INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 4, Issue 4, 2026

DIGITAL RADICALISATION IN PAKISTAN: REASSESSING THE CRIMINAL JUSTICE RESPONSE UNDER ANTI-TERRORISM AND CYBERCRIME LAW

Mr. Ayaz Khan[*1], Professor Dr. Muhammad Zubair Khan[2], Muhammad Kashif Irshad[3]

[*1]*Ph.D (Law) Research Scholar, Department of Law, Abdul Wali Khan University Mardan , Khyber Pakhtunkhwa, Pakistan*
[2]*Chairman/Supervisor, Department of Law, Abdul Wali Khan University Mardan , Khyber Pakhtunkhwa, Pakistan*
[3]*Additional Director General, Khyber Pakhtunkhwa Centre of Excellence on Countering Violent Extremism, Pakistan*

[*1]ayazkhan.law@awkum.edu.pk, [2]mzubair@awkum.edu.pk, [3]kashifkhankhail@hotmail.com

Corresponding Author: *
Mr. Ayaz Khan
DOI: https://doi.org/10.5281/zenodo.19437132

Received	Accepted	Published
11 February 2026	21 March 2026	06 April 2026

ABSTRACT

Digital radicalisation has transformed the relationship between extremist mobilisation, public communication, and criminal law. In Pakistan, this transformation is especially significant because longstanding patterns of terrorism, sectarian conflict, and weak institutional coordination now intersect with rapidly expanding digital connectivity, social media use, and encrypted communication. This article examines whether Pakistan's current legal and criminal justice framework can respond coherently and lawfully to digitally mediated radicalisation. The paper adopts a qualitative doctrinal and policy-analysis methodology grounded in the Constitution of Pakistan, the Anti-Terrorism Act 1997, the Prevention of Electronic Crimes Act 2016 and its 2025 amendment, the Qanun-e-Shahadat Order 1984, public policy documents issued by the National Counter Terrorism Authority, and relevant contemporary scholarship on online extremism, cyber regulation, preventive justice, and procedural fairness. The article argues that Pakistan's present framework remains fragmented across anti-terrorism law, cybercrime law, regulatory blocking powers, investigative practice, and evidentiary rules. The main weaknesses are conceptual ambiguity in defining punishable online extremism, overbreadth in some speech-related offences, weak procedural safeguards, persistent digital-evidence challenges, and inadequate coordination among the Federal Investigation Agency, provincial Counter Terrorism Departments, prosecutors, courts, and policy institutions. The study further contends that an effective response to digital radicalisation cannot rely solely on punitive logic. A sustainable framework must combine clear legal thresholds, judicially reviewable platform-intervention powers, specialised evidentiary standards, inter-agency coordination, and preventive measures that remain compatible with constitutional rights and the rule of law. The paper concludes by proposing a structured reform agenda for Pakistan centred on legality, proportionality, evidential reliability, institutional specialisation, and rehabilitation-oriented prevention.

Keywords: *digital radicalisation; Pakistan; terrorism law; PECA; Anti-Terrorism Act; online extremism; criminal justice; digital evidence*

1. Introduction

The digitalisation of public life has reshaped how political ideas, identities, grievances, and solidarities are produced and circulated. Social media platforms, encrypted messaging applications, video-sharing sites, algorithmically curated feeds, and online forums no longer operate merely as neutral channels of communication. They structure visibility, amplify affective content, reward engagement, and enable rapid cross-border diffusion of ideological narratives. Extremist actors have adapted quickly to this environment. Contemporary radicalisation may now occur through dispersed, iterative, and technologically mediated pathways rather than through only face-to-face recruitment, territorial control, or membership in formal organisations.

Pakistan presents a particularly important site for examining this transformation. The country has experienced prolonged exposure to terrorism, sectarian conflict, and militant mobilisation, while simultaneously undergoing rapid growth in mobile connectivity and platform-based communication. Publicly available reporting indicates that Pakistan remains among the countries most affected by terrorism, while its online population and social media user base have expanded dramatically over the last decade. In this setting, digital platforms can be used to circulate propaganda, glorify violence, spread sectarian hatred, recruit sympathisers, intimidate opponents, and facilitate movement between online grievance and offline mobilisation.

Yet digital radicalisation does not map neatly onto conventional legal categories. The law must distinguish between protected belief, offensive opinion, extremist advocacy, incitement to violence, unlawful support, digital facilitation, and conduct sufficiently proximate to terrorism to justify penal intervention. This challenge is not merely semantic. It goes to the heart of legality, due process, constitutionalism, and the legitimacy of state power. If intervention is too narrow or too late, dangerous pathways may harden into operational violence. If intervention is too broad or too early, the state risks criminalising lawful expression, chilling dissent, and weakening public trust in criminal justice institutions.

This article argues that Pakistan's current response remains conceptually and institutionally fragmented. Relevant norms are spread across the Anti-Terrorism Act 1997 (ATA), the Prevention of Electronic Crimes Act 2016 (PECA), the 2025 PECA amendment, ordinary criminal law, evidentiary rules, platform-control practices, and policy instruments such as the National Prevention of Violent Extremism framework. These instruments touch aspects of online extremism, but they do not yet form a coherent, rights-compatible criminal justice model tailored to digital radicalisation.

The purpose of this paper is therefore twofold: first, to analyse the principal legal and criminal justice issues raised by digital radicalisation in Pakistan; and second, to develop a normative reform framework that aligns prevention, investigation, adjudication, and rights protection.

2. Review of Literature

The contemporary literature on radicalisation has moved away from linear and deterministic accounts. Earlier models often implied that individuals progress through fixed stages from grievance to ideology and then to violence. More recent scholarship is more cautious. It treats radicalisation as a contingent process shaped by social context, peer reinforcement, political grievance, identity narratives, media ecosystems, and opportunity structures. Within this broader shift, digital radicalisation is understood less as a separate phenomenon than as a technologically mediated environment that can accelerate exposure, repetition, social validation, and perceived belonging.

Research on online extremism identifies several recurring mechanisms. First, digital platforms lower the cost of ideological dissemination and audience targeting. Second, recommendation systems and engagement-based metrics may intensify exposure to emotionally charged or polarising content. Third, closed and encrypted channels permit stronger forms of in-group bonding, secrecy, and operational coordination. Fourth, digital content can create cumulative symbolic effects even where it falls short of explicit incitement. Memes, short videos, coded rhetoric, and repeated narratives of humiliation or

victimhood may normalise exclusionary worldviews without overtly calling for immediate violence.

The legal literature responds to these dynamics through three major debates. The first concerns definitional precision: what counts as extremist speech, glorification, encouragement, or facilitation, and at what point does online conduct become criminal rather than objectionable? The second concerns prevention: whether legal systems should intervene before tangible violence occurs, and how far preventive logic can extend without collapsing into punishment for beliefs. The third concerns procedural justice and legitimacy: whether expansive state powers used in the name of security generate distrust, discriminatory enforcement, or a chilling effect that ultimately undermines long-term compliance and cooperation.

Comparative scholarship is particularly instructive on the distinction between content moderation and criminal justice. Platform governance tools such as takedown orders, algorithmic demotion, account suspension, and transparency obligations may play a preventive role, but they are not substitutes for clear criminal law standards. European debates under the Digital Services Act, United Kingdom debates on online safety regulation, and Australian developments in e-safety governance all demonstrate that the architecture of response must combine regulatory duties with due process, oversight, and principled limits on coercive state action.

The Pakistani literature is expanding but remains uneven. Available studies document the role of social media, encrypted spaces, and online hate ecosystems in the spread of sectarianism and extremist messaging. They also emphasise Pakistan's youthful demography, digital-literacy deficits, uneven internet governance, and the persistence of offline grievances that can be digitally amplified. However, much of the existing work is either security descriptive, platform oriented, or policy general. There remains comparatively limited integrated analysis of how anti-terrorism law, cybercrime law, evidentiary doctrine, and criminal procedure interact when applied to digital radicalisation. That doctrinal gap is where this article makes its central contribution.

Theoretical perspectives help organise the inquiry. Social learning theory remains valuable because online environments multiply opportunities for observation, imitation, reinforcement, and status signalling. Preventive justice theory is relevant because digital threats often emerge before a conventional completed offence. Procedural justice theory is equally important because the legitimacy of counter-extremism intervention depends not only on outcomes but on fairness, transparency, and consistency. Taken together, these lenses suggest that Pakistan needs neither a speech-suppressive security model nor a purely reactive criminal law model, but a calibrated framework that links early lawful intervention with strict protections against arbitrariness.

3. Methodology

This study employs a qualitative doctrinal and policy-analysis methodology. The primary materials are constitutional provisions, statutes, publicly available amendments, official policy documents, and reported institutional mandates relevant to digital radicalisation in Pakistan. The doctrinal component examines the substantive and procedural architecture of the legal regime, with special focus on the Constitution of Pakistan 1973, the ATA 1997, PECA 2016, the Prevention of Electronic Crimes (Amendment) Act 2025, and the Qanun-e-Shahadat Order 1984. The analysis also considers publicly accessible mandates and policy statements of NACTA and other criminal justice institutions.

The secondary-material component reviews contemporary peer-reviewed scholarship, policy reports, and reputable analytical publications on online radicalisation, platform governance, digital evidence, and counter-extremism law. Sources were selected on three criteria: direct relevance to digital radicalisation, analytical value for the Pakistani setting, and reliability of publication. The purpose was not to conduct a statistical meta-analysis, but to synthesise doctrinal, policy, and comparative insights into a coherent legal argument.

Methodologically, the article proceeds through four steps. First, it clarifies the concept of digital radicalisation and identifies the forms of online conduct most relevant to criminal justice:

incitement, recruitment, facilitation, propaganda, glorification, and coordination. Second, it maps the Pakistani legal framework and evaluates where the core powers, offences, and safeguards currently lie. Third, it assesses the operational problems of applying those rules in practice, particularly questions of overbreadth, attribution, authentication, jurisdiction, and inter-agency coordination. Fourth, it formulates normative recommendations based on constitutional principles, comparative regulatory developments, and the demands of evidential fairness.

4. Pakistan's Existing Legal and Institutional Framework

Pakistan's response to digital radicalisation is dispersed across several legal and institutional sites. The ATA remains the principal anti-terrorism instrument and is designed to address acts intended to intimidate the public, coerce government, or create fear through serious violence and related conduct. In the digital setting, the ATA becomes relevant when online activity amounts to encouragement, support, facilitation, coordination, financing, or operational connection with terrorism. However, the ATA was not originally crafted for platform-mediated radicalisation, and its terminology can become strained when applied to diffuse digital conduct that is ideational, symbolic, or preparatory rather than immediately operational.

PECA was enacted to address a wider range of electronic offences, including unlawful access, interference, data misuse, electronic fraud, cyberstalking, and certain forms of unlawful online content. Its practical relevance to digital radicalisation lies in its content-related provisions, investigatory powers, and regulatory interface with telecommunications and platform control. The 2025 amendment further expanded the state's role in relation to social media governance, including a new offence linked to dissemination of false or fake information and the institutional restructuring of oversight and investigation. While these developments reflect the state's concern with online harms, they also intensify long-standing rule-of-law concerns about vagueness, breadth, and the concentration of discretionary power.

Constitutional law remains an essential counterweight. Freedom of speech in Pakistan is not absolute, but restrictions must still be legally grounded, proportionate, and connected to legitimate aims such as the integrity, security, or defence of Pakistan, public order, decency, or morality. That constitutional structure matters because digital radicalisation policy often tempts lawmakers to legislate at the level of anxiety rather than precision. The constitutional question is therefore not whether harmful extremist content may be regulated; it plainly may. The question is whether the terms of regulation are sufficiently clear, reviewable, and limited to avoid arbitrary or discriminatory enforcement.

Evidentiary law creates an additional layer of complexity. Digital investigations require reliable attribution of authorship, custody, context, and integrity. Screenshots alone may be incomplete or manipulated. Anonymous accounts, reposted content, spoofed identities, end-to-end encryption, and deleted metadata complicate proof. The Qanun-e-Shahadat Order and general criminal procedure do not disappear in cyberspace; rather, they require adaptation through better digital forensics, chain-of-custody protocols, expert testimony, and standards for preserving context. Without these safeguards, digital prosecutions can become either ineffective or unfair.

Institutionally, the challenge is fragmented enforcement. The Federal Investigation Agency investigates cybercrime. Provincial Counter Terrorism Departments and police handle terrorism-linked matters. Prosecutorial services, trial courts, telecom regulators, and policy bodies each hold partial authority. NACTA has a coordinating and policy role, but coordination in law does not always translate into integration in practice. As a result, Pakistan's response can oscillate between under-enforcement against genuinely dangerous conduct and overbroad intervention against speech or online activity that is offensive, false, or politically controversial but not properly terrorism-related.

5. Discussion

Five major problems emerge from the doctrinal analysis.

First, the legal threshold for intervention is not sufficiently differentiated. Pakistani law needs clearer separation between mere possession or exposure, ideological sympathy, expressive endorsement, unlawful incitement, recruitment, material support, and operational facilitation. Collapsing these categories into a single discourse of 'extremism' risks punishing status or viewpoint instead of conduct. A criminal justice framework must focus on demonstrable connection to harm, violence, recruitment, instruction, financing, or coordinated support.

Second, some speech-related provisions remain vulnerable to overbreadth. Broadly framed offences relating to glorification, fake information, or harmful content may serve legitimate state aims in narrow circumstances, but they can also be deployed in a manner that suppresses critical speech, minority expression, journalism, or political contestation. That danger is especially acute when executive or regulatory bodies exercise blocking or takedown powers without robust reasons, notice, appeal, and independent judicial oversight. Counter-radicalisation law loses legitimacy when it becomes indistinguishable from general information control.

Third, evidentiary fragility remains one of the most serious operational barriers. In digital cases, context is everything. A reposted video may be shared for endorsement, criticism, documentation, or research. A screenshot may omit prior messages, edits, timestamps, or account identifiers. Encrypted communication may create inference gaps. Courts therefore require stronger evidential protocols than are often visible in routine cyber-investigation practice. At minimum, prosecutions should rest on preserved metadata, verified extraction methods, device-linkage evidence, and contextual interpretation rather than isolated screen captures or decontextualised posts.

Fourth, Pakistan's framework remains too punitive and insufficiently preventive in a principled sense. A mature preventive model does not mean earlier punishment for weaker evidence. Rather, it means creating lawful non-penal interventions for lower-level risk: referral systems, digital-literacy initiatives, community support, disengagement pathways, and monitored compliance measures that sit below criminal prosecution. Such a structure would reserve the heaviest coercive tools for conduct that meets clear thresholds of incitement, facilitation, or operational support.

Fifth, institutional coordination is still underdeveloped. Digital radicalisation cases often cut across cyber forensics, terrorism intelligence, platform engagement, prosecution strategy, and judicial evaluation. Without specialised case-routing, joint protocols, and shared evidentiary standards, agencies will continue to duplicate effort or work at cross-purposes. Fragmented enforcement is especially dangerous where one agency treats a matter as simple content violation while another views it as terrorism facilitation. Coherence requires structured jurisdictional guidance and interoperable practice.

These weaknesses do not support an argument for legal passivity. On the contrary, they demonstrate why Pakistan needs a narrower but stronger framework. The goal is not to decriminalise dangerous online conduct. The goal is to identify with precision the types of conduct that justify criminal intervention and to ensure that investigation and adjudication meet constitutional and evidential standards. The most effective response to digital radicalisation is therefore not maximalist censorship or loosely worded criminalisation. It is calibrated legality.

6. Conclusion

Digital radicalisation in Pakistan should be treated neither as a purely technological problem nor as a justification for limitless control over online speech. It is a criminal justice problem with constitutional dimensions. The existing framework - centred on the ATA, PECA, regulatory blocking practices, and general evidentiary law - provides partial tools but not a fully coherent model. It is strongest where online conduct can be tied to recruitment, incitement, or operational support for terrorism. It is weakest where the state relies on vague speech categories, broad executive discretion, or thin digital proof.

The central claim of this article is that Pakistan needs a principled, layered response in which criminal law addresses incitement, recruitment, facilitation, and terrorist support; regulatory

powers are supervised and reviewable; evidentiary practice meets rigorous forensic standards; and prevention includes education, referral, disengagement, and rehabilitation. Such a model would better protect both public safety and constitutional legitimacy. In that sense, the challenge of digital radicalisation is not simply how to expand state power, but how to discipline it.

7. Recommendations

The study recommends that relevant statutes be amended to create separate and clearly defined offences for online incitement to terrorist violence, digital recruitment, and operational facilitation, with each offence containing explicit mens rea and actus reus requirements. It further recommends narrowing vague or catch-all speech provisions so that restrictions on content are tied to demonstrable risk, intent, and a clear nexus with violence or unlawful support, rather than ideological disagreement or mere offensiveness. In addition, measures such as blocking, takedown, and account restrictions that significantly affect freedom of expression or access to information should be subjected to prompt judicial review. The study also proposes the development of national digital-forensics protocols for terrorism-related electronic evidence, including standards for preservation, metadata capture, translation, contextual analysis, and expert verification. Alongside this, specialized training modules should be introduced for prosecutors and judges on online extremist ecosystems, encrypted communications, digital evidence, and comparative jurisprudence concerning speech and security. Institutional reform is also necessary, particularly through the formalization of inter-agency case coordination between the FIA, Counter Terrorism Departments, prosecutors, regulators, and NACTA by means of written case-routing guidelines and accountability mechanisms. At the same time, the legal response should not remain exclusively punitive; it should incorporate non-penal prevention measures such as digital literacy initiatives, civic resilience programmes, referral pathways, and rehabilitation or disengagement mechanisms for lower-risk cases. Finally, the study recommends the commissioning of transparent periodic reviews of counter-radicalisation powers, including the publication of aggregate data on content removals, investigations, prosecutions, and case outcomes in order to strengthen accountability and enhance public trust.

8. References

Aryaeinejad, K., & Scherer, J. (2024). Digital radicalisation and extremist adaptation in online environments. Journal of Policing, Intelligence and Counter Terrorism, 19(1), 1-18.

Center for Justice. (2023). Rights, regulation and due process in Pakistan's cyber-law framework. Islamabad: Center for Justice.

DataReportal. (2025). Digital 2025: Pakistan. Retrieved from https://datareportal.com/reports/digital-2025-pakistan

Digital Rights Foundation. (2025). Analysis of Pakistan's Prevention of Electronic Crimes (Amendment) Act 2025 and implications for digital rights. Lahore: Digital Rights Foundation.

Institute for Economics & Peace. (2025). Global Terrorism Index 2025: Measuring the impact of terrorism. Sydney: Institute for Economics & Peace.

Institute for Economics & Peace. (2026). Global Terrorism Index 2026: Measuring the impact of terrorism. Sydney: Institute for Economics & Peace.

National Counter Terrorism Authority. (2024). National Prevention of Violent Extremism Policy. Islamabad: NACTA.

National Counter Terrorism Authority. (2025). Message from the National Coordinator and policy implementation materials. Islamabad: NACTA.

Pakistan. (1973). Constitution of the Islamic Republic of Pakistan.

Pakistan. (1984). Qanun-e-Shahadat Order, 1984.

Pakistan. (1997). Anti-Terrorism Act, 1997.

Pakistan. (2016). Prevention of Electronic Crimes Act, 2016.

Pakistan. (2025). Prevention of Electronic Crimes (Amendment) Act, 2025.

Scrivens, R., & Gaudette, T. (2024). Online hate, extremist ecosystems, and pathways of radicalisation. Terrorism and Political Violence, 36(2), 211-229.

Sohail, M. (2024). Youth, online grievance, and extremist messaging in Pakistan. Contemporary South Asia, 32(3), 355-372.

Warraich, U. A., Ahmed, S., & Riaz, H. (2023). Social media, misinformation, and violent extremism in Pakistan. Pakistan Journal of Criminology, 15(4), 77-101.