Pakistan Journal of Criminology
Vol. 17, No. 01, January—March 2025 (167-170)

Short Essay
2025 Amendments to the Prevention of Electronic Crimes Act, 2016: An Introduction

Kamran Adil

Introduction

On 29th January 2025, new amendments were enacted to the Prevention of Electronic Crimes Act, 2016 (PECA). For context, it may be recalled that the PECA is the primary legislation on cybercrimes and cybersecurity in Pakistan. As it defines cybercrimes and provides standards for cybersecurity, it is omnibus in nature when it comes to the law related to cyberspace in the country. In addition, the PECA is a criminal law and provides for criminal liability in cyberspace, therefore, any tweaks in it, undoubtedly, invite attention and generate discourse. Presently, the discourse about the new amendments to the PECA has predominantly revolved around two themes: first, the right to freedom of speech, and second the security concerns emanating out of misinformation and disinformation caused through the use of social media platforms. While the two themes are very important and do cut at the heart of the debate, the legal content of the amendments needs an objective assessment. For this, one needs to understand the amendments, as they are, and to firm up an opinion that may inform citizens' perspectives. The legal content of the amendments is, therefore, examined in this write-up followed by general observations.

Salient Features

The salient features of the 2025 amendments to the PECA are:

Definitional Aspects

Definitional provisions in modern legislation are conceptual in nature; more often than not, these set the limits of inclusion and exclusion. Lawyers tend to use definitions for examining the scope and subject of the law insofar as its application is concerned. The new amendments amend section 2 of the PECA and provide nine new 'definitions'. These definitions are mostly linking in nature as these link the newly added concepts to the later part of the legislation. However, among these definitions, the most substantial are three concepts of 'aspersion' (primarily triggered by defamation-related concerns), 'complainant' (including non-victims in the definition to expand its meaning enabling anyone to make an application), and the term 'social media platform' to include both a natural person as well as a legal person (corporate body or website or mobile web application). The definition of 'social media platform' has significant consequences from the viewpoint of criminal liability and the moot question that will be addressed by the courts would be to ascertain the extent of liability for owners, content creators, service providers, hosts of information and the intermediaries that partake the whole information generation and sharing chain.

Establishment of New Structures

The 2025 amendments to the PECA establish the following structures:

i. The Social Media Protection and Regulatory Authority

By adding two new Chapters 1-A and 1B to the PECA, the Federal Government has been authorized to establish a new Social Media Protection and Regulatory Authority (SMPRA) and to provide for a system of enlistment for social media platforms, respectively. The SMPRA shall be a body corporate with functions to, inter alia, ensure 'online safety' and 'regulate the unlawful or offensive content' on the social media. It has also been assigned the function of 'enlistment' of social media platforms. The powers of the SMPRA authorize it to 'issue directions… to block or remove the unlawful or offensive content' within thirty days. SMPRA is also authorized to carry out 'international cooperation' with other agencies. The SMPRA shall comprise nine persons including a Chairman. The law provides, in detail, the qualifications and process for the composition of the SMPRA. There is a conflict of interest provision that bars members of the SMPRA from engaging in any 'media related businesses (sic)'. The SMPRA will meet its financial needs from the newly established Social Media Protection and Regulatory Authority Fund. The accounts of the SMPRA shall be auditable. The Federal Government has been given the power to issue directions to the SMPRA, which shall be binding on it. Through inserting new section 2-Q, the SMPRA may require enlistment of social media platforms/outlets. Section 2-R is the most empowering as it authorizes SMPRA to issue directions for the removal/blocking of online content. The power is not general in nature but has been tied to meet different criteria like it should not incite people to commit violence, or to incite hate, or should not contain obscene or pornographic material. The law specifically provides that the duly expunged material discussed on the floor of the parliament shall not be streamed on social media platforms.

ii. The Complaint Redress Mechanism

The complaint redress mechanism of the PECA has been strengthened. For self-accountability, section 2-S provides that each social media platform must provide for a complaint redress mechanism against unlawful or offensive content. For the third-party sort of accountability, section 2-T provides a five-member Social Medial Complaint Council (SMCC) to be established by the Federal Government to receive complaints made by the general public against the violation of the PECA.

iii. The Social Media Protection Tribunals

For adjudication, the new amendments add new Chapter 1-C to the PECA. Section 2-V provides for Social Media Protection Tribunals (SMPTs) comprising three members: one with a law background; one with journalistic credentials and one with an information technology background. Persons aggrieved by the decisions of the SMPRA may prefer an appeal to the SMPTs. The SMPRA may also reach out against persons for not implementing its directions.

iv. The National Cyber Crime Investigation Agency

The law provides for the establishment of the National Cyber Crime Investigation Agency (NCCIA) that will substitute the extant Cyber Crime Wing of the Federal Investigation Agency (CCW-FIA). The NCCIA shall be headed by a Director General for a non-extendable three years period who shall have powers of the Inspector General of Police (as contained in the Police Order, 2002). The NCCIA has been given the power to establish its own forensic analysis lab that may generate reports, which shall be admissible in a court of law. Section 30 of the PECA which had earlier authorized police and FIA to investigate cyber crimes has been amended providing exclusive powers to the NCCIA to investigate cybercrime-related cases.

Criminalization of False and Fake Information

The new amendments introduce section 26-A to the PECA criminalizing 'intentional' dissemination of false and fake information. The quantum of corporal punishment has been increased to three years while the fine has been increased to two million rupees.

GENERAL OBSERVATIONS

Some general observations about the amendments are:

1. Reactionary Nature of Cyber laws

Policing cyberspace is evolving and has started occupying a central place in the national security paradigm of many a country; Pakistan is no exception. The technology-driven cyberspace is always ahead of the law-making, and more often than not, the law is reactionary (and not responsive) to the emerging challenges of cyberspace. Against this background, the amendments to the PECA should be appreciated as an evolutionary legislation trying to react to emerging challenges.

2. Composite Law on Cybercrime and Cybersecurity

The cybercrime and cybersecurity are two different regimes; the former affects the rights of individuals whereas the latter affects the information systems. In the context of Pakistan's federalist constitutional law, cybercrime being a species of criminal law is the concurrent legislative subject under articles 142 and 143 of the Constitution of Pakistan while cybersecurity better subsumes in items 1 (defence) and 7 (wireless and communications) of the Federal Legislative List as contained in 4th Schedule. Nonetheless, due to the composite nature of the PECA, the cybersecurity aspect overwhelms the cybercrime part. The net result is that the PECA is perceived as state-centric. Any measure to protect cybersecurity (by extension defence-related) is seen differently and the standard of the fundamental rights is applied in total disregard to article 8 of the Constitution that precludes (applicability of the fundamental rights standards to) defence.

3. Pre-judging the New Structures

The infrastructure of the governance and the cyberspace related justice system are in evolution. The PECA morphed out of the Prevention of Electronic Crimes Ordinance, 2007 and imagined working through the conventional structures for regulation and adjudication. But the time has shown that the PECA requires

dedicated structures for its governance and adjudication. Accordingly, the new amendments try to address this and only after the formation/establishment of the new structures any inference can be drawn about their utility.

4. Misuse of Law

Many laws vested powers in the executive and entrusted jurisdictions to courts, but were misused. The argument of misuse of laws holds true for most if not all, legal powers in Pakistan where under Article 184(3) of the Constitution, even the judges of the Supreme Court abused their legal powers. The structures under the new law have yet to be established and pre-judging these before their inception would be reading too much into the intention of the legislature.

5. Policing Cyberspace

In the era of global tech wars, there is need to have specialist approach towards the areas of cybercrimes and cybersecurity. Vesting the powers to work on both in one body i.e. NCCIA is a good starting point. There is need to invest generously in establishment of the NCCIA so that it can cater to citizens' needs and to the national security requirements. Half-hearted efforts by episodic funding are likely to sap the energy required to establish robust institutions.