The Prevention of Electronic Crimes (Amendment) Act, 2025

DRF Analysis and Recommendations

Context:

Following their return to power, the ruling government has been focused on regulating the internet, in what is being pitched as their battle against organized disinformation perpetuated by some political actors against state authorities. Over the past year, multiple initiatives were undertaken including the enactment of the Punjab Defamation Act, the installation of a Chinese firewall (referred to by authorities by the more anodyne "Web Management System"), and the regulation of Virtual Private Networks (VPNs). In December 2024, amid controversy around the number of casualties of opposition party workers at the hands of security forces during their protest rally, the Prime Minister launched a high-level taskforce to tackle "fake news" and "anti-state" propaganda. Furthermore, the government announced its plans to amend the Prevention of Electronic Crimes Act (PECA) 2016, to further tighten the noose around "fake news" as they so construed. Following their announcement and despite repeated inquiries about the proposed amendments, government officials remained evasive and did not share the contents of the proposed amendments with civil society organizations. Eventually, on 22 January, Law Minister Azam Nazir Tarrar tabled the draft of PECA amendments in the National Assembly, and the amendments were approved in a day by the assembly amid concerns of opposition lawmakers and civil society. The next step

for the bill is for it to be tabled in the Senate. If the Senate approves it without proposing any changes, it will go to the President for formal assent before coming into effect. The draft is unlikely to face much resistance in the Senate amid reports of how the coalition government, with significant influence in the Senate, are on one page on the proposed amendments. Based on the draft available on the National Assembly's website, DRF has prepared a short legal analysis of the contents of the recent PECA amendments.

Concerns pertaining to the PECA Amendment Act 2025

1. **Overbroad and Vague terms:**
    - **Impact of the term "Aspersion" Insertion (Section 2):** The proposed insertion of clause (iiia) in the PECA introduces the term "aspersion," defined as "*spreading false and harmful information which damages the reputation of a person*." This addition revives the same issues that led to the unconstitutionality of Section 20 (cyber defamation) of the PECA. Section 20 was struck down by the Islamabad High Court, declaring the phrase *"harms the reputation"* inconsistent with the Constitution of Pakistan, 1973 due to its subjective nature.[1] The new amendment reintroduces a similar concept under the guise of "aspersion," which includes the same vague terms like *"false and harmful"* information. These terms will likely be interpreted subjectively, as was the case with Section 20, and could once again be weaponized as a tool for persecuting journalists, activists, dissenting voices, or anyone who challenges the status quo, similar to how

[1] The Pakistan Federal Union of Journalists through its Secretary General Versus the President of Pakistan through the Secretary & 4 others (Writ Petition No. 666/2022), Order Sheet dated April 8, 2022: https://digitalrightsmonitor.pk/wp-content/uploads/2022/04/PFUJ-v-The-President-of-Pakistan-etc-WP-No-666-of-2022.pdf

Section 20 was previously misused.[2] The broad wording can lead to government overreach and self-censorship. Citizens will refrain from speaking out on critical issues due to the fear of legal repercussions, while the law could be misused to target political dissent or criticism under the guise of protecting reputations.

- The amendment to the definition of "complainant" and the introduction of the term "person" under Section 2(1)(c) bring changes that impact various aspects. Previously, a complainant could report an offense they believed *"is being committed or likely to be committed"* but the amendment restricts this to offenses *"that have been committed,"* which means complaints based on anticipation or suspicion of future offenses are no longer valid. Additionally, the previous definition of complainant included *"any authority referring the complaint for investigation,"* meaning official bodies could initiate complaints. The amendment removes this provision, potentially limiting institutional intervention. However, this change must be viewed alongside and in the context of the newly introduced definition of "person," which now includes both natural and legal persons, such as corporate entities and political bodies. This new definition of person suggests that authorities have not been entirely excluded but rather repositioned under the category of "person," allowing them to file complaints from an institutional standing rather than in their previous capacity.

[2] https://cfj.org/wp-content/uploads/2023/10/Pakistan_PECA-Report_September-2023.pdf

2. **Expansion of the scope of the term "Social Media Platforms":** The Amendment redefines "social media platform" under Section 2 to include tools and software used to access social media. This change potentially gives the government powers to block or restrict the use of Virtual Private Networks (VPNs), which observed increased use after the government blocked X (formerly Twitter) (formerly Twitter) and during frequent internet shutdowns across the country. This shift will potentially create the necessary legal framework for the government, which they had previously indicated was unavailable to block VPNs.[3] If the government chooses to block or restrict VPN services under this new legal framework, it could directly affect the fundamental right to access information, especially given the frequent and often unexplained internet shutdowns in the country. Moreover, since VPNs are commonly used to safeguard privacy, limiting their use could lead to significant privacy violations for many individuals and organizations.

   Additionally, the new definition now includes any person who owns, provides, or manages an online information system, as well as "websites," "applications," or "communication channels" that allow individuals to access social media. This expansion raises significant concerns, as it could be used to justify more aggressive censorship or control over online speech. With this change, the government could now be empowered with broad powers to regulate, block, or remove online content even at platforms or services that are not traditionally considered social media but will now fall under scrutiny.

   The wording of Section b of 2(d), relating to "websites", "applications" et al, for example, includes "any other such application that permits a "person to become

[3] https://www.dawn.com/news/1875860

a registered user, establish an account, or create a public profile" for social media purposes. With the wording as it stands in mind, there is the concern that users who have registered with websites or apps for commercial or promotional purposes, such as for food or book deliveries, could have their inputted data and preferences potentially used against them e.g. having their access blocked to said apps or services. The lack of data protection legislation could also exacerbate this scenario, given that the wording does not provide provisions here in the event of identity theft and other forms of fraudulent exploitation of people's information.

With "communication channels", furthermore, there is the possibility that newsletters or mailing lists - as used by civil society or hobby groups for a myriad of innocuous purposes - could be included, given that they are a form of mass-communication, as per the overly broad definitions. Messaging services such as WhatsApp or Facebook Messenger, though end-to-end encrypted, could also fall under this category, given they can and are widely used for mass or group communications - a number of domestic and international media outlets and companies now utilize "WhatsApp Channels" for this purpose. Also, this broader definition could have far-reaching implications for the country's digital economy. Foreign tech companies that provide tools enabling access to social media might hesitate to operate in Pakistan due to the increased legal scrutiny risks, especially in light of continued government demands for localized data registration, regarding VPNs or other services.

3. **Establishment, Powers, and Composition of the Regulatory Authority:** The amendments propose the creation of a **Social Media Protection and Regulatory Authority under section 2** ('Regulatory Authority') with powers to monitor social media platforms, enforce compliance, and curb misinformation, hate

speech, and threats to national security through increased oversight of digital platforms. The establishment of the Regulatory Authority under Section 2A of the Amendment is set to replace the Pakistan Telecommunication Authority (PTA) (Section 2(1)(b)). According to Section 2B of the Amendment, the new authority will be tasked to ensure online safety (Section 2B(d)), regulate unlawful or offensive content on social media platforms (Section 2B(e)), and issue guidelines, directives and standards for social media platforms (Section B(i)). While these are important powers and functions, the setup of the Regulatory Authority raises serious concerns about the potential for more governmental control over digital spaces.

A key concern lies in the Authority's broad powers, particularly the power to partially or fully block social media platforms if they fail to comply with the provisions under this Act until compliance is made (section 2B(h)), which leads to the Authority keeping overarching powers over online spaces. Further, the power to initiate action on its own motion (Section 2B(t)) could lead to arbitrary enforcement. Also, the power to issue directions to authorities for blocking unlawful or offensive content (Section 2B(l)) without clear, narrowly defined criteria can result in excessive content takedowns. Furthermore, Section 2B(v), which allows the authority to perform any functions that are *"ancillary, incidental, or consequential,"* is overly vague and could be used to justify actions beyond the intended legislative purpose. Given these powers and the potential for misuse, especially when the definition of "unlawful online content" under section 2R is also expanded, the Regulatory Authority could become a tool for persecution. This opens the door to excessive censorship, with the potential for content to be removed or blocked without clear or objective standards as previously discussed.

Furthermore, the composition of the authority raises questions about its independence. According to Section 2C, the authority will consist of a chairperson and eight other members. One of the members will be the chairman of the PTA or someone he nominates. The federal government will appoint the Chairperson and five other members for three years based on their qualifications and experience. This structure makes it likely that the authority will be government-controlled and suggests the retention of control through the authority. As per the amendment, the chairperson also holds exclusive powers to perform which require immediate action including the issuance of direction for blocking of any unlawful online content (Section 2G(2)). This gives the Regulatory Authority significant control over what can be said or published online, posing the risk of censorship, especially when considering that "fake news" under the guise of unlawful content can be defined by the authority itself (Section 2R(g)).

Moreover, the law also grants excessive powers to the authority to remove or block access to content within 24 hours of receiving a complaint of fake news and fake information (section 2C). This rapid removal of content without sufficient scrutiny or oversight also raises concerns about the right to fair trial and accountability in the decision-making process as the other side is not given an opportunity to be heard, meaning they have no chance to present their case before such a harsh action will be taken.

4. **Unlawful and offensive Content:** The inclusion of 'unlawful and offensive content' within the definitions under Section (xxxva) as further elaborated in Section 2R, appears to be a direct replication of provisions from the Anti-Terrorism Act, 1997 (ATA). By duplicating the threshold definition of

'terrorism' from the ATA and applying it to 'unlawful content,' dangerously lowers the bar and opens the door to blatant misuse of authority. This definition significantly broadens the scope of restricted content far beyond the already expansive and arguable overreaching categories outlined in Section 37 of PECA and its rules, which themselves stretch the limitations of Article 19 of the Constitution. It creates a scenario where legitimate speech could be lawfully censored, including content that criticizes state institutions potentially being labelled as "aspersion". This addition could set an alarming precedent for curbing freedom of expression and dissent under the guise of legal protections.

5. **Fake or False information (Section 5):** Section 5 inserts Section 26(A) to the PECA to penalize the dissemination of "Fake or False information" including cases where an individual *"intentionally disseminates, publicly exhibits, or transmits any information through any information system, which he knows or has reason to believe to be false or fake and likely to cause or create a sense of fear, panic, disorder, or unrest in the general public or in society."* The law introduces severe penalties for violations, including imprisonment for up to three years, a fine ranging from one to two million rupees, or both. This language mirrors that of the Anti-Terrorism Act (ATA) and is again also incorporated into Section 10 of PECA. However, this creates a vague criminal offense, potentially weaponized to suppress accountability and construct malafide cases. The fear of such harsh penalties may intimidate individuals, discouraging them from speaking out or sharing information due to the looming threat of legal repercussions.

6. **Power of the Federal Government:** Under the previous framework of Section 37, the Pakistan Telecommunication Authority ('PTA') was empowered to operate independently, with Federal Government directives deemed non-binding. The IHC in 2018 reinforced this position, holding that "the federal government like

any other person can lay information before the PTA but the same cannot be treated as binding in the context of subsection (1) of section 37".[4] However, the insertion of section 20 shifts this balance by granting arbitrary powers to the Federal Government, effectively undermining the PTA's autonomy and raising serious concerns over unchecked executive influence.

7. **Jurisdiction and Procedural Barriers:** The insertion of Section 2X represents yet another example of overreach in expanding jurisdiction. Section 2X inexplicably directs appeals of final decisions directly to the Supreme Court, bypassing the natural progression of cases via High Courts which are accessible to Pakistani citizens across all provinces. The removal of this crucial step creates significant barriers to justice, as the Supreme Court is neither accessible nor practical for the majority of litigants.

8. **Federal Government's Expanded Powers in Appointment Process Threaten Tribunal and Complaint Council Independence:** The Amendment establishes a Social Media Complaint Council under Section 2T, comprising a chairman and four members, all appointed by the Federal Government. Moreover, it creates a tribunal to address non-implementation of the authority's directives, with tribunal members appointed by the Federal Government. This heavy involvement of the Federal Government undermines the autonomy and independence of these bodies, raising serious concerns about overreach and potential bias in the regulatory framework.

9. **Legalization of Overreach and Unlawful Practices by Law Enforcement Agencies:** The Amendment also introduces that investigation teams may seek

[4] https://www.dawn.com/news/1828972

assistance from any intelligence agencies marking a significant shift. Previously, the inclusion of an intelligence agency in the Joint Investigation Team (JIT) under PECA was challenged in the Supreme Court,[5] where it was argued that such involvement exceeded the law's scope. This inclusion appears to be an attempt to retroactively legitimize a practice that was previously beyond PECA's legal framework.

10. **NCCIA:** The National Cyber Crime Investigation Agency ('NCCIA') was introduced in 2024 via an SRO, which directly conflicted with the PECA 2023 Amendment. Although its powers were later revoked and reassigned to the FIA, the proposed amendments now pave the way for the NCCIA's resurgence under Section 29, effectively seeking to establish its legal legitimacy once again.

NOTE: An inconsistency arises as the statement of objects and reasons continues to reference the DRPA as the authority, and also, there appears to be a clerical error in Section 2(1)(c) of the Amendment as it is repeated twice within the text. These errors need to be corrected and removed to avoid any confusion or ambiguity.

[5] https://www.supremecourt.gov.pk/downloads_judgements/s.m.c._4_2021_11032024.pdf

Overlooked International Frameworks in the Drafting of The Amendment

1. International law does not explicitly define terms like "fake news," "harmful content," or "unlawful content" but provides principles and frameworks for states to draft laws that balance the protection of freedom of expression and the need to address harmful propaganda or disinformation. These frameworks stem from key international treaties such as the **Universal Declaration of Human Rights (UDHR)** and the **International Covenant on Civil and Political Rights (ICCPR)**, of which Pakistan is a signatory, this also includes interpretations by international human rights bodies.

2. **Freedom of Expression (Article 19, ICCPR)**:
    - Protects the right to seek, receive, and impart information and ideas.
    - Restrictions on expression are permissible only when:
        - Provided by law.
        - Necessary for respect of the rights or reputations of others.
        - Necessary for the protection of national security, public order, or public health or morals.

3. **Legitimate Limitations**:
    - General Comment No. 34 of the UN Human Rights Committee emphasizes that any restriction must be clear, precise, and necessary.
    - Vague terms like "fake news" should be avoided unless precisely defined to prevent misuse.

4. **Proportionality Principle**:
    - Measures to address harmful content must balance public interest with individual freedoms.
    - Overbroad or blanket bans on content are discouraged.

5. **Avoiding Censorship**:
    - Any regulation must avoid stifling dissent or enabling government overreach.
    - Definitions must not be used to target political opposition, journalists, or activists.