharing of private images.

Courts have demonstrated willingness to apply this section effectively. In 2022, the Peshawar High Court upheld a conviction for online stalking and harassment, affirming custodial sentences and fines[46]. Earlier, in 2018, another offender received eight years' imprisonment for blackmailing a woman via Facebook. These judgments show the potential of Section 24 when implemented correctly as mentioned in legal firm's guide on Women's Safety from Cyber Crimes[47].

However, the number of prosecutions remains low compared to the scale of abuse. Many women hesitate to file complaints due to fear of stigma, lack of female officers, and concerns about data privacy during investigations.

Section 22: (Child Protection and online exploitation)

Section 22 is among PECA's strongest provisions. It criminalizes the production, possession, and dissemination of child sexual abuse material (CSAM), a crime that disproportionately affects girls. According to data from the NGO Sahil, 3,364 cases of

[44] "AI Governance and Gender Sensitive Policies," UN Reports (2024).
[45] Annual Cybercrime and Harassment Report FIA Pakistan (2023).
[46] Peshawar High Court, *Judgment in QP 50-2022*, available at: https://peshawarhighcourt.gov.pk/PHCCMS/judgments/QP50-2022---FFFRRR.pdf (accessed 12.Oct 2025).
[47] "Women's safety from cybercrimes in pakistan," DSI law Associates, https://drshahabimamlawassociates.co/womens-safety-from-cyber-crimes-in-pakistan/

child sexual abuse were reported in 2024—of which 53 percent involved female victims[48].

Section 22 classifies these crimes as non-bailable, non-compoundable, and cognizable, ensuring swift state intervention. Notably, Pakistan's first conviction under this section occurred in 2018, when a Lahore court sentenced Sadat Amin to seven years in prison and fined him Rs. 1.2 million for participation in an international child pornography racket[49].

The section's integration into the Anti-Rape Act ensures that such cases are handled under enhanced procedural safeguards. Nevertheless, resource constraints, digital forensic limitations, and coordination gaps with international agencies continue to impede effective enforcement.

Section 21 (Offences Against Modesty / Image Based Abuse):

Section 21 criminalizes offences against a person's modesty or privacy, including the non-consensual distribution of intimate images, online blackmail, and sexual extortion. This section is essential for addressing "revenge porn" and other forms of image-based sexual abuse offences that carry devastating social repercussions for women in Pakistan's conservative environment.

Courts have successfully invoked Section 21 in several high-profile cases. In 2021, a Karachi court sentenced a university professor to eight years' imprisonment for creating fake social media profiles to harass a female colleague[50]. In another 2025 case, a man received six years in prison for misusing a woman's photographs online to damage her honour[51].

However, Section 21 also reveals significant gaps. It lacks explicit recognition of consent, creating ambiguity in cases where intimate material is initially shared voluntarily but later weaponized. Moreover, while the section is cognizable—empowering the state to prosecute—victims often have to bear legal costs and navigate proceedings without guidance from the FIA.

Alarmingly, this provision has also been weaponized against women journalists. In February 2025, Section 21 of PECA was invoked in a controversial manner when an FIR was registered under Section 21(1)(d) against four women journalists who administered a WhatsApp group titled "NPC Women Journalists Caucus." The case stemmed from a private dispute between an ex-husband and ex-wife that became

[48] Ikram Junaidi, " Over 3350 child abuse cases reported across Pakistan in 2024:report," Dawn News, 6.may.2025, https://www.dawn.com/news/1908682

[49] Rana Bilal," Sargodha man handed 7 year jail term, Rs1.2m fine in Pakistan's first ever child-pornography conviction," *Dawn News,* 26.April.2028, https://www.dawn.com/news/1404010?utm

[50] Naeem Sahoutara, "KU professor sentenced to 8 years imprisonment for harassing female teacher online," *Dawn News*, 16.Jun.2021 https://www.dawn.com/news/1629708?utm_source

[51] Sumair Abdullah, "Karachi man sentenced to six years in prison for creating fake facebook accounts to balckmail woman," *Dawn News*, 22.Sep.2025, https://www.dawn.com/news/1943725?utm_source

public. The complainant, identified as Nasir Khan Khattak, approached the Federal Investigation Agency (FIA) alleging online harassment and defamation, and implicated the four journalists in the alleged defamation on social media. Observers have noted that Section 21 was potentially misapplied in this instance, as the matter primarily pertained to personal defamation. Concerns were raised that the provision was used because it is cognizable, allowing an FIR to be registered without prior court approval[52].

Section 20 (Offences Against Dignity of a Natural Person):

Section 20 criminalizes false or defamatory information that harms the "dignity of a natural person." While originally intended to protect individuals from online slander, this section has become the most controversial part of PECA. It lacks gender-sensitive language and has been repeatedly misused against women who report harassment or express opinions online especially when they challenge powerful actors[53].

During the #MeToo movement, Section 20 was employed against women who named their alleged harassers. The most notable example was the Ali Zafar–Meesha Shafi case, in which the FIA registered cybercrime complaints against women who supported Shafi's harassment allegations. This use of criminal law highlights how

[52] Ramna Saeed, "4 women journalists face PECA charges, union calls it intimidation," Digital Rights Monitor, 19 August 2025, https://digitalrightsmonitor.pk/peca-cases-against-npc-women-journalists/

[53] "Prevention of Electronic Crimes (Amendment) Act 2025," *Human Rights Comission of Pakistan (HRCP)*, Feb 2025, https://hrcp-web.org/hrcpweb/wp-content/uploads/2020/09/2025-LWC10-PECA-Amendment-Act-2025.pdf

Section 20 has been transformed from a protective tool into a mechanism of control[54].

Recognizing these risks, the Islamabad High Court in 2022 struck down amendments that expanded Section 20's scope, declaring them inconsistent with constitutional guarantees of free expression[55]. Nonetheless, the section's broad wording continues to invite misuse.

Section 33 and 34 (Investigative Powers and Privacy Concerns):

Sections 33 and 34 grant investigators the power to search, seize, and access data with minimal oversight. While these powers are vital for law enforcement, they carry gender-specific risks. Women who report harassment often must surrender personal devices containing private images, family conversations, and other sensitive material.

Several instances reveal a systemic pattern of pre-trial coercion and procedural misconduct within cybercrime investigations.

In multiple TFGBV cases, both the complainant and the accused have reported being pressured by FIA officials to surrender personal electronic devices and disclose passwords—often without a formal warrant or judicial authorization. While PECA's Section 33 requires that searches and seizures adhere to judicial oversight and principles of proportionality, in practice this requirement is frequently bypassed, especially in cases framed as urgent.

Once in possession of the devices, investigators have been documented browsing through entire photo galleries, message histories, and private communications unrelated to the alleged offence. HRCP's 2023 report "Human Rights and Digital Policing in Pakistan" cited multiple incidents where female complainants' personal data—family photos, private chats, and documents—were copied or viewed by multiple officers, sometimes in the presence of others, in clear violation of privacy and chain-of-custody protocols.

In some cases, sensitive data from victims' phones was leaked informally within FIA offices or to third parties**,** either to pressure the accused into a settlement or to force the complainant to withdraw the case. For example, a Lahore-based woman who reported sexual extortion under Section 21 told DRF's helpline that after submitting her phone for evidence, her private photos reappeared on secondary WhatsApp

[54] Farieha Aziz,"Rethinking the Prevention of Electronic Crimes Act: How cybercrime laws are weaponized against women," *Human Rights Comission of Pakistan (HRCP*), Jan 2022, https://hrcp-web.org/hrcpweb/wp-content/uploads/2020/09/2022-Rethinking-PECA-How-cybercrime-laws-are-weaponised-against-women.pdf

[55] "PECA S.20 Amendment will not stand, Attorney General tells Islamabad High Court," *Digital Rights Monitor,* 16.October 2025, https://digitalrightsmonitor.pk/peca-s-20-amendment-will-not-stand-attorney-general-tells-islamabad-high-court/

groups linked to FIA staff—causing severe distress and forcing her to drop her complaint[56].

HRCP's field investigation in Karachi and Lahore further recorded instances where families of women complainants were contacted without consent once investigators viewed private information, leading to familial backlash and pressure to keep quiet. In other complaints, women said they were threatened with countersuits or moral policing if they did not cooperate with the officers' demands[57].

These patterns amount to a form of secondary victimisation, where the process itself reproduces the trauma of abuse. They also undermine public trust in PECA enforcement: survivors become reluctant to approach authorities for fear that their private lives will be exposed or used against them.

Although PECA and its procedural rules nominally require "proportionality, integrity and chain-of-custody" in searches and seizures, these standards are not gender-specific and lack enforcement mechanisms. There are no internal audit systems, no disciplinary consequences for privacy breaches, and minimal representation of women officers in cybercrime units. As a result, women victims of online harassment face a double jeopardy—first at the hands of the perpetrator, and then within the very institutions meant to protect them.

While Sections 21, 22, and 24 of PECA provide crucial safeguards against image-based abuse, CSAM, and stalking, the law's credibility is undermined by the repeated misuse of Sections 20 and 21 against women journalists and survivors, as well as by enforcement flaws under Sections 33 and 34 that enable intrusive investigations and deter reporting.

Structural and Regional Disparities

Punjab reports the highest number of TFGBV cases—owing partly to its population size and stronger awareness campaigns. However, the majority of complaints arise from districts without local FIA cybercrime units. This leaves victims, particularly women in rural areas, without timely access to justice. Sindh and Balochistan have also witnessed an increase in cases, suggesting either improved awareness or a growing prevalence of digital abuse.

Women journalists and transgender persons represent two especially vulnerable groups. Female reporters face organized online campaigns that include fake sexual content and doxxing, while transgender individuals endure targeted hate speech with limited legal recourse.

---

[56] https://digitalrightsfoundation.pk/wp-content/uploads/2024/04/DRFs-Cyber-Harassment-Helpline-Report-2023.pdf?

[57] "Prevention of Electronic Crimes (Amendment) Act 2025," *Human Rights Comission of Pakistan (HRCP)*, Feb 2025, https://hrcp-web.org/hrcpweb/wp-content/uploads/2020/09/2025-LWC10-PECA-Amendment-Act-2025.pdf

Digital Hate and Gender- diverse Community

While PECA provides limited protection for women from online abuse, *the protection of transgender individuals remains largely neglected.*Transgender persons continue to experience severe and targeted forms of online harassment, including impersonation, doxxing, extortion, and coordinated shaming campaigns. A notable example is the surge in digital hate speech targeting the transgender community in 2022. The exclusion of a transgender activist and policy specialist from the panel of speakers at a TEDx conference spilled into an online hate campaign—not only against the individual but against the entire transgender community[58]. Transgender persons remain easy targets for online abuse due to deep-rooted marginalisation and societal stigma at the national level.

When these victims seek help from the NCCIA, they are often ridiculed, misgendered, or dismissed, with their complaints trivialized as "social issues" rather than recognized as punishable cyber offences. The example of Laiba Nayab, a transgender from Khyber Pakhtunkhwa, highlights NCCIA's failure to protect vulnerable communities from online violence. After Laiba's social media photos were stolen and circulated with derogatory captions, she began receiving death threats and extortion messages. Despite filing a formal complaint, law enforcement failed to act; officers allegedly mocked her gender identity and told her to "stay offline" rather than pursue the perpetrators. The intimidation she faced both online and at the hands of investigators forced her to leave her home province for safety, underscoring how digital harassment against transgender persons often escalates into real-world violence[59]. Many others describe being advised simply to withdraw from social media instead of receiving legal protection or case registration.

Other times the investigator officers encourgae parties to reach a settlement, allowing perpetrators to evade accountability. A notable example is the high-profile case of Peshawar's transgender activist, Dolphin Ayan, whose intimate videos were shared online. Despite an extensive investigation, the case ultimately concluded in a private settlement, reflecting systemic gaps in ensuring justice for victims of digital abuse[60].

Such responses not only deny transgender citizens equal access to justice but also contravene Pakistan's constitutional guarantees of equality under Article 25 and the Transgender Persons (Protection of Rights) Act, 2018, which requires state institutions to uphold their safety and dignity. The NCCIA's lack of trained personnel, designated focal points, and gender-inclusive procedures reflects a systemic

[58] Hyra Basit,Anmol Sajjad, Ayesha Sarwar, Ayesha Nooral, "Cyber Harassment Helpline 2023," Digital Rights Foundation (DRF), 2023 https://digitalrightsfoundation.pk/wp-content/uploads/2024/04/DRFs-Cyber-Harassment-Helpline-Report-2023.pdf?

[59] Islam Gul Afridi, "She danced online and he came with a gun," *Digital Rights Monitor,* 16 October 2025, https://digitalrightsmonitor.pk/socialmediaprofiles-turned-deadly-trans-cyber-harassment-kp/

[60] Ibid

institutional failure—one that leaves transgender individuals especially vulnerable to digital violence and effectively excluded from the country's cyber-justice framework.

Since 2010, the Manzil Foundation has recorded 1,800 cases of violence against transgender Pakistanis; 158 have been murdered. This year's first six months saw eight killings.The experiences of transgender citizens illustrate the urgent need for gender-sensitive protocols and accountability mechanisms within NCCIA so that all citizens—regardless of gender identity—can access justice without fear or humiliation.

Chapter 6

National Legal Framework

In a nation of many laws, justice depends not on their number, but on their harmony.

National Legal Framework

The Constitution of Pakistan, as the supreme law of the land, establishes the fundamental legal framework within which all legislation must operate. However, (PECA) 2025, drafted in the context of national security, appears to undermine several constitutional rights in the course of combating cybercrime. In constitutional terms, the wide application of PECA may infringes upon key fundamental rights, including Article 4, which ensures the right to be treated in accordance with the law; Article 10-A, which guarantees the right to a fair trial and due process; Article 14, which upholds the right to privacy; Article 19, which protects the freedom of speech and expression; and Article 19-A, which secures the right to access information on matters of public importance [61].

In addition to its constitutional challenges, PECA is an intricate blend of regulatory, administrative, and criminal laws that frequently overlaps with existing legislation, such as the Pakistan Electronic Media Regulatory Authority (PEMRA) Ordinance and the Defamation Ordinance. In many instances, sections of PECA are applied alongside provisions of the Pakistan Penal Code (PPC) and the Anti-Terrorism Act (ATA), particularly in cases involving speech about public officials and state institutions. This overlapping and fusion of legal provisions create a complicated framework that not only blurs the boundaries between different legal domains but also raises concerns about civil liberties and the protection of fundamental rights.

Content regulatory laws such as PEMRA and PECA were introduced to combat disinformation. However, both lack clear and specific definitions that distinguish disinformation from misinformation. The distinction in PEMRA is particularly problematic due to the subjective nature of intent and verification. Proving intent to harm is inherently challenging, and the term *"verifiably false"* remains undefined, creating ambiguity about what qualifies as verified information[62]. PECA complicates this further by introducing the concept of *aspersion,* defined as *"spreading false and harmful information which damages the reputation of a person[63]."* However, PECA's criminalization of aspersion does not clearly address intent, making it difficult to differentiate between misinformation (unintentional) and disinformation (intentional).

By introducing the term *"reputation of a person"* in the definition of aspersion, PECA encroaches upon the domain of defamation law. Both the Defamation Ordinance, 2002, and PECA, 2025, address harm to reputation caused by defamatory content,

[61] "The Constitution of Islamic Republic of Pakistan, 1973," Article 199, https://www.na.gov.pk/uploads/documents/1549886415_632.pdf (accessed 3 March 2025)
[62] " Pakistan Electronic Media Regulation Authority (Amendment) Act, 2023," *The Gazette of Pakistan extraordinary published by Authority*, pg 769, Amendments of section 2, Ordinance XIII of 2002, (iii)
[63] " Prevention of Electronic Crimes (Amendment) Act,2025," *The Gazette of Pakistan extraordinary published by Authority*, pg 24, Amendment of section 2, Act XL of 2016 (iiia)

but they differ significantly in scope, enforcement, and penalties. The Defamation Ordinance primarily aims at civil compensation, offering remedies like compensatory damages and apologies. Courts can order compensation starting from a minimum of Rs. 50,000, with higher amounts applicable for the originator in certain cases[64]. In contrast, PECA introduces criminal penalties that make it a far more forceful deterrent. Under Section 26A of PECA, punishment for offenses against the dignity of a natural person includes imprisonment of up to three years, a fine of up to one million rupees, or both[65]. This shift from civil to criminal consequences makes PECA disproportionately punitive compared to the Defamation Ordinance.

By introducing punitive measures, PECA has effectively transformed into a criminal law, frequently used in conjunction with the Pakistan Penal Code (PPC) and the Anti-Terrorism Act (ATA). This convergence creates a complex and layered legal framework that significantly amplifies the consequences of alleged offenses.

One of the most concerning aspects of PECA's implementation is its alignment with PPC provisions that criminalize speech and expression. For instance, PECA criminalizes hate speech (Section 11) and cyberstalking (Section 21), which may involve defamatory or objectionable content shared online. These offenses are often linked with sections of the PPC, particularly Sections 499–502, which pertain to defamation[66]. This alignment allows the state to pursue criminal charges instead of civil remedies, thereby intensifying the legal repercussions.

PECA is frequently applied alongside PPC provisions such as Sections 131, 133, and 153[67]. Section 153 criminalizes speech intended to incite rioting or disrupt public order, while Sections 131 and 133 explicitly prohibit speech against the armed forces. These sections are framed to address incitement, making it illegal to provoke or incite mutiny, hostility, or contempt toward military institutions. The inclusion of these PPC sections alongside PECA offenses criminalizes speech that may be perceived as critical of state institutions, even when expressed in a non-violent or opinionated context.

There is also a significant overlap where digital acts under PECA are linked to terrorist motives under the Anti-Terrorism Act (ATA), leading to dual prosecution. This raises concerns of double jeopardy, where an individual could be penalized twice for the same offense.

---

[64] " The Defamation Ordinance no LVI of 2002," *The Pakistan Code Minsitry of Law and Justice*, pg 4, Section 9 https://pakistancode.gov.pk/pdffiles/administrator741de22e068540827860696207 9d12b2.pdf accessed 3 March 2025)

[65] " Prevention of Electronic Crimes (Amendment) Act,2025," *The Gazette of Pakistan extraordinary published by Authority*, pg 36, Section 26A

[66] Farieha Aziz, "Project PECA 1: How to silence a Nation," *Dawn News,* 12.Dec.2022 https://www.dawn.com/news/1725805/project-peca-i-how-to-silence-a-nation (accessed 5.March.2025)

[67] Ibid

A Senior journalist voiced strong criticism of these overlapping and excessively punitive laws, stating that they appear to be inherently anti-people. He remarked that even the Anti-Terrorism Act (ATA), which seemed reasonable at first, was later weaponized against activists[68]. Speaking about PECA, he highlighted that the right to know is a fundamental human right, and PECA directly contradicts that by curbing freedom of expression and access to information. Some cases illustrate how cybercrime laws have been used alongside PPC and anti-terrorism provisions, blurring the line between regulating online spaces and restricting critical speech[69]. A more balanced approach is needed to ensure digital regulations align with Pakistan's constitutional commitments while safeguarding freedom of expression and access to information.

[68] Shazia Hasan, "Jouranlists, rights activists in Karachi reject PECA as black law," *Dawn News*, 14.Feb.2025, https://www.dawn.com/news/1891769 (accessed 5.March.2025)

[69] Farieha Aziz, "Project PECA 1: How to silence a Nation," *Dawn News,* 12.Dec.2022 https://www.dawn.com/news/1725805/project-peca-i-how-to-silence-a-nation (accessed 5.March.2025)

Chapter 7

International Legal Framework

Freedom of expression is not a domestic privilege; it is a global standard that binds us to justice and accountability.

International Legal Framework

The (PECA) Amendment Act 2025 has raised serious concerns about its compliance with Pakistan's international human rights obligations, particularly under the International Covenant on Civil and Political Rights (ICCPR). The United Nations Human Rights Council (UNHRC) has repeatedly emphasized that any digital regulation, particularly those targeting disinformation, must align with international human rights law and adhere to principles of legality, legitimacy, necessity, and proportionality. However, several key provisions of PECA directly conflict with ICCPR standards, as demonstrated by past international cases highlighted by Human Rights Council (HRC).

Key ICCPR Articles Contravened	
Article 14 - Fair Trial	Ensures the right to a fair, impartial, and independent judicial process.
Article 17 - Privacy	Protects individuals from unlawful interference with privacy and reputation.
Article 19 - Freedom of Expression	Guarantees the right to hold opinions and share information freely.
Article 21 - Peaceful Assembly	Affirms the right to gather and express views collectively.
Article 22 - Freedom of Association	Upholds the right to form and join groups or organizations freely.

Restrictions on Free Speech (Violation of ICCPR Article 19)

ICCPR Article 19 guarantees the right to freedom of expression, stating that any restrictions must be clearly defined, necessary, and proportionate. However, PECA's vague and overly broad definitions of “false information" and “aspersions" against state institutions pose a significant threat to free speech. The Act criminalizes speech deemed "sufficiently likely to be fake," making it easier for authorities to suppress dissent, investigative journalism, and political criticism.

The Human Rights Committee (HRC) has consistently ruled that laws restricting speech should not be used to shield public officials from accountability. In Zeljko Bodrožić v. Serbia and Montenegro, the Committee ruled that a journalist's criticism of a public figure was protected under the ICCPR, emphasizing that public debate on

political figures is particularly valuable in democratic societies[70]. The HRC has consistently held that uninhibited expression is crucial for democracy.

PECA also misinterprets Section 19(3) of the ICCPR, which allows restrictions only to protect the rights of others, national security, or public order. However, the HRC requires that restrictions be both necessary and proportionate, considering the content and context of the speech. The truthfulness of a statement, for instance, increases the value of protecting that expression and reduces the state's interest in restricting it. In Bodrožić's case, the HRC found that a criminal conviction for insult was not a necessary restriction, as the speech was factually true and aimed at a public figure. Despite the domestic court's finding that sarcasm was used to belittle, the HRC concluded that the restriction was disproportionate, as the state has no legitimate interest in protecting a public figure's reputation from truthful statements. Thus, the truthfulness of an expression reduces the legitimacy of imposing restrictions on it [71].

Fair Trial and Due Process Rights (Violation of ICCPR Article 14)

Article 14 of ICCPR guarantees the right to a fair trial and due process, requiring an independent and impartial tribunal. However, PECA establishes Social Media Protection Tribunals (SMPT), whose members are appointed rather than independently selected judges. This structure raises concerns about political interference in digital cases. The HRC has warned against the dangers of executive control over the judiciary, as seen in Burundi's Universal Periodic Review (UPR), where the Committee criticized the lack of judicial independence due to direct executive influence over judicial bodies. The country's President was the head of the Superior Council of the Judiciary, where the Minister of Justice also sat, and that the Council had the power to monitor the quality of judgements, rulings and related enforcement measures[72].

Additionally, PECA's appeal mechanism undermines due process protections under ICCPR by skipping High Courts and directing appeals straight to the Supreme Court.This imposes financial and procedural barriers to justice, as litigation at the Supreme Court level is costly and inaccessible to most individuals. The HRC has previously condemned similar practices, such as in Spain's UPR review, where the Committee ruled that denying defendants the right to appeal through multiple levels

[70] Helen Jasper Keegan James Marco Guzman Arturo J. Carrillo, "He Who Dares Not Offend Cannot Be Honest: United Nations Human Rights Committee Jurisprudence and Defamation Laws Under the ICCPR," *GW Law Faculty Publications & Other Works. 1679*, 2023, pg 7 https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2932&context=faculty_publications (accessed 1 Mar 2025P)

[71] Ibid

[72] Caroline Da Silva e Sousa and Daisuke Shirane, *The International Covenant on Civil and Political Rights (ICCPR) Article 14: Right to Equality before Courts and Tribunals and to a Fair Trial Factsheets for legal practitioners and civil society actors,* February 2024, *pg 8*

of the judiciary violates ICCPR[73]. Furthermore, the HRC criticized Egypt for restricting appeals in military courts, reinforcing that all defendants must have meaningful avenues for appeal[74]. PECA's direct-to-Supreme Court model creates an unjust legal bottleneck.

Unchecked Surveillance and Privacy (Violation of ICCPR Article 17)

Article 17 of the ICCPR protects individuals from arbitrary or unlawful interference with privacy, family, or correspondence. However, PECA grants the National Cyber Crime Investigation Agency (NCCIA) excessive surveillance powers, including broad data collection and monitoring capabilities without adequate judicial oversight. These powers raise serious concerns about potential abuse, particularly against journalists, activists, and political opponents. The European Court of Human Rights (ECHR) reinforced these concerns in *Big Brother Watch and Others v. the United Kingdom*, where a coalition of civil society organizations and journalists, including Big Brother Watch, challenged the UK's surveillance regime. They argued that the regime violated the right to privacy and freedom of expression. The ECHR ruled in favor of the complainants, finding that the surveillance practices lacked adequate safeguards and oversight, thereby breaching privacy rights [75]. This decision highlights the dangers of unchecked surveillance and underscores the need for strong legal safeguards to prevent government overreach, a concern that is particularly relevant given NCCIA's sweeping authority under PECA and increases the risk of politically motivated surveillance.

Criminalization of Disinformation and the Need for Decriminalization

One of the most concerning aspects of PECA is its criminalization of disinformation, which contradicts international best practices. The HRC has consistently ruled that defamation and misinformation should be handled through civil remedies rather than criminal prosecution.

In the case of Eglė Kusaitė v. Lithuania, the Human Rights Committee (HRC) found that Kusaitė's statements were vague, negative remarks made about prosecutors in response to a highly stressful situation. The HRC expanded its consideration of proportionality to assess whether the imposed restrictions could constitute an excessive burden, particularly considering Kusaitė's age and economic status[76]. The

[73] Ibid, pg 18
[74] Ibid
[75] "UK Surveillance Regime Violates Human Rights to Privacy and Free Speech, European Court of Human Rights holds," *Human Rights Law Centre*, 13.Sep.2018, https://www.hrlc.org.au/human-rights-case-summaries/2019/4/25/uk-surveillance-regime-violates-rights-to-privacy-and-free-speech (accessed 28 Feb 2025)
[76] Helen Jasper Keegan James Marco Guzman Arturo J. Carrillo, "He Who Dares Not Offend Cannot Be Honest: United Nations Human Rights Committee Jurisprudence and Defamation Laws Under the ICCPR," *GW Law Faculty Publications & Other Works. 1679*, 2023, pg 5 https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2932&context=faculty_publications (accessed 1 Mar 2025)

HRC concluded that even the imposition of a minor fine, given her circumstances, could be seen as disproportionate. As a result, the Committee determined that the restrictions on her speech were neither necessary nor proportionate.

A landmark example is Konate v. Burkina Faso (2014), where the African Court on Human and Peoples' Rights ruled that sentencing a journalist to prison for defamation was disproportionate and violated ICCPR protections[77]. The Court emphasized that defamation laws must serve a legitimate purpose without suppressing public discourse.Pakistan's approach under PECA mirrors the same flaws that led to Burkina Faso's conviction at the African Court. The HRC has repeatedly urged states to follow these international precedents, making it likely that Pakistan's criminalization of disinformation under PECA will face scrutiny.

Suppression of Political Dissent (Violations of ICCPR Articles 21 & 22)

Articles 21 and 22 of ICCPR protects the right to freedom of assembly and association, including online activism. However, PECA empowers authorities to block social media platforms that fail to comply with government directives, effectively silencing opposition and restricting digital activism. Social media is often the only space for grassroots movements in restrictive environments, making its regulation a key concern under ICCPR.

The HRC has previously ruled that states cannot impose blanket restrictions on digital platforms. In M.T. v. Uzbekistan, the Committee found that criminalizing the creation of an unregistered association violated ICCPR[78], reinforcing that individuals must be free to organize and communicate online without excessive state interference. The Special Rapporteur on Freedom of Assembly has further affirmed that unregistered associations must be allowed to operate freely. PECA's approach to social media censorship and platform bans contradicts these rulings, ostensibly contravening International digital assembly rights.

[77] Laura Holt, Rebecca Nica and Arturo J. Carrillo, "Decriminalizing Defamation: A Comparative Law Study," *International Law and Policy Brief,* 19 Mar, 2022, https://studentbriefs.law.gwu.edu/ilpb/2022/03/19/decriminalizing-defamation-a-comparative-law-study/ (accessed 27th February 2025)

[78] "M.T. v. Uzbekistan, Human Rights Committee, UN Doc. CCPR/C/114/D/2234/2013, Views of 23 July 2015, paras. 7.7-7.8.," *European Center for Not-for-Profit Law (ECNL) International Center for Not-for-Profit Law (ICNL),* July 2023, pg 5

Chapter 8

Economic Repercussions

When rights falter, economies follow—freedom is not just a moral imperative; it is an economic one.

Economic Repercussions

The PECA Act 2025 may have unintended and adverse effects for Pakistan on the global stage, Pakistan currently enjoys GSP+ block III status with the European Union, allowing the nation to trade goods with the EU bloc on a friendly tariff regime, effectively allowing 20% of total goods to be traded on zero tariffs while another 70% of goods exported are given preferential rates. GSP+ has proven to be pivotal for EU-Pakistan bilateral trade ties. From 2014 to 2022, Pakistan's exports to the EU increased by 108% whereas imports from the EU increased by 65% and the total trade volume increased from EUR 8.3 billion in 2013 to EUR 14.85 billion[79]. This Generalized Scheme of Preferences is awarded to nations who ratify with the EU Bloc on 27 international conventions, of which some seem to have already been breached by the recent PECA 2025 Act[80]. The potentially breached Conventions are as follows:

1. International Covenant on Civil and Political Rights.
2. Freedom of Association and Protection of the right to Organize Convention.

The upcoming GSP+ monitoring team visit in June 2025 was preceded by the visit of Olof Skoog, the EU Special Representative for Human Rights who emphasized that freedom of expression is a key condition for GSP+ status. [81]

"You can't restrict freedom of expression just to protect politicians, authorities, or the system from being criticized."
- Olof Skoog-

He also highlighted that the next round of the GSP+ scheme depends on Pakistan's compliance with its international obligations, warning that GSP+ status cannot be taken for granted.

If the concerns raised by the EU regarding freedom of expression are not addressed, Pakistan's GSP+ status and trade relations with the EU could be at risk. Additionally,

[79] Saeed Akhtar, "The European Union Releases the Fourth GSP Report: Evaluating Implementation of 27 International Conventions in Beneficiary Countries, including Pakistan" *European Commission and the European External Action Service (EEAS),* 21.Nov.2023 https://www.eeas.europa.eu/delegations/pakistan/european-union-releases-fourth-gsp-report-evaluating-implementation-27-international-conventions_en?s=175#:~:text=Pakistan%20was%20awarded%20GSP%2B%20status,sustainable%20development%20by%20facilitating%20trade (accessed 28.Feb.2025)
[80] "At a glance: EU preferential imports from GSP+ beneficiary countries (2023, € million)," *GSP HUB*, https://gsphub.eu/country-info/Pakistan (accessed 28.Feb.2025)
[81] Absa Komal, "Don't take GSP+ for granted, says EU envoy," *Dawn News,* 30.Jan.2025 https://www.dawn.com/news/1888586 (accessed 28.Feb.2025)

Chapter 9

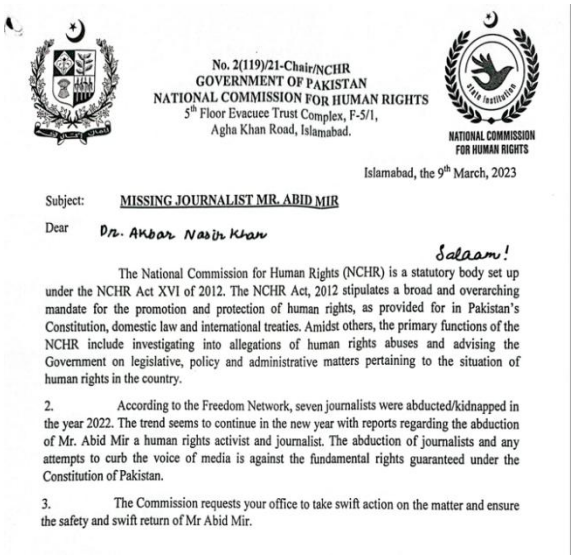
Conclusion

Pakistan's digital future will not be defined by technology, but by whether it chooses fear or freedom as its guiding code

Conclusion

NCHR has played a central role in promoting digital rights, defending press freedom, and advancing human rights-based digital governance in Pakistan. Acknowledging the growing misuse of cybercrime laws and their chilling impact on free expression, the Commission initiated a series of multi-stakeholder consultations to foster dialogue between state institutions and civil society. These forums brought together leading digital rights organizations—Digital Rights Foundation (DRF), Bolo Bhi, and the Human Rights Commission of Pakistan (HRCP)—as well as senior journalists, editors, and representatives from the Pakistan Telecommunication Authority (PTA). The discussions centered on the PECA and its successive amendments, examining their implications, challenges, and the road ahead for rights-based digital reform.

The Commission also intervened directly through formal correspondence with relevant government bodies, particularly the Ministry of Human Rights, law enforcement agencies, and regulatory authorities. These communications raised serious concerns over the misuse of PECA provisions against journalists, activists, and citizens for exercising their right to free expression. Letters were issued protesting arbitrary arrests, including those of Asad Ali Toor and Abid Mir, emphasizing that journalism and public criticism are constitutionally protected under Articles 19 and 19A. The NCHR urged authorities to uphold due process, prevent abuse of power, and align PECA's enforcement with Pakistan's international obligations under the ICCPR.



No. 2(119)/21-Chair/NCHR
GOVERNMENT OF PAKISTAN
NATIONAL COMMISSION FOR HUMAN RIGHTS
5th Floor Evacuee Trust Complex, F-5/1,
Agha Khan Road, Islamabad.

NATIONAL COMMISSION FOR HUMAN RIGHTS

Islamabad, the 9th March, 2023

Subject: MISSING JOURNALIST MR. ABID MIR

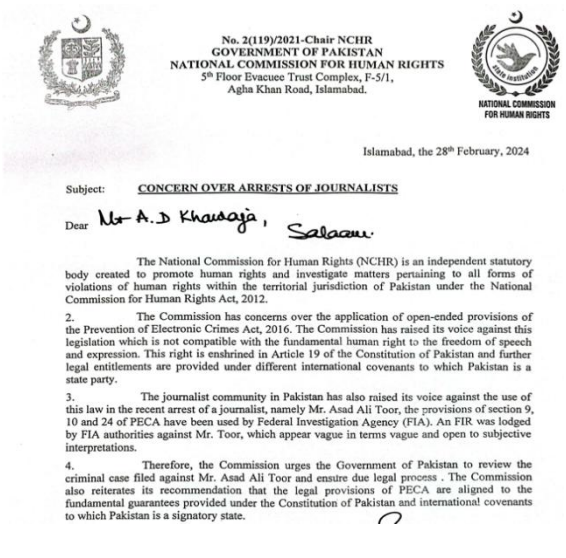
Dear Dr. Akbar Nasir Khan

Salaam!

The National Commission for Human Rights (NCHR) is a statutory body set up under the NCHR Act XVI of 2012. The NCHR Act, 2012 stipulates a broad and overarching mandate for the promotion and protection of human rights, as provided for in Pakistan's Constitution, domestic law and international treaties. Amidst others, the primary functions of the NCHR include investigating into allegations of human rights abuses and advising the Government on legislative, policy and administrative matters pertaining to the situation of human rights in the country.

2. According to the Freedom Network, seven journalists were abducted/kidnapped in the year 2022. The trend seems to continue in the new year with reports regarding the abduction of Mr. Abid Mir a human rights activist and journalist. The abduction of journalists and any attempts to curb the voice of media is against the fundamental rights guaranteed under the Constitution of Pakistan.

3. The Commission requests your office to take swift action on the matter and ensure the safety and swift return of Mr Abid Mir.



No. 2(119)/2021-Chair NCHR
GOVERNMENT OF PAKISTAN
NATIONAL COMMISSION FOR HUMAN RIGHTS
5th Floor Evacuee Trust Complex, F-5/1,
Agha Khan Road, Islamabad.

NATIONAL COMMISSION FOR HUMAN RIGHTS

Islamabad, the 28th February, 2024

Subject: CONCERN OVER ARRESTS OF JOURNALISTS

Dear Mr. A.D Khawaja, Salaam.

The National Commission for Human Rights (NCHR) is an independent statutory body created to promote human rights and investigate matters pertaining to all forms of violations of human rights within the territorial jurisdiction of Pakistan under the National Commission for Human Rights Act, 2012.

2. The Commission has concerns over the application of open-ended provisions of the Prevention of Electronic Crimes Act, 2016. The Commission has raised its voice against this legislation which is not compatible with the fundamental human right to the freedom of speech and expression. This right is enshrined in Article 19 of the Constitution of Pakistan and further legal entitlements are provided under different international covenants to which Pakistan is a state party.

3. The journalist community in Pakistan has also raised its voice against the use of this law in the recent arrest of a journalist, namely Mr. Asad Ali Toor, the provisions of section 9, 10 and 24 of PECA have been used by Federal Investigation Agency (FIA). An FIR was lodged by FIA authorities against Mr. Toor, which appear vague in terms vague and open to subjective interpretations.

4. Therefore, the Commission urges the Government of Pakistan to review the criminal case filed against Mr. Asad Ali Toor and ensure due legal process . The Commission also reiterates its recommendation that the legal provisions of PECA are aligned to the fundamental guarantees provided under the Constitution of Pakistan and international covenants to which Pakistan is a signatory state.

Through its continued advocacy and monitoring, the Commission has identified a deep divide surrounding the PECA Amendment Act 2025. On one side, journalists, civil society, and the judiciary have formed a united front, firmly rejecting the Act in its entirety. They argue that the very foundation of the amendment is rooted in control rather than protection—undermining its original purpose of safeguarding digital users from cybercrime. On the opposite end, the government remains resolute, unwilling to revise or reconsider the law. Officials maintain that, in today's digital age, regulation is essential to protect citizens from serious online offenses.This deadlock has led to a stalemate, with no substantial progress or consensus in sight. Despite this impasse, the Commission believes there are three possible paths forward:

1. Full Repeal of the PECA Amendment Act 2025:

The Act could be scrapped entirely to prevent its misuse. However, the law remains in effect, and several cases have already been registered under the new amendments[82]. Without repeal, public reliance on the law will continue—regardless of its flaws.

2. Reform Through Rules and Implementation Frameworks:

Rather than rejecting the law altogether, efforts can be directed toward reforming the rules that govern its provisions. The example of the (RBOUC) Rules shows how implementation guidelines can significantly shape the impact

[82] News Desk, "Pindi traffic police register PECA case against citizen," *The Express Tribune*, 23.March.2025, https://tribune.com.pk/story/2535988/rawalpindi-traffic-police-register-peca-case-against-citizen (accessed 2nd April 2025)

of a law[83]. As technology continues to evolve, regulations must be dynamic, rights-based, and adaptable rather than rigid and punitive.

3. Targeted Amendements and Integration of Global Governance Principle:

Recognizing that PECA is still a relatively young law with limited institutional maturity, selected provisions could be amended or replaced. The Commission recommends aligning the law with UNESCO's five key principles for digital governance[84]:

By embedding these values, Pakistan can develop a more balanced and effective digital regulatory system.

[83] Farieha Aziz, "The ministry of (dis)information and the ban on X," *Dawn News Prism,* 25.April.2024, https://www.dawn.com/news/1828972 (accessed 20th Feb 2025)

[84] " Guidelines for the governance of Digital Platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach," *UNESCO 2023,* pg 25, https://unesdoc.unesco.org/ark:/48223/pf0000387339 (accessed 20th Feb 2025)

Chapter 10

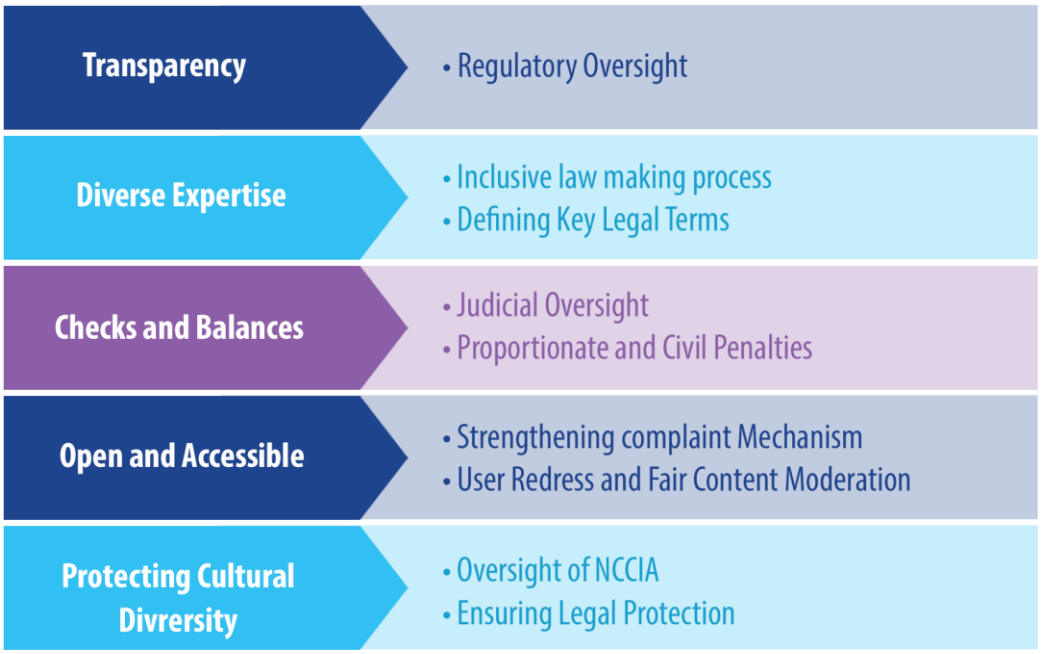
Recommendations

A just digital future will be built through reform, not repression—through dialogue, not decrees

Recommendations

Moving forward, the implementation of the following recommendations can help ensure that PECA fulfills its core objective—protecting digital users from cybercrime—while also upholding democratic freedoms, promoting accountability, and restoring public trust in Pakistan's digital governance framework.The **UNESCO Digital Platform Governance Guideline**[85] provides a valuable blueprint to address the challenges and resistance PECA has encountered.The following recommendations are categorized under the five key principles of UNESCO's digital governance framework:

UNESCO Digital Platform Governance Guideline



1.Transparency

Regulatory Oversight:

Transparency in digital governance is essential to ensure accountability, fairness, and public trust in the regulatory process. The four new agencies established under the PECA Amendment Act—the Social Media Protection and Regulatory Authority (SMPRA), Social Media Complaint Council (SMCC), Social Media Protection Tribunal (SMPT), and National Cybercrime Investigation Agency (NCCIA)—must operate independently, free from political influence. The appointments of the members of the agency should be made through a transparent, merit-based process, with oversight

[85] " Guidelines for the governance of Digital Platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach," *UNESCO 2023,* https://unesdoc.unesco.org/ark:/48223/pf0000387339 (accessed 20th Feb 2025)

by parliament or the judiciary, rather than by executive discretion. Furthermore, these agencies should be required to publicly disclose their enforcement actions, policies, and financial expenditures to prevent misuse of authority.

To prevent arbitrary restrictions on digital content, SMPRA should be mandated to maintain a publicly accessible list of blocked websites and restricted content, along with the legal justifications for such actions. Decisions regarding content moderation and censorship should be subject to judicial review to ensure compliance with Articles 19(3) and 20 of the ICCPR, which safeguard freedom of expression while allowing for proportionate restrictions in exceptional cases. In addition, the NCCIA must be subject to strict oversight to prevent unauthorized data retention and mass surveillance. Any surveillance activities must comply with internationally recognized privacy protections to uphold digital rights and ensure government accountability.

Digital platforms must also play a role in ensuring transparency. Companies operating in Pakistan should be required to publish periodic transparency reports that outline their content moderation policies, algorithmic decision-making processes, and enforcement mechanisms. These platforms must also provide users with clear explanations of how their algorithms prioritize or demote content, ensuring that individuals receive diverse viewpoints by default. By fostering transparency across government agencies and digital platforms, PECA can ensure that its enforcement mechanisms remain fair, accountable, and resistant to political misuse.

2. Diverse Expertise

Inclusive Law making Process:

The formulation and amendment of digital laws should involve input from a wide range of stakeholders, including civil society organizations, legal experts, journalists, and digital rights activists. PECA amendments must undergo a consultative and transparent legislative process, ensuring that all relevant voices, including dissenting opinions, are considered in drafting, reviewing, and refining legal changes. This participatory approach will help create digital regulations that address the complexities of modern online interactions while safeguarding fundamental rights. Additionally, fostering inclusivity in the lawmaking process will help rebuild public trust in government regulations. The OHCHR guidelines on participation in decision-making should serve as a framework for ensuring meaningful stakeholder engagement, preventing unilateral decision-making by the state and promoting balanced, rights-based digital governance. Before proposing further amendments, we can seek guidance from experts such as the Special Rapporteur on the Promotion

and Protection of the Right to Freedom of Opinion and Expression, Irene Khan, to ensure that the reforms align with international human rights standards[86].

Defining Key Legal terms:

One of the key challenges in regulating online content is the lack of precise legal definitions. Laws must clearly distinguish between different forms of harmful speech to prevent overreach. The **UN Rabat Plan of Action (2012)** provides a six-part threshold for assessing whether speech constitutes incitement to violence, discrimination, or hostility, offering a clear framework to differentiate between hate speech and legitimate free expression [87] . Similarly, disinformation and misinformation must be clearly defined in law. The United Nations defines disinformation as inaccurate information that is intended "to deceive and is spread in order to do serious harm."This is confused with misinformation, which is information that is false or misleading, but not intended to cause harm or deceive. By adopting internationally recognized definitions, PECA can ensure that legal interventions in digital content regulation are precise, necessary, and proportionate.Additionally, certain definitions, such as the expanded definition of a complainant allowing third-party involvement, should be repealed to prevent misuse and politically motivated legal actions.

3. Checks and Balances

Judicial Oversight:

A well-functioning digital governance system must incorporate strong judicial oversight to prevent abuse of power and ensure fair trial protections. The Social Media Protection Tribunal (SMPT) should function as an independent judicial body, free from executive influence, with appointments made through an impartial and transparent process. This tribunal should have clearly defined jurisdiction and must adhere to due process standards, ensuring that any decisions restricting digital rights are necessary, lawful, and proportionate. Furthermore, all major decisions by regulatory agencies, including SMPRA, should be subject to judicial review to prevent arbitrary enforcement.

The appeal mechanism under PECA must be revised to enhance access to justice. Appeals should be allowed at the High Court level before reaching the Supreme Court, ensuring a multi-tiered judicial review process that provides meaningful recourse for those affected by regulatory decisions. Judicial precedents from international cases reinforce the need for checks and balances in digital governance. The landmark case

[86] Irene Khan, "Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," *UN Human Rights Council 47th Session Agenda item 3 (A/HRC/47/25),* 21 June–9 July 2021, https://docs.un.org/en/A/HRC/47/25 (accessed 20th Feb 2025)
[87] Ibid, pg 9

of Anuradha Bhasin v. Union of India, in which Anuradha Bhasin, editor of the Kashmir Times (Srinagar Edition), challenged the State of India's internet shutdown and additional restrictions on movement and public assembly[88]. The Supreme Court ruled that the government failed to justify the necessity of the internet suspension, leading the court to mandate a review of suspension orders and the lifting of any that did not meet legal requirements. This case underscores the critical role of judicial oversight in preventing arbitrary restrictions on fundamental rights in digital spaces.

Proportionate and Civil Penalties:

The criminalization of disinformation should be reconsidered, with penalties restricted to civil fines rather than imprisonment, in line with international best practices. Sri Lanka decriminalized defamation in 2002 following sustained civil society advocacy, recognizing that criminal penalties for speech-related offenses threaten press freedom and democratic discourse[89]. This reform took place even as Sri Lanka was grappling with an internal conflict involving the Tamil Tigers—demonstrating that security concerns need not justify the suppression of free expression. Pakistan, similarly facing challenges from militant groups, should take note. Other countries have also taken steps in this direction. Several African countries such as Ghana repealed its criminal libel and seditious laws in 2001, and Kenya declared criminal defamation unconstitutional in 2017[90]. These examples reflect a growing global consensus that civil remedies are more appropriate and less harmful to democratic values. Pakistan's PECA law should align with these international precedents—protecting press freedom and public debate while ensuring accountability through proportionate, civil mechanisms.

4. Open and Accessible

Strengthening Complaint Mechanism for Digital Users:

Ensuring access to digital rights requires regulatory mechanisms that are user-friendly and efficient. The Social Media Complaint Council (SMCC) should be made accessible through both physical offices and an online complaint portal, allowing individuals to file grievances without unnecessary delays. The complaint process should be simplified to eliminate bureaucratic barriers, ensuring that digital users can seek redress without facing legal or logistical challenges. The agency must also have sufficient financial and human resources to process complaints in a timely manner.

---

[88] " Bhasin v. Union of India: Writ Petition (Civil) No. 1031/2019," *Global Freedom of Expression, Columbia University,* 10 Jan 2020, https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india/ (accessed 20th Feb 2025)

[89] Laura Holt, Rebecca Nica and Arturo J. Carrillo, "Decriminalizing Defamation: A Comparative Law Study," *George Washington University: International Law and Policy Brief (ILPB),* 19 Mar 2022, https://studentbriefs.law.gwu.edu/ilpb/2022/03/19/decriminalizing-defamation-a-comparative-law-study/ (accessed 20th Feb 2025)

[90] Ibid

User Redress and Fair content Moderation:

To further strengthen user protections, social media platforms should establish robust internal appeals mechanisms that allow individuals to challenge content removal decisions. Additionally, external oversight mechanisms, such as independent social media councils, should be considered to monitor content moderation practices and provide an additional layer of accountability. These mechanisms will help prevent unjustified content takedowns and ensure that online platforms operate within a framework of fairness and transparency.

5. Protecting Cultural Diversity

Oversight of NCCIA:

Cultural diversity must be safeguarded to ensure an inclusive digital environment that respects the rights of marginalized communities, including women, journalists, artists, and human rights defenders. To prevent the misuse of digital laws against vulnerable groups, Parliament should enact comprehensive data protection legislation that upholds Article 14 of Pakistan's Constitution, which guarantees the right to privacy and dignity. Stronger oversight of the NCCIA is necessary to ensure that cybersecurity measures do not lead to mass surveillance or violations of individual freedoms.

Ensuring Legal Protection:

Journalists and whistleblowers, who are frequently exposed to digital threats and harassment, require robust and independently enforced legal protections. While Pakistan has established the Commission for the Protection of Journalists and Media Professionals under the Protection of Journalists and Media Professionals Act, 2021, its effectiveness depends on ensuring genuine institutional independence, adequate resourcing, and operational autonomy from executive influence.

Strengthening the Commission's mandate to proactively oversee violations against media professionals, provide legal assistance, and facilitate secure reporting mechanisms would significantly enhance press safety. Comparative models such as Sri Lanka's Press Complaints Commission demonstrate how independent self-regulatory mechanisms can address complaints, enable corrections and protect reputations without state interference[91].Adapting similar principles of independence and accountability within Pakistan's existing framework would help safeguard press freedom while responsibly addressing concerns related to misinformation.

[91] Press Complaints Commission of Sri Lanka (PCCSL)https://www.presscouncils.eu/press-complaints-commission-of-sri-lanka-pccsl/#:~:text=Introduction,Act%20No%2011%20of%201995. (Accessed April 2025)

Annexure

PECA 2016 Concerning Provisions	Comments on the Concerns	PECA 2025 Concerning Provisons	Comments on the Concerns
No. F. 22(03)/2015 - Legis.— The following Acts of Majlis-e-Shoora (Parliament) received the assent of the President on 18th August, 2016 are hereby published for general information: ACT NO. XL of 2016 An Act to make provisions for the Prevention of Electronic Crimes		No. F. 9(05)/2025 - Legis.— The following Act of Majlis-e-Shoora (Parliament) received the assent of the President on 29th January, 2025 and is hereby published for general information: ACT NO. II of 2025 AN ACT Further to amend the Prevention of Electronic Crimes Act,2016	
(iii) "access to information system" means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;		after clause (iii), the following new clause (iiia), shall be inserted, namely: - "(iiia) "aspersion" means spreading false and harmful information which damages the reputation of a person;";	The terms 'false' 'harmful' are vague and ambiguous. So is the term 'damaging' the reputation, when there is sufficient precedent in comparative jurisdictions that false and defamatory statement or prohibited false speech, are protected within the ambit of 'freedom of speech' as well as guaranteed under constitution.
(iv) "Authority" means the Pakistan Telecommunication Authority established under the Pakistan Telecommunication (Re-organization) Act,1996 (XVII of 1996);		for clause (iv), the following shall be substituted, namely: — "(iv) "Authority" means the Social Media Protection and Regulatory Authority established under section 2A";	Authority changed from PTA to SMPRA

(vi) "authorized officer" means an officer of the investigation agency authorized to perform any function on behalf of the investigation agency by or under this Act;		for clause (via), the following shall be substituted, namely: — "(via) "complainant" means any person who makes complaint of any offence under this Act and includes a victim, or an individual having substantial reasons to believe that the offence has been committed;	(vi) "authorized officer" means an officer of the investigation agency authorized to perform any function on behalf of the investigation agency by or under this Act;
xvi) "dishonest intention" means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence;	This definition has been made extremely subjective due to the inclusion of the words "to create hatred". "Creating hatred" leaves room for interpretation and ambiguity.		
(xxv) "offence" means an offence punishable under this Act except when committed by a person under ten years of age or by a person above ten years of age and under fourteen years of age, who has not attained sufficient maturity of understanding to judge the nature And consequences of his conduct on that occasion;		after clause (xxv), the following new clauses shall be inserted, namely: — "(xxva) "Unlawful or offensive content" means the offence as defined in section 2R; (xxvb) "person" means a legal or natural person and includes a body politic or corporate; (xxvb) "prescribed" means rules or regulations made under this Act;";	Granting corporations and government bodies the same legal standing as individual's risks suppressing journalistic reporting, whistleblowing, and critical speech. To prevent misuse, the definition should explicitly exclude government and political entities. Clear limitations must be imposed to prevent corporations from using legal provisions to silence criticism, with safeguards against complaints filed in bad faith.
(xxviii) "service provider" includes a person who, — acts as a service provider in relation to sending, receiving, storing, processing or distribution of any electronic		after clause (xxviiia), the following new clause shall be inserted, namely: - "(xxviiib) "social media platform" means— (a) any person that owns, provides or	Provision (b): The amendment introduced a new definition for social media platforms, adding "communication channels" to its scope. This broad definition allows authorities to block VPNs used to

communication or the provision of other services in relation to electronic communication through an information system owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or processes or stores data on behalf of such electronic communication service or users of such service;		manages online information system for provision of social media or social network service; or (b) a website, application or mobile web application, platform or communication channel and any other such application and service that permits a person to become a registered user, establish an account, or create a public profile for the primary purpose of allowing the user to post or share user-generated content through such an account or profile or enables one or more users to generate content that can be viewed, posted or shared by other users of such platform but shall not include the licensees of Pakistan Telecommunication Authority;"; and	access the blocked platforms like X, which have been under increasing government scrutiny. With this legal cover, the PTA and federal government now have a legitimate tool to enforce such restrictions. The broad definition of "social media platform" encompasses all internet users engaging with social media, including those managing YouTube channels, Facebook pages, or X accounts. By mandating registration with the new Authority, this amendment subjects' ordinary users, journalists, and activists to government oversight, raising serious concerns about state control over independent journalism and digital activism. Moreover, enforcing such a requirement is impractical, as it would necessitate registering every Pakistani with a social media presence, creating an unrealistic and unworkable regulatory burden.
		3. Insertion of Chapters 1A, IB and IC, Act XL of 2O16. — In the said Act, after Chapter 1, the following new Chapters shall be inserted, namely:- "CHAPTER 1A AUTHORITY	
		2B. Powers and functions of the Authority.—(1) In	The sections are from (a) to (v)

		addition to the functions and powers specified otherwise in this Act, the Authority shall have the following powers and functions, namely:— (d) ensure online safety and rights of persons on social media platforms from any kind of harm; (e) regulate the unlawful or offensive content on the social media platforms accessible from Pakistan; (f) regulate enlistment of social media platforms; (g) grant, renew, refuse, suspend and revoke enlistment of social media platform; (h) to partially or fully block social media platform if it fails to comply with the provisions under this Act until the compliance is made; (k) prescribe fines for contravention of the provisions of Chapters 1A and 1B or rules or regulations made thereunder; (l) issue directions to the relevant authorities to block or remove the unlawful or offensive content for the reasons to be recorded in writing for a period of thirty days subject to grant of another extension if any for maximum period of thirty days by majority of all the members of the Authority;	The SMPRA has been given vague and undefined powers. What constitutes as 'offensive content' is not clearly defined by the text of the Act, yet the authority has been given power to regulate it, which leaves much of its decisions up to its own discretion, and sense of morality and ethics. The enlistment requirement effectively establishes a licensing system for digital expression, allowing the government to control who can use social media. This mirrors past attempts under PMDA and PMRA to register digital platforms, granting authorities the power to refuse, suspend, or revoke enlistment, thereby silencing critical voices. With the added ability to block platforms entirely and issue guidelines without legislative oversight, the Authority risks becoming a tool for censorship rather than regulation. Its powers must be strictly limited to ensuring transparency, protecting users, and preventing actual harm. Content regulation should be clearly defined, align with international free speech standards, and be subject to judicial oversight. Enlistment should not apply to individuals, independent journalists, or non-commercial platforms, and blocking entire social media platforms

			should be permitted only under exceptional circumstances with strict judicial review and due process.
		2C. Complaint to the Authority on fake information.—Any person aggrieved by fake and false information may apply to the Authority for removal or blocking access to such information and the Authority shall, on receipt of such application, forthwith, but not later than twenty-four hours, pass such orders as it considers necessary including an order for removal or blocking access to such information,	Raises concerns over Section 26-A, which criminalizes "fake or false news" without defining what constitutes such information. Vague language gives more room to the government to exert control.
		2D. Composition of the Authority.—(1) The Authority shall consist of a Chairperson and eight other members out of which Secretary Ministry of Interior, Chairman PEMRA and Chairman Pakistan Telecommunication Authority (PTA) or any member of PTA nominated by him shall be the ex-officio members. (2) The Chairperson and five members, other than ex-officio members, shall be appointed by the Federal Government on such terms and conditions as may be determined by it. The Chairperson shall be eminent professional with recognized bachelor's degree and	2D consists of 4 points. However, the first 3 points are concerning. The appointment of the members of the Authority are completely controlled by the executive, leaving the functioning of the authority and the policies at the complete mercy of the government, completely controlling narrative building and the voice of the opposition or the criticisers.

		with fifteen years' experience in information technology or law or social media policy governance or related emerging technologies. (3) The Chairperson and members, other than ex-officio members, shall be appointed for a non-extendable period of five years/provided the Chairperson or a member does not exceed fifty-eight years of age on the date of his initial appointment.	
		(2E) Removal of Chairperson and members.—(1) The Federal Government may remove the Chairperson or a member, other than ex-officio members, from his office if he is found unable to perform the functions of his office due to mental or physical disability, inefficiency or to have committed misconduct.	The term 'inefficiency' is dangerously vague, and therefore keep the members of the Authority completely unprotected.
		(2G) Powers and functions of the Chairperson.—(1) The Chairperson shall also function as the chief executive of the Authority and shall perform such functions and exercise such powers as may be delegated by the Authority. (2) The Chairperson shall have exclusive powers to perform such functions and exercise such powers which require immediate action including issuance of	The Chairperson has been given complete authority to block content, when the term 'unlawful' is so vague and not clarified by the text of the Act. This leaves decisions up to his discretion and personal sense of morality.

		direction for blocking of any unlawful online content: Provided that any such exercise of power or performance of function shall be subject to ratification by the Authority within forty-eight hours: Provided further that such notification can be done by circulation.	
		2O. Power of the Federal Government to Issue directives.—The Federal Government may, as and when it considers necessary, issue directives to the Authority on matters of policy relating to this Act, and such directives shall be binding on the Authority, and if a question arises as to whether any matter is a matter of policy or not, the decision of the Federal Government shall be final.	This effectively makes the government's directives binding, stripping regulatory bodies of any autonomy. This centralizes power over social media regulation within the executive branch.
		2P. Indemnity.—No suit, prosecution or either proceedings shall lie against the Government or public authority or functionary or any other person exercising any powers or performing any function under this Act or for anything done in good faith.	While indemnity clauses are standard in legal statutes, this provision effectively prevents any scrutiny when government officials or authorities act in contravention of the law or Constitution.
		CHAPTER-IB ENLISTMENT ETC 2Q. Enlistment.—(1) The Authority may require any social media	The amendments introduce a mandatory enlistment requirement for social media platforms with the authority, effectively

		platform to enlist with it in such manner, form and on payment of such fee, as may be prescribed. (2) The Authority may stipulate, in addition to the requirements of this Act, such conditions or requisites as it may deem appropriate while enlisting a social media platform.	forcing platforms to register locally and comply with censorship demands. Non-compliance grants the authority the power to block these platforms entirely. The enlistment requirement, while vaguely worded, aligns with the registration mandate in the Social Media Rules 2021, reflecting a long-standing aspiration to exert greater control over digital content rather than legitimate regulation. Under Section 2Q, the authority is empowered to determine the enlistment process, impose unspecified conditions, and charge fees at its discretion.
		2R. Unlawful or offensive online content.—(1) The Authority shall have the power to issue directions to a social media platform for removal or blocking of online content, if such online content— (a) is against the ideology of Pakistan, etc.; (b) incites the public to violate the law, take the law in own hands, with a view to coerce, intimidate or terrorize public, individuals, groups, communities, government officials and institutions; (c) incites public or section of public to cause damage to	SMPRA has been given vast and undefined powers to block and remove online content. It has been given the power to remove content deemed unlawful or against the “ideology of Pakistan" whilst it is unclear that who would determine, and how, what aligns with Pakistan's ideology. Content that targets or criticizes members of the judiciary, armed forces, Majlis-e-Shoora (Parliament), or provincial assemblies can also be removed now, making it a tool for suppressing dissent.

		governmental or private property; (d) coerce or intimidate public or section of public and thereby preventing them from carrying on their lawful trade and disrupts civic life;	
		2R. Unlawful or offensive online content.—(2) Without prejudice to any other restrictions in this regard, while reporting the proceedings of the Majlis-e-Shoora (Parliament) or a Provincial Assembly, such portion of the proceedings as the Chairman of the Senate, the Speaker of the National Assembly or, as the case may be, Speaker of the Provincial Assembly may have ordered to be expunged, shall not be streamed or made available for viewing on social media platforms in any manner and every effort shall be made to release a fair account of the proceedings.	This is a violation of constitutional right to information.
		2R. Unlawful or offensive online content.—(3) The statements of prescribed organizations or their representatives or members thereof shall not be streamed or made available for viewing on social media platforms in any manner.	
		(2T) Social Media Complaint Council,—(1) The Federal Government shall by notification in	The grounds for removal of the members of the council are very vague and indeterminate,

		the official Gazette, constitute Social Media Complaint Council which shall consist of a Chairman and four members including one ex-officio member to receive and process complaints made by persons, organizations and general public against violation of any provision of this Act as may be prescribed by regulations. (2) The Chairman and members other than ex-officio members of the Council shall be appointed by the Federal Government for a term of three years extendable for another similar term on the terms and conditions of service as may be determined by it. (7) The Federal Government may remove the Chairman or a member of the Council if he is found unable to perform the functions of his office due to mental or physical disability, inefficiency or to have committed misconduct. Explanation.—For the purposes of this section, the expression "misconduct" means conviction for any offence involving moral turpitude and abuse or misuse of authority. (8) In case of a vacancy occurring due to the death, resignation or removal of Chairman or any member of the Council, other than the ex-officio member, the	specifically the term 'inefficient' and 'moral terpitude'. This does not allow the members of the council to make principled decisions. The government is acting as the judge, jury and the executioner, in relation to regulating the media. This centralization of power will impact democracy.

		Federal Government shall appoint another qualified person within a. period not exceeding two months from the date the vacancy occurred.	
		CHAPTER IC SOCIAL MEDIA PROTECTION TRIBUNAL 2V. Tribunals.—(1) The Federal Government may, by notification in the official gazette, establish as many Social Media Protection Tribunals for the purposes of this Act as it may determine. Where more than one such Tribunals are established, the Federal Government shall specify territorial limits within which or the class of cases in respect of which each of such Tribunal shall exercise jurisdiction under this Act. (2) A Tribunal shall consist of— (a) a Chairman, who has been or is qualified to be a judge of a High Court; (b) a journalist registered with any press club of Pakistan having not less than twelve years of relevant experience with known professional competence in his field and having a bachelor's degree in journalism recognized by the Higher Education Commission of Pakistan; and (c) a software engineer, and expert in the field of	The establishment of Social Media Protection Tribunals raises serious concerns about judicial independence, due process, and access to justice. The Federal Government's discretionary power to establish tribunals, define their territorial or subject-matter jurisdiction, and appoint members without an independent, transparent selection process undermines judicial impartiality. The lack of procedural safeguards creates a risk of tribunals being politicised or used for selective enforcement against journalists, activists, and online dissenters. The composition of the Tribunal further raises serious legitimacy concerns. The requirement that a journalist be registered with a press club does not guarantee expertise in digital rights or human rights law. Likewise, the requirement for a software engineer with expertise in "social media rights" is

		social media rights haying a minimum of bachelor's degree recognized by the Higher Education Commission, of Pakistan, in relevant field or allied subject. (3) The Chairman and members of a Tribunal shall be appointed by the Federal Government for a period of three years, on such terms and conditions as may be prescribed. (5) The Federal Government may remove the Chairman or a member of the Tribunal if he is found unable to perform the functions of his office due to mental or physical disability, inefficiency or to have committed misconduct. Explanation.—For the purposes of this section, the expression "misconduct" means conviction for any offence involving moral turpitude and abuse or misuse of authority. (7) The Tribunal shall decide all cases within ninety days. In case the decision is not rendered within the stipulated time, the Tribunal shall record the reasons for the same. (8) The Tribunal shall follow such procedure as may be prescribed.	imprecise and lacks defined selection criteria, creating the risk of politically influenced appointments rather than guaranteeing genuine expertise in internet governance, digital rights, or relevant legal frameworks. According to this law any young engineer with a bachelor's degree and no experience is eligible to sit in the tribunal.
		2X. Appeal against decisions of the Tribunal.—Any person aggrieved by the final decision of the Tribunal	The amendments deny individuals the right to appeal decisions made by regulatory authorities to the High Court, which

		may prefer an appeal to the Supreme Court of Pakistan within sixty days of receipt of the decision."	violates the principles of due process and access to justice. Fair trial rights under Article 10-A of the Constitution are undermined when individuals are denied the ability to challenge unjust restrictions on their speech.
CHAPTER II OFFENCES AND PUNISHMENTS 3. Unauthorised access to information system or data. — Whoever with dishonest intention gains unauthorised access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both. 4. Unauthorised copying or transmission of data. — Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both. 6. Unauthorised access to critical infrastructure information system or data. — Whoever with dishonest intention gains unauthorised access to any critical	Provisions 3, 4, 6, and 7 present a significant risk of misapplication against whistleblowers and journalists, raising serious concerns about potential misuse. A prevailing culture of information denial exists, where exclusionary clauses are frequently invoked to withhold disclosure rather than promote transparency. In many cases, leaked information serves as the primary mechanism through which wrongdoing is exposed, underscoring the crucial role of whistleblowers in holding governments, organizations, and other entities accountable. However, the broad and often vague provisions risk facilitating overreach, enabling authorities to target individuals who disclose information in the public interest. While it is essential to prevent the misuse of information for intimidation or malintent, it is equally imperative to recognize that certain critical		

infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both. 7. Unauthorised copying or transmission of critical infrastructure data. — Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to five million rupees or with both.	information only reaches the public domain through leaks and whistleblower disclosures. In the absence of adequate protections, individuals exposing corruption, misconduct, or violations of public trust may face legal repercussions, effectively silencing dissent and undermining transparency.		
9. Glorification of an offence. — (1) Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism, or activities of proscribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both. Explanation. — For the purposes of this section "glorification" includes depiction of any form of	The vague and overly broad scope of the legislation creates a risk of misuse against individuals engaging in political expression, advocacy, or legitimate dissent. Those supporting political movements, voicing grievances could face prosecution under the pretext of glorifying offences, effectively suppressing freedom of speech and political engagement.		

praise or celebration in a desirable manner.			
10. Cyber terrorism. — Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to, — (a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance interfaith, sectarian or ethnic hatred; or (c) advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.	Cyber-terrorism is a critical concept under this Act, yet its definition has an overly broad scope and lacks the necessary nexus to violence, harm, or injury. Critics argue that cyber-terrorism offences should be clearly linked to acts of violence or the imminent risk of harm, ensuring that the provision targets genuine threats rather than being applied indiscriminately. However, Section 10(b) expands the scope of cyber-terrorism to include the advancement of "inter-faith, sectarian, or ethnic hate" as a qualifying factor. This broad wording blurs the distinction between terrorism and offences related to incitement or hostility, creating legal ambiguity that could result in the disproportionate application of counterterrorism measures to speech-related offences. Furthermore, violations of Section 10 carry harsher penalties than offences committed under Sections 6 through 9, raising concerns about excessive punishment and selective enforcement. In practice, Section 10 is frequently added to FIRs and leveraged against		

	dissidents to justify arrests, as it remains one of the three cognizable offences under PECA, alongside Section 21 (offences related to minors) and Section 22 (pornography) under provision 43 in Chapter V . This pattern of enforcement underscores the risk of overreach and misuse, particularly against individuals engaging in political expression or dissent.		
11. Hate speech. — Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance interfaith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.	The definition of hate speech under PECA is vague and open to misuse, making it difficult to draw a clear distinction between protected free speech and unlawful hate speech. Section 11 of PECA, a non-cognizable offence, specifically pertains to interfaith, sectarian, or racial hatred and does not extend to criticism of state institutions. Despite this, individuals are frequently charged under Section 11 for so-called “hate speech” reflecting a pattern of misuse where the provision is applied beyond its intended scope to suppress dissent and political expression.		
20. Offences against dignity of a natural person. — (1) Whoever intentionally and publicly exhibits or displays or transmits	Distinguishing ‘factual information' from ‘false and fake information' is a very delicate subject. This provision effectively criminalizes defamation, significantly restricting		

any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both: Provided that nothing under this subsection shall apply to anything aired by a broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002). (2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in subsection (1) and the Authority on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.	freedom of speech., satire, and citizen journalism are at risk of being interpreted as reputational harm, creating a chilling effect on free expression. Moreover, defamation is already addressed under civil law, eliminating the need for criminal penalties. Criminalizing defamation will deter journalistic work, public accountability, and criticism of official conduct. As a result, individuals may self-censor, a trend already evident in broadcast and print media, or face FIRs and potential jail terms for engaging in legitimate criticism. Such measures undermine democratic discourse and restrict the public's ability to hold those in power accountable. Section 20 requires that the complainant be an individual and the aggrieved party be the person personally defamed. By definition, an institution does not fall within the scope of this offence. However, in practice, this provision has been misapplied to shield institutions from criticism, contradicting its intended purpose. In 2022, Justice Minallah declared Section 20 of the PECA law “null and void."		
24. Cyber stalking. — (1) A person commits the offence of cyber stalking	Provision 24(d) is broadly worded and open to wide		

who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the Internet, website, electronic mail or any other similar means of communication to— (a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person; (b) monitor the use by a person of the internet, electronic mail, text message or any other form of electronic communication; (c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or (d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person. (2) Whoever commits the offence specified in subsection (1) shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both: Provided that if victim of the cyber stalking under subsection (1) is a minor the punishment may	interpretation, raising concerns about its potential misuse. For instance, does it apply to photographs taken at public gatherings, protests, or large events without individual consent? What about images highlighting public figures attending rallies or congregations organized by banned groups, particularly when such documentation is intended to expose affiliations or hold individuals accountable? The provision lacks clear safeguards, potentially restricting public interest reporting and investigative journalism. Moreover, violations under Section 24(d) carry a jail term of up to three years, with the PTA, rather than the courts, designated as the authority to handle complaints. This bypasses judicial oversight, concentrating enforcement power in an administrative body. Additionally, the (3) grants the PTA authority to direct its licensees to obtain and secure information, including traffic data, which infringes on privacy rights. Such provisions enable intrusive surveillance and risk facilitating arbitrary or politically motivated actions in the name of digital regulation.		

extend to five years or with fine which may extend to ten million rupees or with both. (3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in subsection (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.			
26. Spoofing. — (1) Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing.		Insertion of new section 26A, Act XL of 2016.—In the said Act, after section 26 the following new section 26A shall be inserted, namely:— "26A, Punishment for false and fake information.—Whoever intentionally disseminates, publicly exhibits, or transmits any information through any information system,, that he knows or has reason to believe to be false or fake and likely to cause or create a sense of fear, panic or disorder or unrest in general public or society shall be punished with imprisonment which may extend upto three	The law is vague and grants the government unchecked power to decide what is true and false. This provision will be weaponized against journalists and opposition voices, further suppressing press freedom under Article 19 of the Constitution and the Journalist Protection Act. Furthermore, this has the potential to create a 'chilling effect' which will further damage freedom of speech, which is essential for stability.

		years or with fine which may extend to two million rupees or with both."	
29. Establishment of an investigation agency. (1) The Federal Government may establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act. (2) Unless otherwise provided for under this Act, the investigation agency and the authorized officer shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act. (3) The investigation agency shall establish its own capacity for forensic analysis of the data or in information systems and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency. (4) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology,	Despite the passage of PECA, no formal investigating agency was initially established to handle cybercrime cases. The FIA received over 250 complaints within just two days of PECA coming into effect, even though its cybercrime wing, the National Response Centre for Cyber Crime (NR3C), had not yet been officially designated as the investigative agency under the Act. This raised serious concerns about the agency's capacity to handle the surge in cybercrime complaints. By October 2017, in the first 10 months, approximately 8,000 complaints had already been filed with the FIA, further highlighting the strain on an understaffed and under-resourced agency. The volume of cases and the complexity of cyber-related offences far exceeded the NR3C's investigative capacity, exposing gaps in enforcement and procedural delays. It was only after seven months that the Law Ministry designated 31 Additional Sessions Judges (ADJs) and Judicial Magistrates (JMs) across Pakistan to handle cybercrime cases. However, legal	Amendment of section 29, Act XL of 2016.—In the said Act, for section 29, the following shall be substituted namely— "29. Investigation agency.—(1) The Federal Government shall establish an investigation agency to be called the National Cyber Crime Investigation Agency (NCCIA) for inquiry into, investigation and prosecution of the offences specified under this Act. (2) The NCCIA shall be headed by a Director General, who shall have the power to employ any other officers, prosecutors and staff as may be prescribed. (3) The Federal Government shall appoint the Director General of the NCCIA for a non-extendable term of three years, and the administration and control of the NCCIA shall vest in the Director General who shall exercise in respect of the NCCIA the powers of Inspector General of Police under the Police Order, 2002 (Chief Executive's Order No. 22 of 2002). (4) For the purposes of inquiry and investigation, the officers of the NCCIA shall be deemed to be	This investigation agency, like the tribunal and the council, are completely under the influence of the executive. Therefore, violating principles of democracy, and concentration of power. The actual structure, mandate, and operational framework of the proposed National Cyber Crime Investigation Agency (NCCIA) is concerning. The Federal Investigation Agency (FIA) has consistently cited resource constraints in handling cybercrime cases, and its performance under PECA, particularly in addressing cases affecting women, has not been good. But the mere creation of a new agency does not guarantee better investigative capabilities, especially if it replicates the same systemic flaws that make the FIA's Cyber Crime Wing so ineffective. Questions about NCCIA's purpose and methods of operation must be answered; How will be ensured that he NCCIA will not repeat the same patterns that FIA had? What are the changes being made in its operational structure, and enforcement

computer science and other related matters for training of the officers and staff of the investigation agency.	experts raised concerns about the judiciary's limited understanding of cybercrimes, noting that without specialized training, the adjudication of cyber-related offences would remain ineffective. The lack of expertise within the judiciary poses a significant risk to the fair application of cyber laws, as judges unfamiliar with digital forensics, electronic evidence, and online offences may struggle to dispense justice effectively. Without comprehensive training programs for both investigators and the judiciary, cybercrime cases risk being mishandled, delayed, or unjustly prosecuted, ultimately undermining the credibility of digital rights enforcement in Pakistan.	the police officer of equivalent rank as required under the Code. The officers of the NCCIA shall have the same powers and functions and related authority for the performance of investigating functions as are conferred on a police officer of the equivalent rank under the Code. (5) After establishment of the NCCIA, the Cyber Crime Wing of the Federal Investigation Agency shall cease to exist and all personnel, cases, inquiries, investigations, assets, properties, budget, liabilities, rights, obligations, privileges and matters related thereto or connected therewith in respect of the defunct Cyber Crime Wing of the Federal Investigation Agency shall stand transferred to the NCCIA. (7) The investigation agency shall establish its own capacity for forensic analysis of the data or in information systems and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency. (8) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment,	mechanisms that will make it effective? What bylaws or rules will govern its functioning, oversight, and accountability? Additionally, the rationale for dismantling the FIA's cybercrime wing and creating a new body, as opposed to tackling the issue of resources within FIA is not clear. Until these critical details are shared, any assessment of this body would not be an informed assessment, and no meaningful recommendation can be made.

		promotion, transfer in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of officers and staff of the investigation agency: Provided that until such time, rules are made by the Federal Government, service matters of officers and staff of the NCCIA shall be regulated under the Civil Servants Act, 1973 (LXXI of 1973) and rules made thereunder. (9) Without prejudice to anything contained in this section, the rules, orders or any instruments made and issued under this Act prior to commencement of the Prevention of Electronic Crimes (Amendment) Act, 2025 (of 2025) shall, mutatis mutandis, apply to the NCCIA with necessary modifications.".	
30. Power to investigate. — Only an authorised officer of the investigation agency shall have the powers to investigate an offence under this Act: Provided that the Federal Government or the Provincial Government may, as the case may be, Constitute one or more joint investigation teams comprising of an authorised officer of the	Investigating officer has sweeping powers. All punitive action should be subject to a court order.	Substitution of section 30, Act XL of 2016.—In the said Act, for section 30, the following shall be substituted, namely:— "30. Power to investigate.—Only an authorized officer of the investigation agency shall have the powers to investigate an offence under this Act: Provided that the Federal Government may constitute one or more joint investigation teams	No limit has been defined under this law. Any investigation agency can be taken on board. No limit has been defined as to what can and cannot be investigated. This is unclear who this law actually aims to protect. If it were the citizens, then there must have been laws setting limitations on what to be investigated or not, a check and balance on it.

investigation agency and any other law enforcement agency for investigation of an offence under this Act and any other law for the time being in force.		comprising an authorized officer of NCCIA and any other law enforcement agency for investigation of offences under this Act. The joint investigation team may seek assistance from any intelligence agency for the purposes of investigation under this Act."	
31. Expedited preservation and acquisition of data. — (1) If an authorised officer is satisfied that— (a) Specific data stored in any information system or by means of an information system is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the authorised officer may, by written notice given to the person in control of the information system, require that person to provide that data or to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety days as specified in the notice: Provided that the authorised officer shall	Section 31 allows an authorised agent to require a person to hand over data without producing a court warrant if it is believed that it is "reasonably required" for a criminal investigation. What is a "reasonable" requirement? No test as to what constitutes reasonable requirement is provided in the section. This can be termed as a blanket authorisation provision that gives the executive direct authority to take action without any judicial oversight or scrutiny. The lack of requisite checks and balances affords the executive a discretionary power that can be used to violate fundamental rights. This can consequently rob a citizen of his right to be treated in accordance with the due process of law. Such a provision can, therefore, be subject to misuse and exploitation in order to achieve certain political agendas and suppress		

immediately but not later than twenty-four hours bring to the notice of the Court, the fact of acquisition of such data and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise. (2) The period provided in subsection (1) for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorised officer in this behalf	any form of lawful debate or dissent. Additionally, the law requires for him to only bring this to the notice of a court within 24 hours after the acquisition of the data. This is too long a period in the tech world. Even in cases involving "cyberterrorism", which is vaguely defined, the officer can search, seize, and retain data without a warrant and notify the court within 24 hours of its seizure. This section delegates arbitrary powers to an officer.		
32. Retention of traffic data. (1) A service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and, subject to production of a warrant issued by the Court, provide that data to the investigation agency or the authorised officer whenever so required. (2) The service providers shall retain the traffic data under subsection (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic	Breach of Privacy Data can be misused - state can get hold of phone numbers + locations of journalists - this data can compromise safety of journalists, rights activists, dissenters. Section 32 of the Act requires ISPs to retain specified traffic data for a minimum of one year and subject to the demands of the PTA, provide that data to an investigation agency or authorised agent. Such an indiscriminate requirement for service providers to retain data breaches the international standards of the right to privacy. This fosters the growth of conditions under which a highly invasive blanket surveillance of		32. Retention of traffic data. (1) A service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and, subject to production of a warrant issued by the Court, provide that data to the investigation agency or the authorised officer whenever so required. (2) The service providers shall retain the traffic data under subsection (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic

Transactions Ordinance, 2002 (LI of 2002). (3) Any owner of the information system who is not a licensee of the Authority and violates subsection (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both.	populations would be able to take place. According to civil society, the practical implications of this particular provision are already beginning to materialise. From January 2017 to June 2017, the Pakistani government sent 1,050 requests for data to Facebook, compared to 2016 when only 719 requests were made. However, nobody knows the reasons as to why such access was requested and whether this law was actually used to prevent tangible harm from materialising. The Court of Justice of the European Union (CJEU), in 2014, noted that metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" and concluded that the retention of metadata relating to a person's private life and communications is, in itself, a disproportionate interference with the right to privacy.		Transactions Ordinance, 2002 (LI of 2002). (3) Any owner of the information system who is not a licensee of the Authority and violates subsection (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both.
33. Warrant for search or seizure. — (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that—	Provision 33 does not specify the procedures through which seized data would be retained, stored, deleted or further copied. These elements should have been specifically enumerated and governed by a clear and accessible legal regime that provides for redress		33. Warrant for search or seizure. — (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that—

(a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or (b) has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorise an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data, device or other articles relevant to the offence identified in the application. (2) In circumstances involving an offence under section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss of data, information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazetted officer of the investigation agency, may enter the specified place and search the premises and any information system, data, device or	for any violations of the right to privacy. Data should not be retained for longer than is necessary, or used for anything other than the purposes for which it was collected. A list of what has been seized should be provided to the owner of the device. Additionally, the owner of the data should receive a forensic image of their seized data.		(a) May reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or (b) has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorise an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data, device or other articles relevant to the offence identified in the application. (2) In circumstances involving an offence under section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss of data, information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazetted officer of the investigation agency, may enter the specified place and search the premises and any information system, data, device or

other articles relevant to the offence and access, seize or similarly secure any information system, data, device or other articles relevant to the offence: Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of such search or seizure and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case.			other articles relevant to the offence and access, seize or similarly secure any information system, data, device or other articles relevant to the offence: Provided that the authorized officer shall immediately but not later than twenty-four Hours bring to the notice of the Court, the fact of such search or seizure and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case.
34. Warrant for disclosure of content data. — (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that the person in control of the data or information system, to provide such data or access to such data to the authorised officer. (2) The period of a warrant issued under subsection (1) may be extended beyond seven	'Disclosure of content data.' In this bill, data is defined as 'traffic data and content data.' Moreover, other forms of 'data' are covered under other definitions.Information for instance is defined as: 'text, message, data, voice, sound, database, video, signals, software, computer programs, any form of intelligence as defined under the PTA. So, while a warrant would be required for disclosure of 'content data,' there is no procedure nor oversight prescribed for the acquisition, disclosure, retention, preservation or handling of traffic data - which is also identifiable data (i.e. can reveal a person's location, identity and		34. Warrant for disclosure of content data. — (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that the person in control of the data or information system, to provide such data or access to such data to the authorised officer. (2) The period of a warrant issued under subsection (1) may be extended beyond seven

days if, an application, a Court authorises an extension for a further period of time as may be specified by the Court.	more). Moreover Section 31 deals with a person in control of the information system or data, and not service providers or those storing data on behalf of others. Therefore the token warrant for contentdata hardly serves as a safeguard for the above-listed sections, which give sweeping powers over - and intrusive access – to everyone's communication and data. And there is no data protection or privacy legislation in Pakistan		days if, an application, a Court authorises an extension for a further period of time as may be specified by the Court.
37. Unlawful online content. — (1) The Authority shall have the power to remove or block or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act. (2) The Authority shall, with the approval of the Federal Government, prescribe rules providing for, among other matters, safeguards, transparent process and effective oversight mechanism for exercise of powers under subsection (1).	Should be Omitted as this is covered by Telecommunications Act Very vague - gives too much power to the authority through statements such as "interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act" —- thereby restricting the right to freedom of expression. PTA is notorious for its dalliances with censorship, and for its arbitrary blocking and removal of content. This is problematic at two levels: The specific cases related to the right to freedom of speech that		37. Unlawful online content. — (1) The Authority shall have the power to remove or block or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act. (2) The Authority shall, with the approval of the Federal Government, prescribe rules providing for, among other matters, safeguards, transparent process and effective oversight mechanism for exercise of powers under subsection (1).

(3) Until such rules are prescribed under subsection (2), the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provisions of this Act. (4) Any person aggrieved from any order passed by the Authority under subsection (1), may file an application with the Authority for review of the order within thirty days from the date of passing of the order. (5) An appeal against the decision of the Authority in review shall lie before the High Court within thirty days of the order of the Authority in review.	fall within or outside the exceptions listed in Article 19 are left to the sole discretion of the executive authority of PTA. PTA has the absolute power to decide as to how Article 19 is to be interpreted and applied. PTA also has the authority to determine the content that may or may not be accessed by internet users in the country. Authorised personnel from the PTA have the power to remove any content that they believe is immoral, anti-state, against any country considered to be an ally of Pakistan, or politically unacceptable. This shows that both legislative and judicial functions have been placed in the domain of a single executive authority. PTA can act unilaterally against such content, without acquiring a court order. This indirectly provides the State with a mechanism to deal with and block content that it deems as unpalatable. Eg: GoP may block access to some political content under the pretext of preventing harm. According to a transparency report issued by Facebook, 177 pieces of content have already been restricted from viewership in the country based on requests forwarded by the PTA for violating		(3) Until such rules are prescribed under subsection (2), the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provisions of this Act. (4) Any person aggrieved from any order passed by the Authority under subsection (1), may file an application with the Authority for review of the order within thirty days from the date of passing of the order. (5) An appeal against the decision of the Authority in review shall lie before the High Court within thirty days of the order of the Authority in review.

	"local laws prohibiting blasphemy and condemnation of the country's independence". Section 37, which copy pastes Article 19 and gives PTA powers to interpret and apply the restrictions is something parliament should legislate on and the judiciary interpret. It is not a function for a telecom regulator to perform. Powers under Section 37. There are no definitions of what constitutes "necessity," what can be deemed against the "glory of Islam," against the "integrity, security or defense of Pakistan," or against "public order, decency and morality." No exceptions or exclusions are identified in this Section nor is there an appeals process. Additionally, there are no guidelines for these bases of removal.		
39. Realtime collection and recording of information.— (1) If a Court is satisfied on the basis of information furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect	The criteria for surveillance is extremely open ended. Furthermore real time activity would be recorded for seven days. There is no mention of the capability and methods that will be used to do this - – how invasive they would be. The same instruments used to record forseven days can (and most likely will) be		39. Realtime collection and recording of information.— (1) If a Court is satisfied on the basis of information furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect

to information held by or passing through a service provider, to a designated agency as notified under the Investigation for Fair Trial Act, 2013 (I of 2013) or any other law for the time being in force having capability to collect real time information, to collect or record such information in real time in coordination with the investigation agency for provision in the prescribed manner: Provided that such realtime collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days. (2) Notwithstanding anything contained in any law to the contrary the information so collected under subsection (1) shall be admissible in evidence. (3) The period of real time collection or recording may be extended beyond seven days if, on an application, the Court authorises an extension for a further specified period.	used for continued and selective and/or broad-based surveillance.		to information held by or passing through a service provider, to a designated agency as notified under the Investigation for Fair Trial Act, 2013 (I of 2013) or any other law for the time being in force having capability to collect real time information, to collect or record such information in real time in coordination with the investigation agency for provision in the prescribed manner: Provided that such realtime collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days. (2) Notwithstanding anything contained in any law to the contrary the information so collected under subsection (1) shall be admissible in evidence. (3) The period of real time collection or recording may be extended beyond seven days if, on an application, the Court authorises an extension for a further specified period.
42. International cooperation.— (1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend	Section 42 of the PECA Amendment Act grants sweeping powers to the government regarding international cooperation in data sharing. The lack of		42. International cooperation.— (1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend

such cooperation to any foreign government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real time collection of data associated with specified communications or interception of data under this Act. (2) The Federal Government may forward to a foreign government, 24x7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offence under this Act. (3) The Federal Government shall	clear limitations and oversight mechanisms raises serious concerns about unilateral data-sharing agreements between the government and foreign entities, including intelligence agencies of other countries. The absence of judicial authorization in this process further exacerbates the risk of unregulated access to sensitive private data. Subsection 2 is particularly troubling as it permits the government to share data collected under the Act with foreign or international agencies without any accountability safeguards or transparency measures. This means that once sensitive personal data is handed over to foreign entities, it is no longer subject to Pakistan's domestic legal protections and could be used without restriction. The information shared could include private details about individuals or large datasets containing information on significant numbers of people, posing serious risks to privacy and data protection. The United Nations human rights experts and bodies have repeatedly raised concerns over privacy violations linked to unregulated data-sharing practices. Significant privacy concerns have been identified by UN human		such cooperation to any foreign government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real time collection of data associated with specified communications or interception of data under this Act. (2) The Federal Government may forward to a foreign government, 24x7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings Concerning any offence under this Act. (3) The Federal Government shall require the foreign government, 24 x 7

require the foreign government, 24 x 7 network, any foreign agency or any international organization or agency to keep the information provided confidential and use it strictly for the purposes it is provided. (4) The Federal Government may, through the designated agency, send and answer requests for mutual assistance the execution of such requests or their transmission to the authorities competent for their execution. (5) The Federal Government may refuse to accede to any request made by a foreign government, 24 x 7 network, any foreign agency or any international organization or agency, if,— (a to g) (7) The designated agency shall maintain a register of requests received from any foreign government, 24 x 7 network, any foreign agency or any international organization or agency under this Act and action taken thereon.	rights experts and bodies. The lack of a robust legal framework for governing information exchanges between foreign intelligence agencies further highlights the need for specific laws that establish strict oversight mechanisms and provide for domestic accountability.		network, any foreign agency or any international organization or agency to keep the information provided confidential and Use it strictly for the purposes it is provided. (4) The Federal Government may, through the designated agency, send and answer requests for mutual assistance the execution of such requests or their transmission to the authorities competent for their execution. (5) The Federal Government may refuse to accede to any request made by a foreign government, 24 x 7 network, any foreign agency or any international organization or agency, if,— (a to g) (7) The designated agency shall maintain a register of requests received from any foreign government, 24 x 7 network, any foreign agency or any international organization or agency under this Act and action taken thereon.
48. Prevention of electronic crimes. — (1) The Federal Government or the Authority, as the case may be, may issue directives to be followed by the owners of the designated information	This provision grants the government and the Pakistan Telecommunication Authority (PTA) broad powers to issue directives to service providers in the interest		48. Prevention of electronic crimes. — (1) The Federal Government or the Authority, as the case may be, may issue directives to be followed by the owners of the designated information

systems or service. Providers in the interest of preventing any offence under this Act. (2) Any owner of the information system who is not a licensee of the Authority and violates the directives issued under subsection (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both: Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Reorganization) Act, 1996.	of preventing offences under the Act. However, the provision lacks clarity, specific limitations, and necessary safeguards, allowing PTA unchecked discretion in formulating additional rules. This unrestricted authority raises serious concerns, particularly regarding the suppression of free speech, as it creates the potential for arbitrary enforcement and excessive restrictions on online expression.		systems or service. Providers in the interest of preventing any offence under this Act. (2) Any owner of the information system who is not a licensee of the Authority and violates the directives issued under subsection (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both: Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Reorganization) Act, 1996.

National Commission for Human Rights, Pakistan

5th Floor Evacuee Trust Complex,
Agha Khan Road, Islamabad

051 9216771

www.nchr.gov.pk