

Suppression of Dissent in the Name of Cyberterrorism: A Critical Study of the Misuse of PECA 2016 Provisions and Their Impact on Human Rights

1. Dr. Hafiz Muhammad Abrar Awan

Assistant Professor, Department of Urdu Encyclopedia of Islam, University of the Punjab, Lahore, Pakistan.

Email: abrara.uei@pu.edu.pk

ORCID: <https://orcid.org/0000-0002-5345-8424>

2. Gulshan Rehman

Advocate High Court & Tax Consultant, Irfan & Farhad Law Associates, Lahore, Pakistan.

Email: Grehman136@gmail.com

3. Asma Rehman

Advocate, Lahore High Court, Lahore; Visiting Faculty Member, Law Department, Punjab University, Gujranwala Campus, Pakistan.

Email: Asmarehman014@gmail.com

Abstract

The Prevention of Electronic Crimes Act 2016 (PECA) was enacted in Pakistan to address cybercrime, interference with information systems, attacks on critical infrastructure, terrorism-related online activity, identity offences, electronic fraud, cyberstalking, and other harms arising from digital technologies. The legitimacy of regulating genuine cybercrime is not disputed. The central legal controversy concerns the breadth of certain speech-related provisions and the possibility that offences originally justified by cybersecurity, terrorism prevention, reputation, or public order may be applied to political criticism, journalism, human-rights advocacy, or other forms of dissent. This study critically examines sections 9, 10, 20 and, following the Prevention of Electronic Crimes (Amendment) Act 2025, section 26A, with particular emphasis on the relationship between “cyber terrorism”, glorification offences, allegedly false information, and constitutionally protected expression. The analysis is situated within Articles 14, 19 and 19A of the Constitution of Pakistan and Article 19 of the International Covenant on Civil and Political Rights. It evaluates the statutory language, judicial scrutiny, enforcement patterns, contemporary prosecutions, surveillance concerns, procedural safeguards, and the contrasting positions of the Government of Pakistan and international human-rights bodies. Particular attention is paid to the 2022 Islamabad High Court judgment concerning the PECA Amendment Ordinance, the United Nations Human Rights Committee’s 2024 observations, the expansion of PECA in 2025, and recent prosecutions involving social-media expression. The study argues that counter-cyberterrorism legislation is legally legitimate only when criminal liability remains closely connected to identifiable terrorist conduct, intentional incitement, serious threats, or protected national-security interests. Where broad concepts such as fear, glorification, anti-state expression, fake information, or reputational harm are disconnected from demonstrable harm and applied to peaceful criticism, the resulting criminal process risks creating a chilling effect inconsistent with constitutional and international standards of legality, necessity, proportionality, and fair trial. The study proposes narrowly defined offences, stronger judicial authorization, independent oversight, public-interest protections, enhanced evidentiary standards, and clear separation between terrorism-related cyber offences and ordinary political expression.

Keywords: PECA 2016, Cyber Terrorism, Freedom of Expression, Dissent, Human Rights, Pakistan, Online Speech, National Security, Cybercrime, Article 19

Introduction

Cybercrime legislation performs an essential legal function in a digitally dependent state. Unauthorized interference with critical infrastructure, online terrorist recruitment, cyberattacks against public institutions, identity theft, financial fraud, malicious interception, and technology-assisted exploitation require effective criminal-law responses. A democratic legal order is therefore not required to choose between cybersecurity and civil liberties; it must protect both.

The constitutional difficulty begins when offences designed for serious digital harms become capable of reaching ordinary expression.

Pakistan's Prevention of Electronic Crimes Act 2016 contains provisions dealing with unauthorized access to critical infrastructure, interference with data, glorification of terrorism, cyberterrorism, hate speech, personal dignity, cyberstalking, electronic fraud, and other offences. The Prevention of Electronic Crimes (Amendment) Act 2025 subsequently introduced further institutional and substantive changes, including section 26A concerning "false and fake information" and a new regulatory structure. The consolidated legislation remains in force as amended.

This study does not proceed from the assumption that every prosecution under PECA constitutes political repression. Cyberterrorism, terrorist propaganda, targeted harassment, criminal threats, and deliberate dissemination of harmful falsehoods can raise legitimate legal concerns. Instead, the article tests a narrower proposition: whether the breadth of certain PECA provisions, combined with enforcement practices documented by courts, international bodies, journalists, and human-rights organizations, creates an identifiable risk that legitimate dissent may be reframed as cybercrime or cyberterrorism.

The distinction is important. A state is entitled to protect national security. It is equally required to distinguish threats to national security from criticism of the state.

The Constitution of Pakistan guarantees freedom of speech and expression while allowing restrictions imposed by law for specified purposes including security, defence, public order, morality, contempt of court, and commission of or incitement to an offence. Article 19A separately protects access to information in matters of public importance, subject to regulation and reasonable restrictions.¹

Pakistan has also been a party to the International Covenant on Civil and Political Rights since 2010. Article 19 of the Covenant recognizes freedom to seek, receive, and impart information and permits restrictions only when provided by law and necessary for specified legitimate purposes.²

The legal question is therefore not whether expression may ever be restricted. Both domestic and international law recognize that it may. The crucial questions are how precisely offences are defined, whether prosecution addresses a real and legally cognizable harm, whether less restrictive responses were available, and whether the restriction bears a direct and proportionate relationship to the threat invoked.

¹ National Assembly of Pakistan, *The Constitution of the Islamic Republic of Pakistan, 1973*, arts. 19 and 19A, official consolidated text, https://na.gov.pk/uploads/documents/63ea176f52421_610.pdf.

² United Nations, *International Covenant on Civil and Political Rights*, December 16, 1966, 999 U.N.T.S. 171, art. 19; United Nations Treaty Collection, "Pakistan: Ratification," June 23, 2010.

Section One: The Statutory Architecture of Cyberterrorism and Online Speech under PECA

PECA contains both conventional computer offences and expression-related offences. Their interaction is especially important because section 10 does not create cyberterrorism in isolation. It links cyberterrorism to specified predicate offences and an additional terrorism-related intention. Understanding this structure is essential before evaluating claims of misuse.

1. Section 10: Cyberterrorism as a Compound Criminal Offence

Section 10 defines cyberterrorism through the commission or threatened commission of offences contained in sections 6, 7, 8 or 9, together with specified forms of intention.

The legislation refers to an intention to:

“coerce, intimidate, create a sense of fear, panic or insecurity”³

in government, the public, a section of the public, a community, or society.

The significance of this language lies in the structure of the offence. Fear or insecurity alone does not constitute section 10. The defendant must first commit or threaten one of the predicate offences under sections 6 to 9, after which the prosecution must establish the additional statutory intent. Sections 6 to 8 concern critical-infrastructure systems and data, while section 9 concerns glorification of terrorism-related offences or proscribed actors. A legally disciplined interpretation should therefore resist treating section 10 as a general prohibition against alarming, hostile, or politically uncomfortable online speech.

Section 10 additionally criminalizes qualifying conduct intended to:

“advance the objectives of organizations or individuals or groups proscribed under the law.”⁴

This limb serves an intelligible counterterrorism purpose where digital conduct intentionally facilitates or promotes the objectives of a legally proscribed entity. Its difficulty arises at the evidentiary stage. Reporting on a proscribed organization, discussing its grievances, criticizing state policy toward it, reproducing its statements for journalistic analysis, and intentionally advancing its objectives are conceptually different activities. Criminal liability should depend upon proof of the statutory intention rather than inference from mere subject matter, association of ideas, or controversial political commentary.

The maximum penalty under section 10 extends to fourteen years’ imprisonment and a substantial fine. The severity of the offence reinforces the need for narrow interpretation. Terrorism offences carry exceptional stigma and consequences; consequently, the evidentiary threshold should correspond to their seriousness. A prosecution that labels peaceful criticism “cyberterrorism” without proving the predicate offence and terrorist intention would not merely regulate expression—it would alter the legal character of expression by associating it with terrorism.

2. Section 9: “Glorification” and the Boundary Between Advocacy, Reporting and Terrorist Propaganda

Section 9 becomes especially important because it is the speech-related predicate most capable of connecting online expression to section 10.

³ Pakistan, *Prevention of Electronic Crimes Act, 2016*, Act XL of 2016, s. 10(a), as amended through the Prevention of Electronic Crimes (Amendment) Act, 2025 (Act II of 2025), Pakistan Code.

⁴ *Prevention of Electronic Crimes Act, 2016*, s. 10(c).

The statutory provision criminalizes dissemination undertaken:

“with the intent to glorify an offence relating to terrorism”⁵

or certain persons and activities associated with proscribed organizations.

The word “intent” provides an important limiting element. A responsible application should require proof that the speaker intended to glorify the terrorism-related offence or relevant proscribed activity. This should be distinguished from reporting, documentary work, legal analysis, academic research, criticism, quotation, or discussion of the causes of violence. The same words or images can perform radically different communicative functions depending upon context. A documentary reproducing propaganda to expose extremism cannot reasonably be treated as equivalent to propaganda designed to celebrate it.

The statutory explanation states that glorification includes:

“depiction of any form of praise or celebration in a desirable manner.”⁶

The definition narrows the concept to some extent by requiring praise or desirable portrayal, yet interpretive difficulties remain. Political discourse frequently involves disputed narratives of violence, resistance, state force, insurgency, and nationalism. When criminal law enters such debates, investigators and courts must distinguish intentional endorsement of terrorism from expression that is sympathetic to a political grievance but does not encourage terrorist violence. Failure to maintain this distinction can convert ideological disagreement into criminal liability.

Before PECA was enacted, United Nations special-procedure mandate holders expressed concern that broadly framed provisions could:

“criminalize a legitimate exercise of the right to freedom of expression”⁷

and generate censorship and self-censorship.

This pre-enactment concern is analytically important because it focused on statutory design rather than on any particular government or defendant. The risk identified was structural: broadly defined speech crimes permit enforcement authorities to decide which narratives qualify as glorification. The more politically sensitive the subject, the more important objective evidentiary criteria become. A sound legal standard should therefore require a demonstrable connection between the impugned expression and intentional advocacy, encouragement, celebration, or advancement of terrorism.

3. The State’s Legitimate Cybersecurity Interest and Its Human-Rights Position

A critical study should also account for the Government of Pakistan’s stated legal position.

In its second periodic report to the United Nations Human Rights Committee, Pakistan maintained:

“PECA is fully in line with the Constitution of Pakistan”⁸

and stated that the legislation fulfilled the country’s ICCPR obligations.

⁵ *Prevention of Electronic Crimes Act, 2016*, s. 9(1).

⁶ *Prevention of Electronic Crimes Act, 2016*, s. 9, Explanation.

⁷ Office of the United Nations High Commissioner for Human Rights, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, “Communication to Pakistan,” OL PAK 8/2016, July 8, 2016; and “Communication to Pakistan,” AL PAK 13/2015, December 14, 2015.

⁸ Government of Pakistan, *Second Periodic Report Submitted under Article 40 of the International Covenant on Civil and Political Rights*, CCPR/C/PAK/2 (December 7, 2022), para. 115.

This position is legally significant. It demonstrates that the state does not present PECA as a mechanism for suppressing political speech but as cybercrime legislation operating within constitutional safeguards. The Act addresses serious offences that governments are ordinarily entitled, and sometimes required, to prevent. Any human-rights analysis must therefore distinguish the legitimacy of the regulatory purpose from the legality of particular provisions or enforcement actions. A law may pursue legitimate objectives while still requiring narrower drafting or stronger safeguards in specific areas.

The same government report emphasized that constitutional writ jurisdiction permits individuals alleging violations of fundamental rights to approach superior courts.⁹

Judicial review is an important safeguard. Pakistan's superior courts have in fact scrutinized PECA measures and, in some instances, invalidated them. Yet post-enforcement judicial review does not completely answer concerns surrounding chilling effects. Arrest, investigation, device seizure, lengthy proceedings, legal expenses, and reputational association with terrorism may themselves impose serious burdens before a final constitutional judgment is obtained. Rights protection therefore requires both judicial remedies after abuse and legal safeguards capable of preventing disproportionate enforcement at the outset.

Section Two: Constitutional Freedom of Expression and the Limits of National-Security Restrictions

The constitutional analysis of PECA cannot be resolved by asserting either that expression is absolute or that national security overrides speech. Neither proposition accurately reflects Pakistani constitutional law. Article 19 protects expression while expressly permitting reasonable restrictions for enumerated purposes. The legal controversy therefore concerns reasonableness, statutory precision, evidentiary connection, and proportionality.

1. Article 19 of the Constitution: Rights and Reasonable Restrictions

Article 19 provides that:

“Every citizen shall have the right to freedom of speech and expression”¹⁰
subject to reasonable restrictions imposed by law for constitutionally specified purposes.

The presence of express exceptions means that national-security legislation is not inherently unconstitutional. Laws addressing terrorist incitement, threats, violent propaganda, or serious disruption of public order may fall within legitimate constitutional objectives. However, describing an offence as relating to “security” cannot itself resolve the constitutional inquiry. The restriction must still be imposed by law and must remain reasonable in scope and application.

The Islamabad High Court stated in 2022 that:

“suppression thereof is unconstitutional and contrary to the democratic values.”¹¹

The Court's observation was made in proceedings concerning the PECA Amendment Ordinance 2022 and criminal defamation, rather than section 10 cyberterrorism itself. Its broader constitutional relevance lies in the Court's recognition that expression and access to information reinforce democratic participation. The judgment demonstrates that cybercrime

⁹ Government of Pakistan, *Second Periodic Report*, para. 6.

¹⁰ *The Constitution of the Islamic Republic of Pakistan*, 1973, art. 19.

¹¹ *Pakistan Federal Union of Journalists through its Secretary General v. President of Pakistan through the Secretary & 4 others*, W.P. No. 666/2022 (Islamabad High Court, April 8, 2022), para. (b).

legislation remains subject to ordinary constitutional review even where the government invokes online harms. Technology does not create a separate constitutional category in which fundamental rights receive diminished protection.

The same order described freedom of expression as a right that:

“reinforces all other rights guaranteed under the Constitution.”¹²

This formulation places expression within the broader structure of constitutional accountability. Political speech enables citizens to expose misconduct, discuss security policy, criticize institutions, defend minority interests, and challenge official narratives. Restrictions capable of criminalizing such speech therefore affect more than Article 19 alone. They may influence access to information, political participation, legal advocacy, journalism, peaceful assembly, and the capacity of civil society to demand institutional accountability.

2. International Human-Rights Law: Necessity, Proportionality and Direct Connection to Harm

Article 19 of the ICCPR permits restrictions on expression for national security and public order, but the Human Rights Committee applies demanding conditions.

The Committee has stated that restrictions must satisfy:

“the strict tests of necessity and proportionality.”¹³

Necessity requires more than governmental preference or administrative convenience. The state must identify a legitimate protected interest and demonstrate why restricting the particular expression is required to protect it. In cyberterrorism cases, this means identifying the actual security threat posed by the impugned communication. A general assertion that criticism damages national morale or creates embarrassment for an institution should not automatically be equated with a threat to national security.

The Committee further requires:

“a direct and immediate connection between the expression and the threat.”¹⁴

This standard is particularly relevant to section 10 prosecutions involving social-media speech. A distant ideological resemblance between a post and the rhetoric of an unlawful organization is not necessarily equivalent to intentionally advancing that organization’s objectives. Similarly, expression concerning military operations, enforced disappearances, insurgency, ethnic grievances, or counterterrorism policy may be controversial without creating an immediate terrorist threat. The prosecution should therefore demonstrate a concrete connection between speech, criminal intent, and the protected security interest.

The principle of proportionality further requires selection of the least intrusive effective measure. If a harmful falsehood can be corrected, a defamatory allegation answered through civil law, or disputed political commentary challenged through public debate, imprisonment under terrorism-related legislation may require particularly strong justification.

3. United Nations Scrutiny of Pakistan’s Contemporary Freedom-of-Expression Framework

The Human Rights Committee’s 2024 concluding observations addressed Pakistan’s broader legal environment.

The Committee reported concern about:

¹² *Pakistan Federal Union of Journalists*, W.P. No. 666/2022, para. (a).

¹³ United Nations Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of Opinion and Expression*, CCPR/C/GC/34 (September 12, 2011), para. 22.

¹⁴ Human Rights Committee, *General Comment No. 34*, para. 35.

“arbitrary restrictions, in law and in practice, on freedom of expression online and offline.”¹⁵

This finding does not establish that every application of PECA is arbitrary. Rather, it records the Committee’s assessment of a broader pattern involving internet shutdowns, content restrictions, criminal laws, and reports concerning journalists and activists. For legal analysis, its importance lies in demonstrating that scrutiny of PECA cannot be isolated from the overall regulatory ecosystem. A speech offence that might appear tolerable in isolation can have a different practical effect when combined with surveillance, platform blocking, criminal prosecution, and broad counterterrorism powers.

The Committee specifically recommended that criminal and counterterrorism legislation:

“are not used to silence journalists, human rights defenders ... and dissenting voices.”¹⁶

This recommendation is carefully framed. It does not prohibit counterterrorism laws from applying to journalists or activists who genuinely commit criminal offences. Status as a journalist or dissident does not create immunity. The principle is instead conduct-based: peaceful expression should not be transformed into criminal terrorism because of the identity or political position of the speaker. Prosecutors should establish every statutory element independently of whether authorities consider the speaker hostile, embarrassing, oppositional, or “anti-state.”

Section Three: Vagueness, Overbreadth and the Chilling Effect of Criminal Speech Provisions

The human-rights concern surrounding PECA does not arise only from conviction. Investigation itself can influence behaviour. If statutory boundaries are difficult to predict, speakers may avoid lawful expression because they cannot determine whether criticism will later be interpreted as glorification, fear creation, fake information, reputational harm, or advancement of prohibited objectives.

1. Vagueness in Cyberterrorism and the Principle of Legality

Criminal offences should enable individuals to understand, with reasonable legal advice where necessary, what conduct exposes them to punishment.

The American Bar Association’s analysis of PECA identifies:

“Vagueness in definitions and terms of this Act”¹⁷

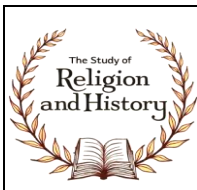
as a particular concern in relation to cyberterrorism.

The difficulty is amplified by the severity of section 10. Concepts such as intimidation, fear, insecurity, and advancement of objectives can acquire very broad meanings unless interpreted through the predicate-offence structure and clear proof of intent. Political criticism frequently seeks to pressure governments, expose abuses, mobilize public opinion, or create concern

¹⁵ United Nations Human Rights Committee, *Concluding Observations on the Second Periodic Report of Pakistan*, CCPR/C/PAK/CO/2 (December 2, 2024), paras. 48–49.

¹⁶ Human Rights Committee, *Concluding Observations on the Second Periodic Report of Pakistan*, para. 49(c).

¹⁷ Ali Changezi Sandhu, “Vagueness in Definition of Cyber Terrorism in Prevention of Electronic Crimes Act 2016,” American Bar Association, Criminal Justice Section, n.d., accessed September 20, 2026, https://www.americanbar.org/groups/criminal_justice/resources/committee-articles/cyber-terrorism-prevention-electronic-crimes-act-2016/.



about government conduct. Criminal law must distinguish democratic pressure from coercion in the terrorism sense.

The UN special-procedure communication concerning the draft law also referred to:

“overly broad provisions that lack sufficiently clear definitions.”¹⁸

The legality problem is not solved merely because a statute contains words. Criminal law requires adequate normative guidance. If officials can attach terrorism consequences to a very wide range of communications based largely on subjective perceptions of fear or anti-state sentiment, the citizen cannot predict the boundary between protected political advocacy and criminal conduct. Narrow judicial construction, prosecutorial guidelines, and explicit evidentiary requirements can reduce this risk without disabling prosecution of genuine cyberterrorism.

2. Section 20, Criminal Defamation and Judicial Findings of Abuse

Section 20 historically criminalized specified false online information that harms reputation or privacy. Its application became a major constitutional controversy.

In its April 2022 order, the Islamabad High Court referred to:

“widespread abuse of powers”¹⁹

by officials of the then FIA Cyber Crime Wing and directed an inquiry.

This language is unusually important because it comes from a constitutional court rather than an advocacy organization. The Court did not merely speculate about possible abuse; it expressly directed the Ministry of Interior to investigate conduct that the Court associated with grave violations of fundamental rights. This judicial finding supports the proposition that safeguards against misuse cannot rest solely on the text of offences. Institutional incentives, investigative practices, arrest decisions, and complaint procedures also determine whether a cybercrime regime protects or undermines rights.

The Court further declared unconstitutional the section 20 expression:

“or harms the reputation”²⁰

together with the relevant punishment, in the proceedings before it.

The decision illustrates the constitutional tension between reputation and criminal punishment. Reputation is a legitimate interest, but criminal prosecution and imprisonment produce consequences substantially more severe than correction, reply, damages, or other civil remedies. The Supreme Court subsequently granted leave to consider constitutional questions concerning section 20, including whether criminalizing defamation suppresses freedom of expression.²¹

The broader lesson for cyberterrorism law is proportionality. If ordinary reputational disputes become criminalized, the distinction between genuine cybersecurity enforcement and regulation of contentious speech becomes increasingly blurred.

¹⁸ Office of the United Nations High Commissioner for Human Rights, “Communication to Pakistan,” AL PAK 13/2015, December 14, 2015; see also OL PAK 8/2016, July 8, 2016.

¹⁹ *Pakistan Federal Union of Journalists*, W.P. No. 666/2022, para. (i).

²⁰ *Pakistan Federal Union of Journalists*, W.P. No. 666/2022, para. (f).

²¹ *Meera Shafi and others v. Federation of Pakistan through Secretary, Ministry of Law and Justice, Islamabad and others*, Civil Petition No. 1431/2022 (Supreme Court of Pakistan, June 8, 2022), order granting leave to appeal.

3. Section 26A after the 2025 Amendment: False Information and Public Disorder

The Prevention of Electronic Crimes (Amendment) Act 2025 inserted section 26A into PECA.

The provision applies where information is believed to be false or fake and is:

“likely to cause or create a sense of fear, panic or disorder or unrest”²²

in the general public or society.

The provision contains important limiting components: intentional dissemination, knowledge or reason to believe the information is false or fake, and likelihood of specified public consequences. Properly applied, these elements can differentiate deliberate harmful disinformation from error, satire, prediction, opinion, or good-faith reporting. The danger arises if “false”, “fake”, “panic”, or “unrest” are applied without objective evidentiary criteria. Political reporting often involves incomplete or contested information, and later correction should not retrospectively transform reasonable journalistic error into criminality.

Amnesty International warned during the amendment process that:

“vague and ambiguous framing”²³

could chill online expression.

This is an attributed assessment rather than a judicial holding. Supporters of the legislation may reasonably argue that deliberate disinformation can produce real harm, particularly during emergencies, communal tensions, financial instability, or security operations. The rights-based response is therefore not that false information can never be regulated. The stronger legal position is that criminal punishment should require demonstrable falsity, culpable mental state, a sufficiently serious risk of legally cognizable harm, and proportionality between the harm and the sanction.

Section Four: Enforcement Patterns, Dissent and the Use of Terrorism-Related Charges

The central empirical question is whether PECA’s serious offences have remained confined to conventional cyberattacks and terrorist activity or have also been applied to contentious political expression. Documented cases show that section 10 and associated provisions have increasingly entered disputes involving social-media criticism, activism, and “anti-state” allegations.

1. The Imaan Mazari-Hazir and Hadi Ali Chattha Case as a Contemporary Test Case

A recent prosecution provides a particularly significant example because the charges included sections 9, 10 and 26A.

Dawn reported that the prosecution accused the defendants of:

“propagating narratives that align with hostile terrorist groups and proscribed organisations.”²⁴

This formulation demonstrates the prosecution’s theory: the case was not formally presented as punishment for criticism alone but as dissemination allegedly connected to hostile or proscribed narratives. The legal question, therefore, is whether the prosecution proved the elements of glorification, cyberterrorism, and false information beyond the content’s political

²² Pakistan, *Prevention of Electronic Crimes (Amendment) Act, 2025*, Act II of 2025, s. 5, *The Gazette of Pakistan*, Extraordinary, January 29, 2025.

²³ Amnesty International, “Pakistan: Authorities Pass Bill with Sweeping Controls on Social Media,” January 24, 2025, <https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/>.

²⁴ Malik Asad, “IHC Admits Imaan, Hadi’s Pleas against Sentences,” *Dawn*, July 26, 2026.

character. In cases of this type, courts must distinguish between intentional advancement of terrorist objectives and expression that criticizes state security policy or expresses solidarity with populations affected by conflict.

On 24 January 2026, a sessions court convicted the two lawyers under PECA sections 9, 10 and 26A and imposed sentences reported as totaling seventeen years.²⁵

The convictions generated substantial criticism from human-rights organizations and legal commentators, but a critical academic treatment must distinguish advocacy assessments from procedural facts. Conviction by a trial court constituted a judicial determination, while appellate proceedings meant the legal findings were not necessarily final. The case therefore illustrates precisely why politically sensitive cyberterrorism prosecutions require careful appellate review: the same expression may be characterized by the prosecution as support for proscribed narratives and by the defence as protected criticism or human-rights advocacy.

On 17 September 2026, the Supreme Court suspended the sentences and granted bail pending further proceedings.²⁶

A suspension of sentence is not the same as final acquittal and should not be described as such. It nevertheless materially changes the procedural position and demonstrates that the convictions remain subject to appellate scrutiny. The case should therefore be analysed as an ongoing legal controversy rather than used to prove categorically either state repression or lawful counterterrorism enforcement. Its value for research lies in the questions it raises about evidentiary thresholds, characterization of political speech, proportionality of punishment, and the relationship between sections 9 and 10.

2. Human-Rights Organizations' Claims of "Weaponization" and the Need for Evidentiary Caution

Rights organizations have repeatedly criticized PECA enforcement.

Amnesty International stated in 2022 that PECA had been used:

"to silence freedom of expression"²⁷

under various cybercrime rationales.

This allegation should be treated as a documented civil-society assessment, not automatically as a finding of fact in every individual prosecution. Human-rights organizations evaluate patterns through a rights-based methodology, while courts determine criminal responsibility according to admissible evidence and applicable law. Nevertheless, repeated allegations from international organizations become legally relevant when they align with domestic judicial findings concerning abuse, especially the Islamabad High Court's 2022 directions concerning misuse of investigative power.

In January 2026, Amnesty described cyberterrorism charges against Mazari-Hazir and Chattha as:

"politically motivated"²⁸

²⁵ Malik Asad, "Day after Dramatic Arrest, Imaan and Hadi Handed Jail Sentence in Controversial Social Media Posts Case," *Dawn*, January 24, 2026.

²⁶ Reuters, "Pakistan Police Re-Arrest Prominent Rights Lawyer after Top Court Granted Bail," September 17, 2026; Nasir Iqbal, "SC Suspends Imaan, Hadi's Sentences in Controversial Social Media Posts Case, Orders Their Release," *Dawn*, September 17, 2026.

²⁷ Amnesty International and Human Rights Watch, "Pakistan: Repeal Amendment to Draconian Cyber Law," February 28, 2022, <https://www.amnesty.org/en/latest/news/2022/02/pakistan-repeal-draconian-cyber-crime-law/>.

and asserted that they criminalized peaceful expression.

A balanced analysis requires simultaneous recognition of the prosecution's contrary position: authorities alleged that the posts advanced narratives associated with hostile or proscribed actors. The decisive legal inquiry is therefore evidentiary rather than rhetorical. Courts should ask what specific posts constituted section 9 glorification, which statutory purpose under section 10 was proven, how intent was established, what evidence connected the expression to prohibited objectives, and whether the disputed material could reasonably fall within political advocacy or reporting.

The existence of polarized characterizations is itself a reason for greater doctrinal precision. When one side calls expression "terrorism" and the other calls the prosecution "political persecution", criminal law should provide objective elements capable of resolving the dispute without relying upon institutional labels.

3. The Chilling Effect on Journalism, Advocacy and Minority Political Expression

The chilling effect arises when individuals refrain from lawful speech because the cost or uncertainty of legal exposure becomes too high.

The Human Rights Committee in 2024 specifically referred to:

"the chilling effect"²⁹

of counterterrorism and other criminal legislation on journalists, activists, human-rights defenders, and minority communities.

A chilling effect is difficult to measure because it concerns speech that never occurs. Its legal relevance nevertheless rests on rational behaviour. Where peaceful online criticism can potentially trigger investigation under offences carrying multi-year imprisonment, individuals may self-censor even when eventual conviction is unlikely. The burden therefore includes not only sentences but the risk of arrest, bail proceedings, device examination, legal expense, stigma, and prolonged uncertainty.

Amnesty's 2025 investigation reported that surveillance and censorship mechanisms were:

"used to silence dissent"³⁰

according to the organization's findings.

Again, this is Amnesty's attributed conclusion. Its significance lies in the interaction between criminal law and technical capacity. Broad offences become more consequential when the state possesses expanding capabilities to identify speakers, monitor communications, restrict platforms, or analyze online behaviour. A rights-protective cybercrime framework must therefore regulate investigative technologies as carefully as substantive offences.

Section Five: Privacy, Surveillance and Procedural Human Rights under PECA

Freedom of expression is not the only right implicated by cybercrime enforcement. Digital investigations involve traffic data, devices, accounts, communications, metadata, and

²⁸ Amnesty International, "Pakistan: Authorities Must End Judicial Harassment of Lawyers Imaan Mazari and Hadi Chatta," January 16, 2026, <https://www.amnesty.org/en/latest/news/2026/01/pakistan-authorities-must-end-judicial-harassment-of-lawyers-imaan-mazari-and-hadi-chatta/>.

²⁹ Human Rights Committee, *Concluding Observations on the Second Periodic Report of Pakistan*, para. 48.

³⁰ Amnesty International, *Shadows of Control: Censorship and Mass Surveillance in Pakistan*, Index No. ASA 33/0206/2025 (September 9, 2025).

potentially extensive surveillance. The exercise of such powers can affect privacy, fair trial, legal professional privilege, journalistic confidentiality, and association.

1. Privacy and Digital Surveillance

The UN Human Rights Committee has previously recommended that Pakistan review PECA-related surveillance and establish:

“independent oversight mechanisms”³¹

including judicial review of surveillance activities.

The importance of independent authorization is particularly strong in politically sensitive investigations. If the same institutional structure identifies controversial speech as threatening, authorizes intrusive collection, controls the evidence, and initiates prosecution without sufficiently independent scrutiny, errors or political bias can become difficult to detect. Prior judicial authorization for highly intrusive measures can provide an external assessment of necessity and scope.

Pakistan’s government responded that section 39 provided:

“an independent oversight mechanism on the implementation of the Act.”³²

This is an important counterpoint. The legal disagreement therefore concerns not simply whether safeguards exist on paper, but whether their institutional design, independence, transparency, and practical operation are sufficient. An evidence-based evaluation should examine authorization procedures, reporting obligations, parliamentary oversight, complaint mechanisms, and the availability of effective judicial review rather than presuming either complete absence or perfect adequacy of safeguards.

2. Fair Trial and the Classification of Digital Evidence

Digital speech prosecutions require rigorous evidentiary safeguards. Screenshots, reposts, edited clips, account attribution, metadata, device extraction, and platform records can raise authenticity and context questions.

The ICCPR requires restrictions on expression to be justified in:

“a specific and individualized fashion”³³

when national-security grounds are invoked.

In evidentiary terms, this means prosecutors should identify the actual communication, prove authorship or legally relevant dissemination, establish context, demonstrate the applicable mental element, and connect the content with the precise statutory harm. Reliance upon generalized descriptions such as “anti-state narrative”, “hostile content”, or “negative propaganda” cannot substitute for proof of the statutory elements unless those descriptions are tied to specific evidence.

This requirement becomes especially important for reposts and quotations. Republishing material can serve endorsement, criticism, reporting, satire, archival documentation, or legal commentary. Digital evidence should therefore be interpreted in communicative context rather than mechanically treating transmission as agreement.

3. Criminal Process as Punishment Before Final Adjudication

Even where defendants are ultimately acquitted, the criminal process can impose substantial costs.

The Islamabad High Court’s 2022 PECA order referred to:

³¹ United Nations Human Rights Committee, *Concluding Observations on the Initial Report of Pakistan*, CCPR/C/PAK/CO/1 (August 23, 2017), para. 36.

³² Government of Pakistan, *Second Periodic Report*, para. 115.

³³ Human Rights Committee, *General Comment No. 34*, para. 35.

“grave violations of fundamental rights of the citizens”³⁴ in connection with conduct it directed the Ministry of Interior to investigate. This reinforces the distinction between substantive law and enforcement procedure. A narrowly drafted offence can still be abused through unnecessary arrest or intrusive investigation, while a broad offence can sometimes be administered cautiously. Human-rights protection therefore requires procedural rules governing complaint registration, arrest, search, data seizure, custody, bail, prosecutorial review, and timely trial. For speech offences, arrest should ordinarily be justified by concrete procedural necessity rather than the mere seriousness of the statutory label. Otherwise, attaching the term “terrorism” to expression can itself produce punitive consequences before a court has determined whether terrorism occurred.

Section Six: PECA 2025 and the Expansion of the Online Regulatory Framework

Although this study focuses on PECA 2016, the legal framework cannot be understood without its 2025 amendment. The amendment did not repeal the earlier speech-related offences; it added new regulatory institutions and a new offence concerning false or fake information.

1. Section 26A and the Criminalization of Harmful False Information

Section 26A imposes liability on specified intentional dissemination of information known or believed to be false or fake where it is likely to produce fear, panic, disorder, or unrest.³⁵

The phrase:

“knows or has reason to believe to be false or fake”³⁶

is crucial because it introduces a culpability requirement.

A rights-consistent interpretation should preserve that requirement rigorously. News reporting and public debate frequently involve developing events in which facts are uncertain. A journalist or citizen who makes a reasonable mistake should not automatically be equated with a person deliberately manufacturing a falsehood. The prosecution should establish why the defendant knew, or had legally sufficient reason to believe, the information was false at the time of dissemination.

Amnesty argued that the amendment would:

“further tighten the government’s grip”³⁷

on Pakistan’s digital environment.

This is an advocacy assessment and should be identified as such. Supporters of the amendment can point to genuine harms caused by organized disinformation, panic-inducing hoaxes, manipulated media, and deliberately fabricated security claims. The strongest legal reform position therefore lies between unconditional criminalization and complete deregulation: intentional harmful falsehoods may be sanctionable, but imprisonment should remain exceptional and the elements of falsity, culpability, likelihood of harm, and causation should be interpreted narrowly.

2. Cumulative Charging and the Risk of Offence Inflation

An important contemporary concern is cumulative charging under sections 9, 10, and 26A.

³⁴ *Pakistan Federal Union of Journalists*, W.P. No. 666/2022, para. (i).

³⁵ *Prevention of Electronic Crimes (Amendment) Act, 2025*, s. 5 (inserting PECA s. 26A).

³⁶ *Prevention of Electronic Crimes (Amendment) Act, 2025*, s. 5.

³⁷ Amnesty International, “Pakistan: Authorities Pass Bill with Sweeping Controls on Social Media.”

The Mazari-Hazir and Chattha prosecution resulted in convictions under:

“sections 9 ... 10 ... and 26-A”³⁸

according to contemporary reporting.

Cumulative charging may be legally justified where a single course of conduct genuinely satisfies distinct offences protecting separate legal interests. The concern arises where substantially the same expressive act is characterized simultaneously as glorification, cyberterrorism, and false information without sufficiently independent proof for each offence. This can magnify potential punishment and increase pressure on defendants while blurring the boundaries among offences.

Courts should therefore examine whether each charge contains a distinct factual and mental element, whether section 10 properly rests upon a proven predicate offence, and whether punishment reflects the actual harm rather than the number of labels attached to the same communication.

3. Regulatory Expansion and Institutional Independence

The 2025 amendment established a new Social Media Protection and Regulatory Authority within the PECA framework and restructured investigative arrangements.³⁹

The broader constitutional question is not whether social-media regulation is permissible. Platforms influence public safety, fraud, harassment, extremist propaganda, child protection, and other legitimate interests. The question is whether regulatory institutions possess sufficient independence, transparent procedures, appeal mechanisms, and clearly defined statutory powers.

Amnesty criticized the amendment for expanding content-control powers on what it considered:

“vague criteria.”⁴⁰

This criticism should be tested institutionally. Effective digital regulation requires published standards for removal decisions, written reasons, notice to affected users where appropriate, independent appeal, periodic transparency reports, and judicial review. Such safeguards protect both speakers and regulators: they allow legitimate harmful-content enforcement to be distinguished from politically selective censorship.

Section Seven: Distinguishing Cyberterrorism from Protected Dissent

The central doctrinal problem can be reduced to a classification question. When does online political expression cross the line into cyberterrorism?

A sustainable legal test should begin from the statutory elements rather than from the political tone of the expression.

1. Criticism of State Institutions Is Not Automatically a Security Threat

Democratic institutions can be criticized severely without losing their legal protection against genuine threats.

The Human Rights Committee recommends that Pakistan ensure counterterrorism legislation is not applied to:

“repress human rights defenders ... journalists, dissidents and activists.”⁴¹

³⁸ Asad, “Day after Dramatic Arrest, Imaan and Hadi Handed Jail Sentence.”

³⁹ *Prevention of Electronic Crimes (Amendment) Act, 2025*, ss. 3 and 6–7 (establishing the Social Media Protection and Regulatory Authority and restructuring investigation through the National Cyber Crime Investigation Agency).

⁴⁰ Amnesty International, “Pakistan: Authorities Pass Bill with Sweeping Controls on Social Media.”

The implication is not that such persons can never commit terrorist offences. The important rule is viewpoint neutrality: criminality must derive from conduct and intent, not from the defendant's political identity or criticism of state institutions.

Statements alleging abuses by security agencies, questioning military operations, supporting constitutional rights of ethnic communities, or demanding investigation of enforced disappearances can be controversial and disputed. Their content should nevertheless be analyzed through the elements of the offence. Criticism becomes terrorism only when the law's terrorism-related requirements are actually satisfied.

2. A Proposed Direct-Harm Test for Section 10 Speech Cases

A rights-sensitive section 10 analysis should require prosecutors to establish four matters.

First, the impugned conduct must satisfy one of sections 6, 7, 8 or 9.

Second, the required section 10 intent must be demonstrated through evidence rather than inferred merely from political hostility.

Third, where expression is relied upon, there should be a sufficiently direct connection between the communication and the terrorist or security harm alleged.

Fourth, the prosecution and penalty should satisfy proportionality.

This approach reflects the Human Rights Committee's requirement that restrictions be:

“directly related to the specific need”⁴²

upon which they are based.

A direct-harm approach would preserve the state's ability to prosecute genuine terrorist propaganda while reducing the possibility that generalized dissent becomes criminalized through expansive interpretation. It would also make judicial reasoning more transparent: a court would identify the predicate offence, the terrorist purpose, the connection to harm, and the justification for criminal punishment separately.

3. The Importance of Public-Interest Expression

National-security discourse often concerns matters of substantial public importance: conflict, terrorism, policing, military operations, foreign policy, missing persons, ethnic grievances, border security, and public expenditure.

The Constitution protects a separate right to access information in:

“all matters of public importance”⁴³

under Article 19A.

This provision strengthens the argument that cyberterrorism offences should not be interpreted in a manner that automatically criminalizes investigation or debate about security institutions. A public-interest defence or explicit statutory protection for good-faith journalism, academic research, legal representation, documentation of human-rights allegations, and reporting on proscribed organizations could reduce uncertainty while preserving liability for deliberate terrorist advocacy.

Public-interest protections are especially important for investigative reporting. Journalists may need to quote militant statements in order to expose them, lawyers may reproduce prohibited material as evidence, and researchers may archive extremist propaganda for analysis. Context should determine whether dissemination constitutes glorification.

⁴¹ Human Rights Committee, *Concluding Observations on the Second Periodic Report of Pakistan*, para. 49(c).

⁴² Human Rights Committee, *General Comment No. 34*, para. 22.

⁴³ *The Constitution of the Islamic Republic of Pakistan, 1973*, art. 19A.

Findings of the Study

The study produces the following principal findings.

First, PECA addresses legitimate and serious forms of cybercrime, and section 10 cannot accurately be described as a general speech offence in textual terms. It depends upon predicate offences under sections 6 to 9 plus an additional statutory intent.

Second, section 9 is the principal expressive gateway through which online speech may become connected to section 10 cyberterrorism. Its interpretation is therefore decisive for freedom of expression.

Third, broad concepts such as glorification, fear, insecurity, advancement of objectives, fake information, panic, and unrest require careful judicial construction because politically contentious expression can superficially resemble some of these concepts without satisfying terrorism-related criminal intent.

Fourth, Pakistan's Constitution permits reasonable restrictions on expression for national security and public order. The legal objection is therefore not to security regulation itself but to restrictions that are insufficiently precise, unnecessary, disproportionate, or disconnected from identifiable harm.

Fifth, the Government of Pakistan has formally maintained before the United Nations that PECA complies with the Constitution and the ICCPR. This position must form part of any balanced assessment.

Sixth, domestic judicial material nevertheless provides evidence that misuse concerns are not purely theoretical. The Islamabad High Court in 2022 referred expressly to widespread abuse of power by the FIA Cyber Crime Wing and grave violations of fundamental rights.

Seventh, international human-rights institutions have repeatedly expressed concern about the combined effect of cybercrime, defamation, counterterrorism, censorship, and surveillance measures on journalists, activists, minorities, and dissenting voices.

Eighth, the 2025 introduction of section 26A creates an additional speech offence that can overlap factually with sections 9 and 10, increasing the importance of avoiding duplicative or inflated charging.

Ninth, recent cyberterrorism prosecutions involving social-media expression demonstrate the unresolved boundary between alleged support for prohibited narratives and constitutionally protected criticism. Appellate review remains central to clarifying that boundary.

Tenth, effective protection of freedom of expression requires safeguards at the investigative stage, not merely eventual acquittal or constitutional litigation.

Eleventh, surveillance capacity and criminal speech offences should be analyzed together because intrusive investigative powers can amplify the chilling effect of broadly worded offences.

Twelfth, a direct and demonstrable connection between expression, criminal intent, and the security harm invoked should become a central judicial requirement in cyberterrorism cases.

Recommendations

1. Section 10 should be interpreted strictly as a compound offence requiring proof of both a predicate offence and the specified terrorism-related intent.
2. Courts should require prosecution evidence identifying the precise communication alleged to satisfy section 9 before section 10 liability is considered.
3. "Glorification" should be distinguished explicitly from reporting, quotation, criticism, academic study, legal representation, and documentary use.
4. Parliament should consider a clear public-interest defence for journalism, research, whistleblowing, legal advocacy, and documentation undertaken without terrorist intent.

5. Political criticism of state institutions should not by itself constitute evidence of cyberterrorism.
6. Prosecutors should establish a direct connection between impugned expression and a concrete security threat.
7. Section 26A should be applied only where falsity and the required mental element are demonstrated through reliable evidence.
8. Good-faith error, opinion, satire, prediction, and reasonable journalistic reporting should be expressly distinguished from deliberate disinformation.
9. Cumulative charges under sections 9, 10 and 26A should require separate proof of the constituent elements of each offence.
10. Arrest in expression-related PECA cases should require individualized reasons demonstrating why less restrictive procedural measures are inadequate.
11. Intrusive digital searches and surveillance should be subject to effective independent judicial authorization.
12. Investigators should preserve complete digital context rather than relying on isolated screenshots or excerpts.
13. Reposting should not automatically be treated as endorsement without proof of communicative intent.
14. Defendants should receive sufficient access to digital evidence to challenge authenticity, attribution, context, and forensic methodology.
15. Regulatory and investigative institutions exercising PECA powers should publish periodic transparency reports.
16. Content-removal decisions should include written reasons and meaningful rights of appeal.
17. Independent parliamentary or multi-stakeholder oversight should review patterns of PECA enforcement involving journalists, activists, and political expression.
18. Investigating officers, prosecutors, and judges should receive specialized training on Article 19 of the Constitution and Article 19 of the ICCPR.
19. Counterterrorism terminology should be reserved for conduct genuinely satisfying terrorism-related statutory elements rather than used as a general description of anti-government or critical expression.
20. Parliament should periodically review PECA's speech offences using publicly available prosecution, conviction, acquittal, and appeal data to determine whether enforcement remains proportionate to genuine cybercrime risks.

Conclusion

Pakistan has a legitimate and substantial interest in preventing cybercrime and terrorism. Critical infrastructure can be attacked digitally. Terrorist organizations can recruit, finance, propagandize, and coordinate through online platforms. Deliberate digital manipulation can create panic, communal violence, or serious public harm. No credible human-rights framework requires the state to remain passive in the face of these threats.

The difficult legal issue is classification.

Cyberterrorism legislation becomes constitutionally dangerous when the category of terrorism loses its connection to terrorist conduct and begins to absorb ordinary criticism, disputed political narratives, journalism, advocacy, or peaceful dissent.

PECA's textual structure provides one important safeguard: section 10 is linked to predicate offences rather than standing as an unlimited prohibition on unsettling speech. But textual

safeguards are only effective when investigators, prosecutors, and courts apply them rigorously.

Section 9 must therefore remain focused on intentional glorification rather than controversial discussion.

Section 10 must require proof of the specified terrorist intent.

Section 26A must distinguish knowing harmful falsehoods from mistakes, opinions, and developing news.

Investigative powers must remain proportionate and independently supervised.

Recent judicial and international material demonstrates that the concern about misuse is neither purely hypothetical nor capable of being reduced to a simple partisan narrative. Pakistan's government has defended PECA as constitutionally compliant and necessary for legitimate cybercrime control. The Islamabad High Court has simultaneously documented serious concerns about abuse of investigative powers. The United Nations Human Rights Committee has repeatedly warned against using criminal and counterterrorism legislation to silence dissenting voices. Contemporary prosecutions continue to test the boundary between national-security enforcement and protected political expression.

A mature constitutional approach should not weaken genuine counterterrorism law.

It should strengthen it by preserving the distinction between terrorism and dissent.

When peaceful criticism is treated as terrorism, the category of terrorism itself becomes legally diluted. When genuine terrorist conduct is precisely defined and prosecuted on strong evidence, both national security and civil liberties are better protected.

The proper objective of reform is therefore not unrestricted speech and not unrestricted state power.

It is a cybercrime regime in which the more serious the criminal label, the more precise the law, the stronger the evidence, the clearer the harm, and the more rigorous the judicial scrutiny must become.

Bibliography

Amnesty International. *Shadows of Control: Censorship and Mass Surveillance in Pakistan*.

Index No. ASA 33/0206/2025. September 9, 2025.

Amnesty International. "Pakistan: Authorities Must End Judicial Harassment of Lawyers

Imaan Mazari and Hadi Chatta." January 16, 2026.

Amnesty International. "Pakistan: Authorities Pass Bill with Sweeping Controls on Social

Media." January 24, 2025.

Amnesty International and Human Rights Watch. "Pakistan: Repeal Amendment to

Draconian Cyber Law." February 28, 2022.

Asad, Malik. "Day after Dramatic Arrest, Imaan and Hadi Handed Jail Sentence in

Controversial Social Media Posts Case." *Dawn*. January 24, 2026.

Asad, Malik. "IHC Admits Imaan, Hadi's Pleas against Sentences." *Dawn*. July 26, 2026.

Government of Pakistan. *Second Periodic Report Submitted under Article 40 of the International Covenant on Civil and Political Rights*. CCPR/C/PAK/2. December 7, 2022.

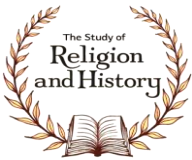
Human Rights Committee. *Concluding Observations on the Initial Report of Pakistan*.

CCPR/C/PAK/CO/1. August 23, 2017.

Human Rights Committee. *Concluding Observations on the Second Periodic Report of*

Pakistan. CCPR/C/PAK/CO/2. December 2, 2024.

Human Rights Committee. *General Comment No. 34: Article 19: Freedoms of Opinion and Expression*. CCPR/C/GC/34. September 12, 2011.

 THE STUDY OF RELIGION AND HISTORY Vol.4, No.1, 2026	ISSN P: 3006-3329 ISSN E: 3006-3337
---	--

- Iqbal, Nasir. "SC Suspends Imaan, Hadi's Sentences in Controversial Social Media Posts Case, Orders Their Release." *Dawn*. September 17, 2026.
- National Assembly of Pakistan. *The Constitution of the Islamic Republic of Pakistan, 1973*. Official consolidated text.
- Office of the United Nations High Commissioner for Human Rights. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. "Communication to Pakistan." AL PAK 13/2015. December 14, 2015.
- Office of the United Nations High Commissioner for Human Rights. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. "Communication to Pakistan." OL PAK 8/2016. July 8, 2016.
- Pakistan. *Prevention of Electronic Crimes Act, 2016*. Act XL of 2016, as amended.
- Pakistan. *Prevention of Electronic Crimes (Amendment) Act, 2025*. Act II of 2025. *The Gazette of Pakistan, Extraordinary*, January 29, 2025.
- Pakistan Federal Union of Journalists through its Secretary General v. President of Pakistan through the Secretary & 4 others*. W.P. No. 666/2022. Islamabad High Court. Order dated April 8, 2022.
- Reuters. "Pakistan Police Re-Arrest Prominent Rights Lawyer after Top Court Granted Bail." September 17, 2026.
- Sandhu, Ali Changezi. "Vagueness in Definition of Cyber Terrorism in Prevention of Electronic Crimes Act 2016." American Bar Association, Criminal Justice Section. n.d. Accessed September 20, 2026.
- Meera Shafi and others v. Federation of Pakistan through Secretary, Ministry of Law and Justice, Islamabad and others*. Civil Petition No. 1431/2022. Supreme Court of Pakistan. Order dated June 8, 2022.
- United Nations. *International Covenant on Civil and Political Rights*. December 16, 1966. 999 U.N.T.S. 171.