Reforming the Prevention of Electronic Crimes Act: A Constitutional and Rights-Based Framework for Pakistan

Policy Paper by PJN Pakistan

PEACE AND JUSTICE NETWORK
پیس اینڈ جسٹس نیٹ ورک پاکستان



JANUARY 2026

The rapid expansion of digital technologies has transformed Pakistan's social, political, and economic landscape. From online journalism and civic activism to digital commerce and public service delivery, the internet has become central to democratic participation and national development. As digital engagement grows, so too does the responsibility of the state to regulate cyberspace in a manner that ensures security while safeguarding constitutional freedoms.

The Prevention of Electronic Crimes Act (PECA), 2016, was enacted to address cybercrime, including hacking, identity theft, cyber terrorism, and online exploitation. However, subsequent amendments, under Prevention of Electronic Crimes (Amendment) Act 2025[1], have significantly broadened the scope of the law, expanding criminal liability related to digital speech and increasing regulatory authority over online content.

While the objectives of combating cybercrime and misinformation are legitimate, concerns have emerged regarding the constitutionality, proportionality, and procedural safeguards embedded within the amended framework. The evolving application of PECA has raised critical questions about its compatibility with Pakistan's constitutional guarantees of freedom of expression, access to information, due process, and privacy.

National and international Human rights organizations including UN warned these changes could tighten government control over digital spaces and suppress dissent and freedom of expression. They criticised the vague framing of offences and the absence of meaningful public consultation during drafting.

This policy paper argues that meaningful reform of PECA is both necessary and urgent. Reform must move beyond reactive enforcement and instead establish a rights-based digital governance framework grounded in constitutional principles, democratic accountability, and international best practices.

The Digital Transformation of Pakistan

Over the past decade, Pakistan has experienced substantial growth in internet penetration, mobile connectivity, and social media usage. Digital platforms now serve as primary spaces for:

- Political debate and civic mobilisation

[1] https://www.na.gov.pk/uploads/documents/679b243193585_457.pdf

- Journalism and public accountability
- Business transactions and entrepreneurship
- Education and public service delivery
- Social engagement and community building

This digital shift has empowered citizens by expanding access to information and enabling participation in governance. At the same time, it has created vulnerabilities, including cyber fraud, online harassment, data breaches, and disinformation campaigns.

An effective legal framework must therefore strike a careful balance: protecting individuals and institutions from genuine cyber threats while preserving the democratic vitality of online expression.

Constitutional Context and Democratic Principles

Pakistan's Constitution provides robust protections for fundamental rights. Article 19 guarantees freedom of speech and expression, subject only to reasonable restrictions in the interests of national security, public order, decency, morality, or other specified grounds. Article 19A protects the right to access information. Article 10A enshrines the right to fair trial and due process.

Any digital regulatory framework must therefore satisfy constitutional tests of:

- Legality (clear and precise language)
- Legitimate aim (protecting defined public interests)
- Necessity (least restrictive means available)
- Proportionality (balancing harm prevention with rights protection)

Where laws are vague, overly broad, or lacking procedural safeguards, they risk failing these constitutional standards.

Moreover, Pakistan is a signatory to international human rights instruments that require restrictions on speech to be narrowly tailored and proportionate. A digital governance framework inconsistent with these obligations may undermine both domestic constitutional order and international credibility.

PECA: Legislative Intent and Expansion

When PECA was introduced in 2016, its stated purpose was to combat electronic crimes such as unauthorized access to data, identity theft, cyber stalking, and online terrorism. It provided investigative powers to law enforcement agencies and established penalties for digital offences.

However, the 2025 amendments expanded the scope of the law, particularly through provisions criminalising the dissemination of "false and fake information" and enhancing regulatory oversight of digital platforms. These changes marked a significant shift from targeting cybercrime to regulating online speech more broadly.

The 2025 amendment changed the definition of a complainant to be any person "having substantial reasons to believe that the offence has been committed" in addition to the "victim", which significantly expands the ability to file a case — from an aggrieved person to any third party. The other significant change is that now the complainant does not have to be a "natural person" but can be any organisation, including a government department. Another significant change in definition includes expanding "social media platform" to include "any person that owns, provides or manages online information system for provision of social media or social network service", which

expands the purview of the law to people administering online groups or channels as well.

The amendment further introduces Section 26-A, which stipulates punishment of three years in jail and/or Rs2 million fine for "false or fake information", without defining what that entails. The amendment also makes Section 20, declared unconstitutional and struck down by the Islamabad High Court in 2022[2], cognisable and non-bailable, despite the court having also restrained arrests and quashed related cases under this provision.

The expansion of criminal liability related to expression has prompted widespread debate among legal experts, media bodies, civil society organisations, and digital rights advocates. Critics argue that broad and undefined language risks arbitrary interpretation, potentially criminalising legitimate criticism, journalistic reporting, and political discourse.

Such concerns are not merely theoretical; enforcement patterns and legal challenges indicate growing tensions between digital regulation and constitutional freedoms.

Emerging Concerns in PECA Implementation

Post-amendment implementation has raised concerns regarding:

- The potential misuse of speech-related provisions to target journalists and critics;
- Arrests and FIR registrations without sufficient evidentiary thresholds;
- Content blocking decisions lacking transparent reasoning or judicial oversight;
- Concentration of regulatory power within executive-controlled institutions.

These issues have resulted in litigation, parliamentary debate, and calls for reform from diverse stakeholders. The challenge is not whether Pakistan should regulate cyberspace — regulation is both legitimate and necessary. The challenge lies in designing a system that combats cybercrime effectively without eroding democratic freedoms.

Post-2025 Amendment - Cases and Enforcement Patterns

Cases Against Journalists and Media

A judicial magistrate's order blocked 27 YouTube channels, including those run by journalists and political commentators, over alleged "fake, misleading, and defamatory" content targeting state institutions — invoking PECA enforcement[3]. Several journalists challenged the order, and a court restored access, highlighting concerns about arbitrary bans and constitutional rights to fair hearing.

Women journalists were implicated in a FIA-registered FIR after private disputes shared in a WhatsApp group were deemed violations of PECA[4], drawing condemnation from media rights groups who called the move an attempt to silence women's voices in media.

In Punjab, arrests of journalists and legal actions in mid-2025 under PECA provisions were reported, including cases interpreted as targeting investigative reporting on issues like alleged corruption[5].

In January 2026, human rights lawyer Imaan Mazari and her husband, Hadi Chattha, were

[2] https://digitalrightsmonitor.pk/islamabad-high-court-quashes-peca-amendment-ordinance-part-of-s-20-of-peca-also-unconstitutional/?utm_source=chatgpt.com
[3] https://www.dawn.com/news/1922836
[4] https://digitalrightsmonitor.pk/peca-cases-against-npc-women-journalists/
[5] https://www.fnpk.org/journalists-assaulted-harassed-and-abducted-across-punjab-in-july-2025/

sentenced to 17 years' imprisonment under various sections of the Prevention of Electronic Crimes Act (PECA) in a controversial tweets case. The decision was strongly condemned by civil society, legal experts, journalists, and human rights bodies. The court sentenced them to five years' imprisonment each, along with a fine of Rs 5 million each, under Section 9 of PECA. They were further sentenced to 10 years' imprisonment each, with a fine of Rs 30 million each, under Section 10 of PECA. Moreover, the couple was also convicted under Section 26-A of PECA and sentenced to two years' imprisonment each, along with a fine of Rs 1 million each[6].

Blocked Online Content

The July 2025 court order to block many online channels under PECA was widely framed by activists as an example of how the law can be used to censor political content by branding it "misleading" or "defamatory"[7].

Ordinary Citizens and Political Speech

A case in early 2025 saw the arrest of a WhatsApp group admin in Pakpattan for allowing an insulting post against a provincial political leader to be viewed, under PECA and additional penal code provisions[8]. This reflects how content moderation responsibilities can be criminalised at the individual level.

In an unusual and high-profile instance, non-bailable warrants were issued in late 2025 for the Khyber Pakhtunkhwa Chief Minister in a PECA case[9] related to alleged defamatory online remarks against state institutions — signaling the law's use even against senior politicians.

Digital rights activist Usama Khilji in his recent article highlighted the current situation "if post-2016 were the years when PECA's misuse against those exercising their right to freedom of speech and press freedom was tested, 2025 was the year when the gaps in the state's ability to fully abuse the law were filled"[10].

Senate Implementation Review

In September 2025, a Senate Standing Committee review found hundreds of PECA cases illegally registered by provincial authorities after the amendment and directed their withdrawal. The panel raised concerns over how the law was being operationalised and potential misuse against journalists and ordinary citizens, urging clearer implementation frameworks[11].

Challenges and Judicial Pushback

Multiple petitions and legal challenges have been filed:

- The Islamabad High Court Journalists Association filed a petition challenging the PECA amendments as unconstitutional, arguing unchecked censorship powers and infringement on press freedom[12].
- The Pakistan Federal Union of Journalists (PFUJ) initiated action in the High Court

[6] https://www.geo.tv/latest/646956-imaan-mazari-husband-hadi-chattha-sentenced-to-10-years-in-controversial-tweets-case
[7] https://www.brecorder.com/news/40371948/ppf-expresses-alarm-over-ban-on-27-youtube-channels
[8] https://www.thenews.com.pk/print/1275885-man-arrested-under-peca-law-for-insulting-maryam-on-social-media
[9] https://www.dawn.com/news/1974924
[10] https://www.dawn.com/news/1964527#:~:text=Muhammad%20Akbar%20Notezai%20of%20this,were%20later%20suspended%20upon%20appeal.
[11] https://www.geo.tv/latest/623077-senate-panel-rules-372-registered-under-peca-illegal-orders-immediate-withdrawal?utm_source=chatgpt.com
[12] https://thetruthinternational.com/ihc-journalists-association-challenges-controversial-peca-amendments/

against the amended law, contending it granted excessive censorship powers[13].

These challenges underscore ongoing constitutional debates over digital rights, freedom of expression, and executive reach.

Absence of a Comprehensive Personal Data Protection Law in Pakistan

Another critical challenge hampering digital safety is the absence of a personal data protection law in Pakistan. Despite significant digital growth, Pakistan does not yet have an enacted and operational Personal Data Protection Act that establishes enforceable privacy safeguards, independent oversight, and clear standards for data collection, processing, storage, and sharing. While draft proposals have circulated in recent years, the absence of binding legislation creates a structural imbalance within the digital regulatory ecosystem[14].

This gap is particularly significant in light of the broad investigative and surveillance powers granted under the Prevention of Electronic Crimes Act. PECA empowers law enforcement agencies to collect, access, and retain digital information during investigations. However, without a comprehensive data protection framework, these powers operate in a regulatory vacuum lacking:

- Clear limitations on data minimisation;
- Defined retention periods;
- Independent supervisory oversight;
- User notification requirements;
- Remedies for unlawful data collection or misuse;
- Strong safeguards for sensitive or personal data categories.

In effect, Pakistan's digital governance model currently emphasises enforcement authority without a parallel rights-protection architecture. This imbalance risks undermining constitutional protections of privacy and due process.

The Case for a Rights-Based Reform Framework

A rights-based approach to PECA reform recognises that security and freedom are not mutually exclusive. In fact, durable security depends on public trust, legal clarity, and institutional accountability.

Reform must therefore pursue three core objectives:

1) Precision in Criminal Law – Offences must be clearly defined and limited to conduct that causes demonstrable harm.
2) Strong Procedural Safeguards – Enforcement must be subject to judicial oversight, due process, and transparent review mechanisms.
3) Institutional Independence and Accountability – Regulatory bodies must operate impartially, with clear reporting obligations to Parliament and the public.

Rather than expanding criminalisation of speech, Pakistan's digital governance framework should focus on combating genuine cyber threats such as financial fraud, data breaches, child exploitation, and cyber terrorism — areas where robust enforcement enjoys broad consensus.

At the same time, alternative non-criminal approaches including digital literacy programs, platform accountability mechanisms, and co-regulatory models offer more sustainable responses to misinformation and harmful content.

[13] https://dunyanews.tv/en/Pakistan/866716-pfuj-challenges-peca-in-islamabad-high-court

[14] https://www.thefridaytimes.com/12-Oct-2025/pakistan-s-digital-vulnerability-urgent-need-strong-data-protection-laws

Key Reform Recommendations and Actions: Rights Based Reform for PECA

The recommendations presented in this chapter are grounded in a comprehensive evidence-based review of Pakistan's digital regulatory framework, particularly the post-2025 amendments to the Prevention of Electronic Crimes Act (PECA). They are informed by key informant interviews (KIIs) with constitutional lawyers, digital rights advocates, journalists, human rights defenders, and civil society experts, as well as focus group discussions (FGDs) with media practitioners and civic actors. These engagements highlighted practical challenges in PECA enforcement, including the criminalisation of online expression, arbitrary arrests, content-blocking practices, and threats faced by human rights defenders in digital spaces.

Additionally, the recommendations draw upon a detailed literature review of legal analyses, policy reports, and international best practices, complemented by the examination of post-2025 PECA cases, such as the blocking of online channels and the sentencing of human rights lawyer Imaan Mazari and Hadi Chattha. By synthesizing these insights, the recommendations aim to provide a rights-based, actionable reform framework that balances the legitimate need for cybercrime enforcement with the protection of freedom of expression, privacy, and civic participation. They integrate constitutional safeguards, international human rights standards, and mechanisms for independent oversight to strengthen Pakistan's digital governance ecosystem.

These recommendations are directed primarily at key decision-makers and stakeholders responsible for Pakistan's digital governance. Parliament and legislative bodies are encouraged to consider reforms that align PECA with constitutional guarantees and international human rights standards. The Ministry of Human Rights is tasked with leading the development and implementation of the Human Rights Defenders Protection Mechanism, integrating digital safety measures into the National Action Plan, and providing legal aid and protection support to HRDs.

Regulatory authorities, including Social Media Protection and Regulatory Authority (SMPRA), are expected to adopt independent, transparent, and accountable practices in monitoring digital platforms and enforcing PECA provisions. The judiciary plays a crucial role in safeguarding due process, reviewing content-blocking decisions, and ensuring fair trial rights. Also, National Commission for Human Rights (NCHR) and National Commission for the Protection of Journalists and Media Workers (NCPJMW) play their role to strengthen independent oversight; ensure accountability in PECA enforcement; provide rapid support to journalists and HRDs facing threats; protect press freedom and civic participation.

Finally, civil society, media advocacy groups, and technical experts are essential partners in monitoring enforcement, providing evidence-based input, and supporting co-regulatory and digital literacy initiatives. Together, these stakeholders form the multi-layered governance ecosystem that can implement the recommendations effectively, balancing the legitimate need for cybercrime enforcement with the protection of freedom of expression, privacy, and civic participation.

Objective	Recommendation	Rationale / Details	Expected Impact
1. Precision in Criminal Law	Redefine "false or fake information" offences (Section 26-A)	Limit criminal liability to intentional and provable harms (e.g., fraud, incitement to violence, public harm). Remove vague definitions and criminal penalties for mere misinformation. Ensure necessity and proportionality standards are applied.	Prevent arbitrary prosecutions; safeguard journalism, political commentary, and civic discourse.
	Decriminalise online defamation under PECA	Shift defamation to civil remedies; arrest only if linked to threats, extortion, or violence.	Prevent harassment of journalists, HRDs, and citizens; prevent strategic lawsuit against public participation-type misuse.
	Clarify "national security," "public order," and enforcement scope	Restrict enforcement to imminent threats, terrorism, or public disorder. Explicitly protect criticism of officials, institutions, and public policy.	Reduce overreach; protect freedom of expression and dissent.
	Restrict complainant scope	Amend law to ensure only legitimate aggrieved persons or entities may file complaints; remove open-ended "any person or organisation" definitions.	Prevent misuse by third parties or state entities to target activists, journalists, or critics.
2. Procedural Safeguards	Mandatory judicial approval for FIRs, arrests, and content takedowns	Magistrate or independent prosecutor review required for speech-related offences; content removal or blocking must have judicial authorization. Emergency blocks permitted for max 48 hours.	Ensure due process; prevent arbitrary enforcement; protect civil liberties.
	Right to notice and appeal	Notify affected parties prior to enforcement; establish independent Digital Rights Appellate Tribunal with review by High Courts.	Enhance fairness, transparency, and reduce chilling effect on civic participation.
	Safeguards on device searches and data access	Warrants must specify scope; enforce data minimisation, retention, deletion, and confidentiality safeguards.	Protect privacy, HRDs, journalists, and confidential communications.
	Law enforcement procedural safeguards	Strengthen rules for National Cyber Crime Investigation Agency (replacing FIA Cybercrime Wing); require clear warrant procedures and	Prevent misuse of investigative powers; protect constitutional rights.

		independent review for surveillance or investigation.	
3. Institutional Independence and Accountability	Reconstitute SMPRA / Regulatory Bodies as independent	Include judiciary, civil society, media, and technical experts; fixed tenure, transparent reporting, and judicial oversight of content blocking/removal.	Reduce executive dominance; improve accountability and legitimacy.
	Establish Digital Rights Ombudsperson	Investigate misuse, review enforcement trends, report annually.	Provide non-judicial oversight; enhance public trust.
	Mandatory transparency reporting	Quarterly disclosure of FIRs, arrests, content removals, blocked platforms, and demographic data.	Enable monitoring by Parliament, civil society, and independent experts; deter arbitrary enforcement.
4. Protection of Human Rights Defenders (HRDs) and Journalists	Media and HRD protection clauses	Explicit protection for journalists, lawyers, and civil society actors from prosecution for good-faith reporting, research, or advocacy. Judicial scrutiny before accessing communications.	Safeguard freedom of expression; reduce chilling effect; protect confidential sources.
	Anti- Strategic Lawsuit Against Public Participation provisions	Early dismissal of vexatious complaints; cost penalties on abusive complainants; prevent harassment through PECA misuse.	Deter misuse; protect civic participation and public accountability.
	National HRDs Protection Mechanism (MoHR-led)	1) Develop National Human Rights Defenders Policy guided by NCHR guidelines. 2) Integrate digital rights reform actions into the MoHR National Action Plan for Safe, Protected, and Inclusive Digital Space. 3) Provide legal aid and protection support to HRDs facing threats due to their work.	Institutionalize protection for HRDs; ensure state support for civic actors; mitigate risk from PECA misuse or other threats.
	Add Chapter on Safe Digital Society in Pakistan in MoHR's Human Rights National Action Plan	Pakistan's digital regulatory framework currently emphasizes enforcement under PECA without a parallel rights-protection strategy. Integrating a dedicated "Safe Digital Society" chapter within the MoHR' Human Rights National Action Plan would institutionalize a preventive, rights-based approach to digital governance.	This reform would shift Pakistan's digital governance from reactive enforcement to proactive protection of rights and safety. It would enhance public trust, strengthen institutional accountability, and reduce misuse of cyber laws against journalists and human rights defenders.

	Role of NCHR and NCPJMW in PECA oversight and protection	NCHR to monitor PECA enforcement trends, provide recommendations, and safeguard constitutional rights of citizens affected by digital regulation. NCPJMW to track cases against journalists and media workers, provide legal and safety support, and advise regulators on media-specific enforcement policies. Both bodies should be formally linked to oversight mechanisms for SMPRA and Digital Rights Appellate Tribunal.	Strengthen independent oversight; ensure accountability in PECA enforcement; provide rapid support to journalists and HRDs facing threats; protect press freedom and civic participation.
5. Alternative Non-Criminal Approaches	Co-regulation with platforms	Develop voluntary but enforceable content moderation codes, fact-checking, and labeling instead of removal.	Reduce reliance on criminalisation; protect speech while managing harmful content.
	Digital literacy and awareness programs	Nationwide public campaigns, school curricula, and training initiatives for critical evaluation of online content.	Empower citizens; reduce societal harm from misinformation.
	Personal Data Protection Act (PDPA)	Enact law establishing independent data protection authority, retention limits, user notification, remedies, and safeguards for sensitive categories (political opinion, HRD communications).	Protect privacy, confidential sources, and HRDs; align PECA enforcement with rights-based governance.
6. Focused Cybercrime Enforcement	Prioritise genuine cybercrime threats	Focus enforcement on fraud, cyber terrorism, child exploitation, and serious data breaches; avoid overcriminalisation of speech.	Efficient allocation of enforcement resources; protect public trust.
7. Legislative and Oversight Reform	Periodic parliamentary review and consultation Half Yearly Report to Parliament under Section 53 of PECA	NCCIA ensure compliance of Section 53 by submitting Half Yearly Report to Parliament. Annual review of PECA enforcement; require transparent stakeholder consultation (civil society, journalists, tech industry, human rights experts) for amendments or drafting new provisions.	Institutionalise accountability; ensure law evolves with technology and aligns with constitutional and international standards.
8. Alignment with International Human Rights Standards	Compliance with ICCPR Article 19 and other treaties	Ensure all definitions, penalties, enforcement mechanisms, and content-blocking measures are lawful, necessary, proportionate, and time-limited.	Enhance Pakistan's international credibility; prevent rights violations and judicial challenges.

Purpose and Structure of Policy Paper

The policy paper provides a comprehensive roadmap for reforming PECA within a constitutional and human rights framework. It examines substantive legal provisions, procedural safeguards, institutional design, and oversight mechanisms. It also outlines phased implementation strategies to ensure smooth transition toward a more balanced digital regulatory system.

The aim of this policy paper is to strengthen the legitimacy, clarity, and effectiveness of the law by aligning it with constitutional guarantees and democratic values.

In the digital age, the credibility of governance depends not only on security enforcement but also on protection of civic space. Reforming PECA presents an opportunity to modernise Pakistan's cybercrime framework while reaffirming commitment to constitutionalism, rule of law, and fundamental freedoms.

