

Redefining Electronic Crimes Or Protecting Digital Rights: Prevention Of Electronic Crimes (Amendment) Act 2025, Challenges And Way Forward

Syed Shaharyar Ahmed	Partner at Ibrar Law Associates, Lahore, Pakistan shaharyargcu@gmail.com
Muhammad Umar Zahid	Senior Lecturer, College of Law, The University of Lahore muhammad.zahid@law.uol.edu.pk
Sundus Rauf (Corresponding Author)	Associate Professor, M A Raoof College of Law, The University of Lahore sundas.rauf@law.uol.edu.pk

Abstract: *It has become difficult to strike a balance between ensuring cybersecurity protection and safeguarding digital rights, as the digital landscape in Pakistan continues to evolve. The Prevention of Electronic Crimes (Amendment) Act 2025 is another attempt in this direction. This amended has been intended to address the emerging concerns regarding disinformation, cybercrimes, online harassment, and data breaches. However, this amendment has also sparked concerns over its jurisdictional overreach by scrutinizing the exercise of fundamental freedoms, for instance, freedom of speech and expression. Furthermore, the law has been criticized for its ambiguous language and lack of procedural clarity. This paper critically examines the amendments made to the existing Prevention of Electronic Crimes Act (PECA), in accordance with constitutional rights protected by the Constitution of Pakistan, international legal frameworks and comparative cybercrime frameworks. The pressing issues concerning jurisdictional challenges, pertaining to extraterritorial offences, liability of intermediaries, as well as the role of newly established authorities such as Social Media Protection and Regulatory Authority (SMPRA) and the National Cyber Crime Investigation Agency (NCCIA) will be discussed. The research further analyses how the redefined concepts of “electronic crimes” could risk penalizing dissent or legitimately exercised digital freedom. The papers conclude with proposing a balanced approach which incorporates judicial oversight, effective procedural frameworks, as well as consultation with relevant stakeholders so that the digital security and protection of fundamental rights of citizens interacting within Pakistan’s digital ecosystem could be ensured.*

Keywords: Electronic crimes, digital rights, PECA, cyber-crime, disinformation

Introduction

The technological advancements and digitalization have obliged countries across the world to regulate the digital cyberspace effectively. In this regard, a novel attempt was made by Pakistan through the enactment of Prevention of Electronic Crimes Act (PECA) 2016, a landmark legislation which primarily aimed at curbing the growth of cybercrimes, such as hacking, cyber harassment, identity theft and online terrorism. Therefore, the enactment of PECA 2016 laid the foundation for a new regulatory regime governing cybercrime in Pakistan which filled the existing vacuum in Pakistan’s legal framework. Through this enactment, the Federal Investigation Agency (FIA) was empowered as being the primary investigation authority, meanwhile, regulatory powers were granted to the Pakistan Telecommunication

Authority (PTA) in order to oversee online content and digital cyberspace (Iqbal, 2023).

However, with the passage of time, PECA 2016 received criticism from human rights activists, members of civil society, and legal experts who were of the opinion that the legislation was poorly drafted and prone to abuse. The Act was used to suppress dissent, or to arbitrarily restrict the dissemination of online content. Furthermore, as cyber crimes evolved, from misinformation, financial scams to state-sponsored cyberattacks, the PECA 2016 enactment started to become inadequate and inefficient in terms of providing enforcement mechanisms and appropriate protection. This contextual background served as the basis for enactment of Prevention of Electronic Crimes (Amendment) Act, 2025 which was aimed at redefining key offences, expanding procedural authority, and making sure the law is in conformity with the global digital landscape (Iqbal, 2023).

The PECA (Amendment) 2025, has led to a paradigm shift in digital regulation landscape. While it intended to revamp Pakistan's cyber laws through incorporating redefined terms and offences, establishing new law enforcement agencies and tribunals, and addressing transnational cyber threats, it has equally triggered a renewed tussle concerning the balance between digital civil liberties and state security. Critics are of the view that through the Amendment Act of 2025, powers of the executive bodies have been drastically enhanced without adequate judicial oversight, specifically in the domains of content management, digital surveillance and data handling. For instance, as per Section 37 of this Amendment, the Social Media Protection and Regulatory Authority (SMPRA), is empowered *"to 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."*

This research paper intends to dissect and determine whether the Prevention of Electronic Crimes (Amendment) Act 2025 is a progressive step towards curbing electronic crimes or if it is a legislative tool to impose digital surveillance and content moderation, thereby curbing the fundamental freedoms guaranteed to the citizens of the country under the guise of national security. This paper will determine the constitutional, jurisdictional as well as enforcement implications of the 2025 Amendment Act, while assessing the legal, technical and structural challenges it faces.

1. NEW DEFINITIONS IN PREVENTION OF ELECTRONIC CRIMES (AMENDMENT) ACT 2025

The PECA (Amendment) Act 2025 came roughly after a decade of the original PECA 2016 enactment. The 2025 Amendment is a legislative response towards emerging digital threats like deepfake technology, AI-generated misinformation, frauds involving blockchain and cryptocurrency as well as transnational cyberattacks. Although, the amendment was intended to modernize Pakistan's cybercrime legal framework, it has raised concerns owing to expanded state discretion and perceived consequences for fundamental rights. Additions have been made to the definitions clause, provided under Section 2 of the Amendment Act 2025, wherein several new key terms have been introduced and defined. These are: -

- *"aspersion" means spreading false and harmful information which damages the reputation of a person.*
- *"Authority" means the Social Media Protection and Regulatory Authority established under section*
- *"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;*
- *"inquiry" includes every inquiry conducted by an investigation agency on a complaint made*

in writing

- *complainant*” means any person who makes complaints of any offence under this Act 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;
- “Unlawful or offensive content” means the offence as defined in section 2R
- “Sexually explicit conduct” means actual or simulated-sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; or (a) bestiality; or (b) masturbation; or (c) sadistic or masochistic abuse; or (d) lascivious exhibition of the anus, genitals, or pubic area of any person
- “Sexual abuse of a minor” shall have the same meaning given to “sexual abuse” in section 377A of the Pakistan Penal Code (Act XLV of 1860)
- “Social media platform” means (a) any person that owns, provides or 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.

The term “*aspersion*” has been defined in a vague and diversified manner, and this could be used negatively to falsely accusing someone of hurting reputes of a person or spreading fake news. Similarly, it is interesting to note that the term “*complainant*” has been redefined and now it includes a non-victim person as being a valid complainant. So, anyone can now lodge a complain of any offence under this Act, irrespective of whether or not he is the victim of such offence. A positive development is the elaboration of sexually explicit content and penalizing the dissemination of such actions. Similarly, the concept of social media platforms has been elaborated in detail as to incorporate the major platforms such as Facebook, Instagram, YouTube and TikTok. However, the term “social media platform” has been redefined as to include both natural person as well as a legal person within its context. This could have serious implications from the standpoint of criminal liability and it would therefore, be difficult for the courts to determine the extent of liability of owners, content creators, service providers, hosts of such information as well as the intermediaries which are involved in the entire process of information sharing (Aslam et al., 2025).

2. ESTABLISHMENT OF NEW REGULATORY AUTHORITIES

Rather than reforming the existing regulatory authorities, new regulatory authorities have been established through the PECA 2025 (Amendment) Act. Through the insertion of Chapters 1-A and 1-B, the Federal Government has established a new Social Media Protection and Regulatory Authority (SMPRA) and provides for a system of enlisting social media platforms. Furthermore, under Chapter 1-C Social Media Protection Tribunal has been established. The adjudication power of Social Media Protection Tribunal has been made equivalent to that of a High Court, and an appeal against the decision of such Tribunal only lies before the Honorable Supreme Court of Pakistan as per Section 2X of the Amendment Act 2025. A brief account of these newly established regulatory bodies has been provided as follows: -

- **Social Media Protection and Regulatory Authority (SMPRA)**

This regulatory authority has been established as a body corporate having perpetual succession and therefore, may be sued or sue in its own name with principal office to be established in Islamabad. It

has been primarily tasked with “regulating the unlawful or offensive content” on the social media platforms. The SMPRA has been empowered to “issue directions, to block or remove the unlawful or offensive content” within thirty days under Section 2-R. Similarly, under Section 2-Q, SMPRA is required to enlist the social media platforms. Other major powers and functions include promoting education, research, awareness through social media platforms, ensuring online safety and protection of digital rights, issue guidelines and directives for social media platforms, proceed on applications made to it and prescribe fines for contravention of the provisions under Chapter 1-A and 1-B of the Act. Furthermore, it has been expressly provided that content expunged during discussion on Parliament’s Floor would not be uploaded on social media platforms. The complaint redressal mechanisms have been transformed through this amendment. The social media platforms are self-accountable, and under Section 2-S it is mandatory for every social media platform must provide for complaint redress mechanism against illegal or offensive content. A third party-based accountability mechanism has also been provided, under Section 2-T. A five-member Social Media Complaint Council (SMCC) has been established by the Federal Government in order to address the complaints received by it against alleged violations of the PECA.

- **Social Media Protection Tribunals (SMPT)**

A new adjudicatory body has been established under Chapter 1-C of the Amendment Act 2025 i.e., Social Media Protection Tribunals (SMPT). It has been provided by Section 2-V that these tribunals shall consist of three members, one with legal background; one with journalistic credentials while one form the domain of information technology. The appeals against the decisions made by the Social Media Protection and Regulatory Authority (SMPRA) can be made by aggrieved persons before the Social Media Protection Tribunals (SMPT). However, the appeal against decision passed by the SMPT only lies before the Honorable Supreme Court of Pakistan. In case of non-compliance made in implementation of decisions made by the SMPT, action can be taken against the persons involved.

- **National Cyber Crime Investigation Agency**

The existing Cyber Crime Wing of the Federal Investigation Authority (CCW-FIA) has been abolished and substituted with the establishment of National Cyber Crime Investigation Agency (NCCIA). The NCCIA has been mandated to have its own forensics lab established for analysis, the generated reports by which, shall be admissible before any legal forum. Furthermore, as per Section 30 of the PECA, the jurisdictional powers for investigation cyber-crimes, which was earlier vested with the authorized police officers and FIA, has been transferred to the NCCIA for exclusively exercising such powers while investigating cases involving cyber-crimes.

3. INTERMEDIARY LIABILITY AND PLATFORM REGULATION

The concept of intermediary liability and platform regulation has been introduced through the insertion of Section 37 of the PECA Amendment Act 2025. Accordingly, the social media bodies and digital platforms, collectively referred to as “intermediaries”, are now subjected to a diverse range of technical and legal obligations. For instance, they are tasked with content moderation according to Pakistan’s community guidelines. They have been mandated to establish local offices, as well as appoint redressal officers in Pakistan. Furthermore, they have to comply with the takedown requests made by the relevant regulatory authority, within tight time frames. These obligations are replica of India’s 2021 IT Rules, however in Pakistan’s case, the adequate procedural protections and judicial oversight is missing which has made its implementation more complicated (Aslam et al., 2025).

Furthermore, the vague language and unchecked discretion vested within Section 37 of the Amendment Act 2025, has been severely criticized. For instance, the key terms such as “unlawful”, “religious values”, “national interest”, “public morality”, and “public decency” lack clear and simple legal definitions. Consequently, any content which is critical towards the government or any other institution of the state, can be removed without any due process owing to the lack of proper definition of these key

terms. Furthermore, the amendment allows the SMPRA to take action suo-motu, while the same contradicts the judicial precedent established by the Islamabad High Court in the case of *Muhammad Ashfaq v. Federation of Pakistan (2020)*, which emphasized that content regulation must adhere to the fundamental rights and the Constitution.

4. DIGITAL RIGHTS AND CONSTITUTIONAL CONCERNS

The enactment of PECA (Amendment) Act 2025 and its implementation poses serious risks which could undermine the fundamental rights, specifically the freedom of expression, right to privacy and due process protected under Articles 19, 14, and 10-A of the Constitution of Pakistan 1973. Therefore, the implications need to be critically examined so as to avoid any violation of these fundamental rights.

- **Freedom of Expression and Censorship**

Through the 2025 (Amendment) Act, section 26-A has been introduced which has criminalized/penalized ‘intentional’ dissemination of false and fake information. Furthermore, the quantum of penal punished has been expanded to three years whereas the pecuniary sentence has been enhanced to two million rupees. This has directly impacted the freedom of expression. Not only sweeping powers have been granted to the SMPRA, the enhancement in penal punishments and extending the scope of criminal offences, has made this framework susceptible to gross misuse. It has been practically observed, that after the enactment of this legislation, many journalists, human rights activists and political statesmen have been facing digital censorship through online content takedowns, digital surveillance, and harassment by lodging bogus cases under this amendment (Aadil, 2025). The unchecked use of PECA for initiating criminal proceedings against online criticism of public offices has discouraged open discourse and dissent which are the hallmarks of a democratic nation (Aadil, 2025). While it is crucial to regulate the dissemination of harmful content in a digital society, the lack of independent judicial oversight over the SMPRA’s censorship and takedown decisions raises severe concerns regarding executive overreach and authoritarian control over digital spaces (Aslam et al., 2025).

- **Privacy and Surveillance: A Conflict with Articles 14 and 19**

Another concerning factor is the increase in the powers of state surveillance under the Amendment Act 2025, which is specifically disturbing when there is no data protection regime in Pakistan. As per the amendment, under sections 39 and 42, the SMPRA has the power to collect, retain and access user data and encrypted communications where the cases are involving issues of national security or “public interest” with minimal judicial scrutiny. These provisions are in stark contrast with the right to digital privacy and privacy in general enshrined under Article 14 of the Constitution. Such surveillance powers could potentially violate digital privacy and cause mass monitoring of online communications if done without warrants or adequate oversight mechanisms (Aadil, 2025). This is particularly concerning in a context where the global trend is shifting towards enhancing privacy protections by data protection laws while there is no such legal framework in Pakistan. Furthermore, the data retention period for internet service providers has been increased under the Amendment Act 2025, which has further enhanced the capabilities of state surveillance without adequate safeguards. The intersection of Articles 14 and 19 becomes relevant while surveillance tools are deployed for silencing dissenting voices under the guise of national security. Within this context, the amendment has failed to strike an intricate balance between legitimate state interests and fundamental rights of individuals (Shah & Butt, 2025).

- **Due Process and Fair Trial under the Constitution**

The Amendment Act of 2025, has also raised concerns regarding the due process and right to fair trial protected under Article 10-A of the Constitution. For instance, the creation of Social Media Protection Tribunals (SMPT), with members appointed by the executive rather than the judiciary, raises doubts regarding institutional independence and impartiality of such tribunals (Shah & Butt, 2025).

Furthermore, the shift from regular court jurisdiction to specialized tribunals, without sufficient measures for protections or judicial oversight, could result in decisions that are arbitrary and politically motivated. Lastly, there are certain offences which have been vaguely defined under the amended law, which makes it very complicated for individuals to determine whether the action is criminalized or not, which violates the principle of **legal certainty**, a core tenet of fair trial jurisprudence (Alexy, 2015).

5. COMPARATIVE LEGAL FRAMEWORKS: LESSONS FROM OTHER STATES

Since the digital crimes have transcended borders, states across the globe have enacted comprehensive legal frameworks for regulating digital cyberspace, for safeguarding user rights and ensuring national cybersecurity. In assessing the implications of PECA (Amendment) Act 2025, it is crucial to comparatively analyze Pakistan's legal approach with international standards and practices. Therefore, statutory instruments from countries such as India, European Union and USA have been analyzed to have a diverse perspective over the subject-matter.

• India's IT Act Amendments and Judicial Trends

India's legal response to cyber crimes regulation started through the enactment of Information Technology Act in 2000, following its subsequent amendments in 2008 and 2021. As per the recent Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, significant obligations have been imposed on social media platforms, which includes the appointment of redressal officers, traceability of messages, and removal of online content upon government orders (Thakkar, 2025). However, some of these regulations have been challenged before the appropriate forums and are still pending adjudication. Nonetheless, the judiciary's take on this matter has been clearly seen in the Indian Supreme Court's landmark decision in *Shreya Singhal v. Union of India (2015)*, in which the Court struck down the Section 66A of the IT Act for being violative to the freedom of speech (Thakkar, 2025). The judiciary emphasized that delegitimization of speech without clear standards is violation of fundamental rights. These trends highlight the need of similar adoption, likeminded judicial oversight, clarity in definitions, and supervision of executive discretion in Pakistan's PECA 2025 framework.

• The EU's Digital Services Act and User Rights Protection

The European Union's Digital Services Act (DSA), which was enacted in 2024, is globally leading the world in efforts towards regulating online platforms while protecting rights of users. Unlike PECA 2025 Act, which has vested powers in regulatory bodies with adequate procedural safeguards, the DSA is grounded in principles of accountability, transparency and due process (Husovec, 2024). The DSA provides for clear obligations of very large online platforms (VLOPs), it calls for mandatory transparency reports and strong protective measures have been provided for the freedom of expression, right to digital privacy and data protection under the EU Charter of Fundamental Rights and the General Data Protection Regulation (GDPR). Crucially, the state overreach has been limited by the DSA through ensuring that restriction on digital content or user data is subject to independent judicial scrutiny, which aligns with the international human rights standards. This European model established that it is possible to protect fundamental rights of users, while still effectively regulating the digital cyberspace (Husovec, 2024).

Through analyzing the legal frameworks of both India and the European Union, Pakistan can take a few lessons for shaping its cyber law framework, in order to ensure effective balance between state security and fundamental rights. In light of the Indian case law and the EU DSA framework mentioned, similar changes should be adopted in legal framework of Pakistan so that content takedown and surveillance could be subject to independent judicial scrutiny in order to prevent arbitrary or politically motivated action. Like the DSA, Pakistan should enhance procedural safeguards for users, for instance, the right to be informed about any content removal and the ability to challenge such decision before an impartial and independent forum. Vague and overly broad terms like "anti-state," "immoral," or "harmful"

should be replaced with narrowly defined categories of criminalized conduct, in order to comply with the principle of legal certainty. Both India and the EU have acknowledged the need of effective data protection laws. Pakistan's continued delay in enacting a Data Protection Act leaves users vulnerable to privacy violations under PECA, which needs to be addressed. Lawmaking in the digital sphere should involve not just state institutions but also members from the civil society, legal experts, tech companies, and common users, in order to ensure democratic legitimacy and efficacy of such legislative instrument.

6. CONCLUSION

It can be conclusively said that the Prevention of Electronic Crimes (Amendment) Act 2025 stands at the crossroads of two crucial imperatives which are enhancing cybersecurity and preserving digital rights. As Pakistan aims to modernize its legal framework in order to cope with emerging cybercrimes such as cyberterrorism, financial fraud, disinformation and online harassment, the amendment is a step in the same direction. However, the approach taken through this amendment has raised concerns regarding proportionality, balance, legality and potential violation of rights which are constitutionally protected. The analysis presented through this paper establishes that while PECA 2025 has introduced new concepts, new regulatory bodies and redressal system, it simultaneously widens the arbitrary powers of regulatory bodies, often at the expense of fair trial, freedom of expression and judicial oversight.

The amendment still does not address adequately the issue of privacy and personal data protection. In a jurisdiction without a comprehensive data protection law, granting law enforcement agencies broad surveillance powers without judicial oversight violates Article 14 (right to privacy) and Article 19 (freedom of expression) of the Constitution of Pakistan. The lack of public confidence in the state's digital governance is compounded by the absence of clear protective and transparent procedural documents, grievance mechanisms, and digital redress frameworks. Comparison with India or EU Member States show that effective digital regulation should aim to be clear and accountable, and center the individual. The Digital Services Act DSA of the European Union is an example of balanced regulation which guarantees platform responsibility and upholds user rights. Indian jurisprudence has also emphasized the need for judicial scrutiny and narrowly tailored constitutional restrictions on cyber law, demonstrated in landmark cases such as *Shreya Singhal v Union of India*. Thus, Pakistan has much to gain from these international approaches in recalibrating its strategy towards the electronic crime regulation.

It is evident that the PECA 2025 Amendment has tilted the balance too far, in favor of state power while violating fundamental freedoms. Although cybersecurity is undoubtedly crucial for ensuring national security and progress, however, it should not come at the cost of violating fundamental rights, democratic norms, and constitutional protections. Therefore, there is a dire need for introducing effective reforms, including the introduction of a comprehensive data protection framework, the establishment of impartial and independent oversight bodies, as well as the addition of judicial scrutiny in all processes concerning content regulation and digital surveillance. Lastly, Pakistan's digital future depends on its capability to create a legal ecosystem which is compliant, secure and rights-respecting. An inclusive and constitutionally sound cyber law regime is not only essential for individual freedom but also for building trust in digital institutions, encouraging innovation, and ensuring sustainable digital governance. Therefore, the way forward lies in accepting reforms which reflects both the threats of the digital age and the values of a democratic society.

BIBLIOGRAPHY

- Aadil, A. A. (2025). The law that listens, but doesn't speak: PECA 2025 and the Future of expression. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5251624>
- Alexy, R. (2015). Legal certainty and correctness. *Ratio Juris*, 28(4), 441–451. <https://doi.org/10.1111/raju.12096>

- Aslam, N. M. A., Kanrani, N. A., & Shehroz, N. M. A. (2025). Regulating misinformation or silencing dissent? A Constitutional Analysis of the PECA Amendments 2025. *the Critical Review of Social Sciences Studies*, 3(1), 1809–1815. <https://doi.org/10.59075/t1c1hz64>
- Husovec, M. (2024). Principles of the Digital Services Act. In *Oxford University Press eBooks*. <https://doi.org/10.1093/law-ocl/9780192882455.001.0001>
- Iqbal, M. (2023). The Prevention of Electronic Crimes Act (PECA) 2016 Understanding the challenges in Pakistan. *Siazga Research Journal*, 2(4). <https://doi.org/10.58341/srj.v2i4.35>
- Muhammad Ashfaq Jutt v Federal of Pakistan, W.P. No. 3028 of 2020. Retrieved from https://mis.ihc.gov.pk/attachments/judgements/W.P-3028-2020_637383806209679982.pdf
- Prevention of Electronic Crimes (Amendment) Act, 2025. Retrieved from https://khalidzafar.com/wp-content/files_mf/1747235902PECAamendment2025.pdf
- Prevention of Electronic Crimes Act, 2016. Retrieved from <https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-iiiiiijiiiiii>
- Shah, S. a. A., & Butt, M. N. (2025). Pakistan’s PECA 2025 and Global Digital Regulations: Balancing Security and Freedom. *Social Prism*, 2(01), 64–91. <https://doi.org/10.69671/socialprism.2.1.2025.28>
- Shreya Singhal v. Union of India, AIR 2015 SC 1523. Retrieved from <https://indiankanoon.org/doc/110813550>
- Thakkar, N. R. D. (2025). Legal Responses to Online Hate Speech in India: Evaluating Section 66A and the Supreme Court’s Judgment in Shreya Singhal v. Union of India. *Studies in Law and Justice*, 4(3), 26–30. <https://doi.org/10.56397/slj.2025.06.03>
- The Constitution of Islamic Republic of Pakistan, 1973. Retrieved from <https://www.pips.gov.pk/resources/the-constitution-of-the-islamic-republic-of-pakistan-31-05-2018-urdu>
- Pakistan Penal Code (Act XLV of 1860). Retrieved from <https://pakistancode.gov.pk/pdf/files/administratord5622ea3f15bfa00b17d2cf7770a8434.pdf>