REVIEW OF CRIME, PEACE AND SOCIETY
ISSN (O): 3079-6105, ISSN (P): 3079-6091
Vol. 3, No. 2, 2026, 411-419

Artificial Intelligence and Cyber Law in Pakistan: Emerging Legal Challenges in Protecting Digital Infrastructure

Liaquat Ali Maitlo[1], Imam Ali Pathan[2], & Muhammad Tabasum Malhan[3]

Abstract

The digital economy has grown at a rapid pace in Pakistan over the last ten years, with the rise of mobile banking, e-governance, satellite television, and the early introduction of artificial intelligence (AI) in financial services, the media, and public administration. This growth has outstripped the nation's capacity to regulate the dangers associated with it. Meanwhile, Pakistan is dealing with two challenges: it is both a brand new and more advanced source of threats to the country's digital infrastructure in the form of artificial intelligence-generated deepfakes, disinformation, automated frauds, and intrusion tools, and it is also a tool that the regulators and critical sector institutions are being asked to use in the interest of national security. The current article explores the emerging legal and institutional framework of cyber governance in Pakistan, including the Prevention of Electronic Crimes Act 2016, the controversial amendment of the same act, 2025, the National Cyber Security Policy, and the recently approved National AI Policy 2025. The article provides an evidence-based assessment of Pakistan's current regulatory framework, citing recent enforcement actions, regulatory circulars, and a series of attacks on the country's national broadcasting and financial infrastructure, which highlights its fragmentation, reactive nature, and inherent structural limitations in addressing AI-related risks. It highlights five fundamental legal deficits (no binding data protection legislation, no liability framework tailored to the various levels of risk, inadequate attribution and enforcement possibilities, regulatory fragmentation between sectoral authorities, and human rights issues due to overly generic content-control regulations) and suggests a law reform agenda based on comparative practice.

Article History
Received 26 May 2026
Revised 29 July 2026
Accepted 30 July 2026
Published 03 August 2026

OPEN ACCESS

Keywords
Artificial intelligence, cyber law, Pakistan, PECA, critical infrastructure, data protection, deepfakes, digital governance

Introduction

Cyberspace is no longer only an economic tool for inclusion in Pakistan but also a controversial area of security. A report by the State Bank of Pakistan (SBP) indicates that the percentage of financial transactions via digital banking and payment channels has increased, pushing the Pakistan Financial

[1] PhD Scholar, Department of Criminology, University of Sindh, Jamshoro. Email: maitloliaquatali659@gmail.com
[2] Postgraduate Scholar, Department of Criminology, University of Sindh, Jamshoro. Email: imamalipathan96@gmail.com
[3] MPhil Scholar & Teaching Assistant, Department of Criminology, University of Sindh, Jamshoro. Email: mohammadtabasummalhan@gmail.com

Inclusion Index higher as account ownership has now touched 67% of adults in the country. Meanwhile, the very rails that are used to transport this financial inclusion are the main target of fraud, data breaches, and disruption of payment systems. The Pakistan Computer Emergency Response Team (PKCERT) received 927 cyberattacks that targeted public and private critical infrastructure throughout 2024-2025, with the 253rd attack of the year, in the form of a ransomware attack on a government organization, restoring data from backup. AI plays a pivotal role in this dynamic threat scenario in two ways. One, AI is now a tool that can help malicious actors: The Federal Investigation Agency (FIA) has reported that financial fraud, impersonation of public officials, and inappropriate non-consensual imagery are all increasingly common forms of crimes committed by AI-generated deepfakes in Pakistan, and security researchers have identified Pakistan-linked and Pakistan-targeting advanced persistent threat (APT) groups using AI-generated "vibe ware" and synthetic content in espionage operations. Second, AI is poised to be considered a vital defensive measure: The finance minister has publicly stated that the finance sector is facing threats from AI, and the SBP's Cyber Shield strategy for 2026 explicitly identifies AI-enabled fraud detection as one of the principles of financial-sector resilience. The dual nature of the AI as a threat vector and as a defense tool poses its own unique regulatory challenge. A system that is designed solely for traditional ideas of "unauthorized access" or "data theft" can't effectively prevent harm from the authorized use of a generative or autonomous system for crafting believable synthetic materials, making automated decisions, and probing defenses at machine pace. This article looks at Pakistan's existing framework of laws in the context of the problem and highlights the gaps in the law (Bhatti & Afraz, 2025; Malik & Gul,2024).

Pakistan's Cyber Legal Architecture: Evolution and Current Structure

1. The Prevention of Electronic Crimes Act (PECA) 2016 and its 2025 Amendment

Since its enactment in 2016, PECA has been Pakistan's main cybercrime law, which prohibits both unauthorized access and identity theft and cyber-fraud. In the absence of a dedicated data protection law, it serves as the closest law to protect personal data—and continues to do so. The government in January 2025 enacted the Prevention of Electronic Crimes (Amendment) Act 2025, which took effect on the date of its publication in the Government Gazette, 29 January 2025, and is the most significant restructuring of the law since the last enactment in 1995. The amendment has three aspects to digital infrastructure protection. First, a new offense (Section 26A) is created, which criminalizes the dissemination of ‘false or fake information' that is ‘likely to cause fear, panic, or unrest,' punishable by up to three years' imprisonment and up to PKR 2 million in fine. Secondly, it establishes new institutions such as the Social Media Protection and Regulatory Authority (SMPRA), also called the Digital Rights Protection Authority (DRPA), that has the authority to register, monitor, and order the blocking of online platforms, and the National Cyber Crime Investigation Agency (NCCIA), which merged the cybercrime wing of the FIA. Third, it broadens the scope of what constitutes a social media platform to include virtually any digital communication platform used in Pakistan, and it allows the chairperson of the SMPRA to initiate an emergency content blocking procedure, only to be ratified thereafter within 48 hours (Karim, 2026; Ahmed, et al.,2025).

This amendment has garnered significant concerns by civil society and human rights groups. In its review, Pakistan's National Commission for Human Rights (NCHR) found that the Aspiration clause in the law is bringing criminal defamation back to the country and downgrading the freedom of expression rights guaranteed by Articles 19 and 19A of the Constitution. But Human Rights Watch has said that the law's broad definitions and lack of judicial scrutiny of blocking provisions alike are inadequate to safeguard the public against real threats to online security and respect fundamental rights. The conflict between the legitimate need for policing of AI-powered disinformation and fraud and the danger that provisions of AI-adjacent policies are used as “censorship” devices is present in almost every AI-adjacent gap that was identified later in this article. The Digital Nation Pakistan Act 2025 (DNPA) was passed along with PECA, creating two new entities, the National Digital Commission

for policy formulation for national digital transformation and the Pakistan Digital Authority (PDA) to formulate and implement a National Digital Masterplan. Both cybersecurity and AI governance now have an institutional home in the DNPA, which will serve as a hub for digital governance in Pakistan, in addition to the sectoral regulators SBP, National Electric Power Regulatory Authority (NEPRA), and Pakistan Telecommunication Authority PTA (Ahmed, et al.,2025; Ahmed, et al., 2025).

2. National Cyber Security Policy, CERT Rules, and Critical Information Infrastructure

The National Cyber Security Policy (NCSP), first drafted in 2021, lays out the goals, such as establishing a governance mechanism for a cyber secure environment and graded information sharing between CERT/SOC and security standards for Critical Information Infrastructure (CII). NCERT can designate both public and private systems as CII if their incapacitation would have a significant impact on national security or economic and social well-being under the CERT Rules 2023; federal ministries have to identify candidate infrastructure and submit it for designation as CII; NCERT establishes grading criteria to classify CII by risk tier. There is clear progress in 2026 in institutional capacity. After a series of coordinated attacks such as PakSat satellite feeds hijacking that hampered news channels during peak evening bulletins, NCERT set up a 24/7 National Cybersecurity Control Room in Islamabad for coordination of ISPs, sectoral CERTs, and provincial CERTs, and mandates reporting of suspicious activity. In a yet-to-be-finalized Pakistan Information Security Framework 2026 (PISF 2026), which is deemed the country's first standard cybersecurity compliance and audit framework, and under cabinet and parliamentary review through mid-2026, PKCERT has asked all public and private entities to set up Security Operations Centres (SOCs) within a period of six months (Ahmad, et al., 2024; Malik, et al.,2025).

3. The Missing Piece: Data Protection Legislation

In Pakistan, there is no data protection law—GDPR equivalent—which has been enacted. The draft Personal Data Protection Bill 2023 and the revised draft Bill 2025 passed by the Federal Cabinet but have not yet passed through the National Assembly and Senate, and the promulgated version may differ greatly from the current draft. As it stands, the draft bill necessitates the creation of a National Commission for Personal Data Protection, will mandate data localization for 'critical personal data,' and will place a 'parental consent' requirement on data collected by children, while reportedly exempting state agencies from many of its obligations. While PECA 2016 and sector-specific rules are not being implemented, they remain the only existing and narrower law to regulate the misuse of personal information in Pakistan, including in the context of the use of AI systems (Saleem, et al., 2023; Malik &Gul,2024).

The National AI Policy 2025: Ambition Without Enforcement Architecture

The Federal Cabinet, with the leadership of Prime Minister Shehbaz Sharif on 30th–31st July 2025, unanimously approved the National Artificial Intelligence Policy 2025, a national artificial intelligence strategy for the first time in the country. The AI policy aims to put in place six strategic pillars: building an AI innovation ecosystem, mass awareness and workforce readiness (with a goal of one million trained professionals and 10,000 trainers by 2027) a secure AI ecosystem; sectoral transformation in health, education, agriculture, and governance; national AI infrastructure; and international collaboration. It establishes an AI Council and AI Implementation Directorate to oversee a Master Plan and Action Matrix, regionally spread Centres of Excellence, and regulated sandboxes for supervised testing of AI applications and sets up a National AI Fund (NAIF) for financing research and commercialization. In terms of security, the third pillar of the policy calls for an AI Directorate to provide regulatory guidance on topics such as misinformation, data breaches, and privacy concerns, as well as on providing a place for testing. The ethical goals include fairness, transparency,

accountability, and the protection of personal data, privacy, and human rights in the use of AI (Burfat et al., 2026; Sohail, 2025).

But independent legal scrutiny has unveiled major flaws. The Digital Rights Foundation's review also indicates that the policy fails to specify a tiered classification of AI systems similar to that of the EU AI Act, which introduces a classification of unacceptable, high-risk, and limited-and-minimal-risk AI systems, and Pakistan does not explicitly ban high-harm uses of AI, like social scoring or exploitative behavioural manipulation. The policy also doesn't mention who owns the intellectual property rights on the AI system or its outputs, which could lead to conflicts in university–startup partnerships. The policy also doesn't provide any clarity on who owns the intellectual property rights of the AI system and/or its outputs, which could present a future scenario for disputes in university–startup partnerships. Most importantly for infrastructure protection, the policy is not a law but a blueprint of what an AI Directorate might look like and a sign of future sanctions for non-compliance and creates no specific enforcement body, license regime, or compliance mechanism that could check for unsafe or malicious use of AI. In the absence of the promised AI Bill, Pakistan's AI governance is based on the policy aspiration that is overlaid on a cybercrime statute, PECA, which was not originally created to deal with autonomous or generative AI systems. This has partly been filled by the regulators in the sector, who have started their own regulatory work. In April 2025, the SBP announced its finalization of guidelines on the responsible use of AI in financial services, which will promote trust, transparency, and accountability in financial products powered by AI, including guidelines for banks to incorporate in their overall risk management frameworks the environmental and operational risk profile of AI. Involving SBP Deputy Governor and key stakeholders such as 1LINK, JazzCash, and NayaPay, the discussions held by the Pakistan Fintech Network indicated progress toward a distinct banking-sector AI framework to tackle issues of bias and risk to financial stability, though as of writing, it is still a policy in progress instead of a rule in itself (Ahmad, 2026).

Artificial Intelligence as Both Weapon and Shield: The Empirical Picture

1. AI-Enabled Harms to Persons and Institutions

The most striking case of the disruption of the legal impact of AI in Pakistan is the rise in the number of deepfake and impersonation cases. According to the Digital Rights Foundation, in one year (2024) there were 3,171 new cases of image and voice manipulation using AI; roughly 1,180 complaints about deepfakes and non-consensual imagery, most of which were from women, were reported in 2023, with only 12 of those cases leading to charges and only 7 to convictions, according to FIA data. This is a legal red flag and indicates that current PECA legislation that is based on traditional understandings of harassment and electronic forgery is not easily translatable to content created by AI systems and that investigative and evidentiary skills are not yet commensurate with the technology. The damage also works with the worst cases of abuse. According to a study conducted by the Child Light Global Child Safety Institute in 2025, Pakistan has over one million reported cases of child sexual abuse material, which are also high for South Asia, given the trend of AI-generated images of child sexual abuse, which surged by over 1,300% in a year, facilitated by the high number of tools that can create realistic explicit images of real children from a few normal photos. There are instances where children were blackmailed using AI-generated images, according to FIA records. There have been cases of minors being blackmailed with AI-generated images, according to FIA records. On its own, FIA has pursued cases under PECA against those who have used the AI to create fake videos of state officials and public figures, including an arrest in Sadiqa for making AI-generated videos of public figures and officials in Pakistan last month that showed that Pakistan's current law could be interpreted to cover synthetic political content. Fraud is another growing threat in the financial industry that makes use of AI technology. Industry experts said that the rise in complaints of fraud from 3,489 in 2023 to 4,171 in 2024 and 4,615 in 2025 was due to the growing sophistication and use of AI in social engineering and transaction-pattern exploitation. Meanwhile, AI is touted as the

solution: SBP and industry experts nowadays tout the benefits of real-time AI-driven transaction monitoring over the old-fashioned rule-based fraud detection (Ünver, 2024).

2. AI and Critical Infrastructure: The 2026 Attack Wave

The group of 2026 events have been a case in point of the increasing intersection between AI-related risk and the national digital infrastructure. The coordinated attacks on PakSat's satellite uplink disrupted live transmissions at Geo News, ARY News, and Samaa TV during peak viewing hours of evening bulletins and showed unauthorized anti-military messages, leading to two nationwide advisories to be issued by NCERT and PEMRA for strengthening the encryption of the uplink and intrusion detection mechanisms of broadcasters. At roughly the same time, researchers at Bitdefender observed the Pakistan-based APT36 group using trusted cloud services as delivery infrastructure to compromise Indian government networks, creating AI-generated vibeware, or tooling written to a large extent with the help of generative AI, in the process. The officials said the ransomware attack on a Pakistani government agency, which was backed up and restored, was not an isolated case but a part of the trend of 2026. The collective incidents show that the infrastructure considered nominally private, such as the broadcasters, banks, etc., is indeed critical national infrastructure and treated as such by the regulatory authorities through the hindsight lens; and that the attribution of attacks enabled by AI has been a huge challenge so far, which is hampering the criminal prosecution of such attacks as well as diplomatic response; and that the institutional response control rooms, mandatory SOCs, and sectoral CERTs as of now have been established through executive circulars and regulatory directives and not a codified statutory framework with clear obligations, liability, and penalties for the attacks helped by AI (Vaseashta, et al.,2025, November).

3. The Financial Sector's Parallel Track

The State Bank of Pakistan has taken the biggest step among the Pakistani regulators in having a structured response. It has announced a series of measures for regulated entities in the upcoming five years under its 'Cyber Shield' strategy, including the creation of a Financial Sector CERT (FinCERT) and implementation of Zero Trust Architecture, as well as five priorities of strengthening technical defenses, maturing governance and accountability, deepening industry-wide information-sharing, building specialized cyber workforce capacity, and adapting to external threat trends. In a preceding step, the country held the first industry-wide cyber drill involving 34 institutions jointly conducted by SBP and the Pakistan Banks' Association, followed by an industry-wide warning from the minister to the bank CEOs and Chief Information Security Officers (CISO) regarding the increasing sophistication of AI-driven attacks to find vulnerabilities and multi-stage attacks (May 2026). The momentum in this particular sector is instructive, as it serves as an example to regulators of the speed at which they can move through a circular and strategic paper, but it also suggests that in Pakistan, the most advanced governance on AI-cybersecurity exists in the banking sector, and so far, there is no comparable binding framework for the energy, telecom, healthcare, or broadcast infrastructure sectors (Srivastav & Rohit,2025).

Emerging Legal Challenges: A Structural Diagnosis

Based on the above framework and incidents, Pakistan's current exposure can be categorized as follows: The above framework and incidents reveal five intertwined gaps that can be identified as the legal exposures of Pakistan: She isn't required to have a binding, enacted data protection law. Given Pakistan's continued use of a draft Personal Data Protection Bill from 2023, updated in 2025, that hasn't yet been promulgated as of 2026, Pakistan's AI systems trained on its personal data, or drawing inferences from it, will operate with minimal legal oversight. No statute mandates the appointment of a Data Protection Officer, no formal or statutory-breach-notification timetable applies in all sectors,

and no independent body is given authority to audit AI-supported data processing, which is done in the framework of PECA. It is a fundamental deficiency that is found in most of the AI governance laws across the globe (the EU AI Act and similar laws in South Asian countries), which is, of course, a data protection law that is already in place and functioning in their country before the AI Act. This is a basic deficiency: Most AI governance laws around the world (the EU AI Act and comparable laws in South Asian countries) are built on top of or alongside a working data protection law; Pakistan is trying to govern AI without a working data protection law. No AI liability or classification regime based on risk. The National AI Policy 2025 is a strategy and not a law. It does not apply a tiered risk classification similar to the one included in the EU AI Act; does not clarify liability in the case of high-impact harm to humans caused by an AI system used in critical infrastructure, financial services, and public administration sectors; and does not include a requirement for licensing or certification for high-impact deployments. If there is no such promised and not yet drafted AI bill, the harms resulting from autonomous or generative systems are now having to be carved out of general offenses like PECA: Electronic Fraud or Forgery, which were not constructed with the goals of model behavior, provenance of training data, or algorithmic decision-making. Conviction data from the FIAs' own complaints shows that 1,180 complaints of deep fakes were reported in just one year, leading to 12 convictions—a significant lack of enforcement action, possibly related to evidence being hard to establish, lack of specialized cybercrime units, and the reorganization of these units under the NCCIA, which lacks expertise in cybercrime evidence and investigations. The infrastructure level is also susceptible to attribution difficulties, including the case of PakSat and APT36, where attribution is linked to the state and its relationship with the APT, and the legal frameworks and institutions for criminal prosecution or a national security response are different (Vinh & Dat, 2026).

Regulatory Fragmentation: Overlapping Authorities. The institutional landscape of AI and cybersecurity in Pakistan is as crowded as ever now: SMPRA/DRPA and NCCIA for AI and cyber in the media; PTA for AI and cyber in the telecom sector; NEPRA for their respective sectors; NCERT/PKCERT under the National Cyber Security Policy and CERT Rules; and SBP for the financial sector and its rules on AI and cyber. All of these bodies have been established or significantly given powers in the same 12–18-month span (2025-2026), and the mandates for each are largely overlapping with respect to "critical infrastructure," "digital platforms," and "AI systems," and there is no specific legislation to resolve jurisdictional order. This increases the level of uncertainty for regulated entities as to compliance and leaves room for malicious actors and ambiguity for good-faith operators to exploit. Risk of human rights and legitimacy in provisions for content control. The PECA Amendment 2025 is especially notable in its broad definitions, such as the standard in Section 26A that uses the phrase “false or fake information,” which lacks specific definition, and the expanded “aspersion” provisions in Section 26, which apply to criticism of the State's institutions, which could be particularly challenging for AI governance. For effective legal responses to AI-driven disinformation, there needs to be some capacity to evaluate and respond to synthetic or fake content; however, in a state that is already lacking judicial authority over blocking orders as noted by the NCHR and international human rights bodies, the anti-disinformation tools could be misapplied to legitimate expression, threatening both civil liberties and the credibility of the law as a means of genuine AI safety (Vinh, D. X., & Dat, N. Q. (2026).

Comparative Perspective

Comparisons with other jurisdictions are helpful. Indeed, the European Union's AI Act explicitly sets out a risk-based approach and bans the use of practices that would be considered unacceptable risk; there is no mention of which in the National AI Policy 2025, while imposing graduated obligations on high-, limited-, and minimal-risk systems. With respect to digital likeness specifically, Denmark's 2025 Copyright Act amendment offers a model for consideration in Pakistan—it recognizes that a person's voice, body, and overall “likeness” are a form of property, giving victims a preemptive

statutory takedown right that circumvents the length of criminal proceedings that would otherwise be needed to secure a conviction for a deepfake, and without broadening the wide-ranging, speech-restrictive categories already challenged in PECA. While the exposure draft of the DPDP Act, 2023, is still a work in progress, it nonetheless demonstrates a regional peer that is on the path towards a formalized baseline standard for data protection on which sector-specific standards for the use of AI can be overlaid, as done in banking, healthcare, and government use (Khalid, 2025).

Conclusion

Since early 2025, the legal profession in Pakistan has transformed itself in a visible way, with new institutions, strategies, and circulars cropping up at a rapid pace to address the twin challenges of harm caused by AI and the need to defend using AI. However, the backbone of the system remains rather incomplete: a cybercrime law that is being extended beyond the scope designed for; an AI policy that has set lofty goals that have yet to be solidified by an enforceable body; a data protection law that has languished for years; and an ever-expanding patchwork of regulators with no clear overarching statutory structure. All of these are examples of the attacks against PakSat's broadcast infrastructure, financial frauds using AI, and the disparity between complaints and convictions for deepfakes are symptoms of this structural incompleteness. Bridging that gap will necessitate Pakistan to do what many of its peer jurisdictions have started: Create a rights-based, risk-based, codified governance framework for this rapidly evolving technology instead of attempting to govern it through an amendment to a cybercrime law from ten years ago.

References

Aaj English TV, FIA Arrests Suspect for Making Fake Videos of State Officials (2025).

Ahmad, F. (2026). A National AI Infrastructure Strategy for Pakistan: A Practical Roadmap for Building Sovereign AI Capability at Low Cost. *Available at SSRN 7059398*.

Ahmad, J. B., Hussain, M. A., & Mir, H. A. (2024). Developing a legal framework for digital policy: A roadmap for AI regulations in Pakistan. *Law and Policy Review*, *3*(1), 162-188.

Ahmed, F. A., Gul, S., & Shahzad, S. (2025). Ensuring accountability and transparency in AI-driven corporate governance. *International Journal of Social Sciences Bulletin*, *3*(5), 330-341.

Ahmed, F. A., Zafar, S., & Gul, S. (2025). Analyzing PECA amendments: Press freedom, democratic values, and digital regulation in Pakistan. *Traditional Journal of Law and Social Sciences*, *4*(01), 41-51.

Ahmed, S., Yaakub, A. N., & Javed, A. (2025). Artificial Intelligence in Pakistan's Cyberspace: Governance Gaps, Dual-Use Dilemmas, and Strategic Vulnerabilities. *Obrana a Strategie (Defence & Strategy)*, *25*(2), 3.

Arab News, Pakistan Finance Minister Calls for Stronger Cyber Defenses as Financial Sector Digitizes.

Associated Press of Pakistan (APP), Pakistan's AI Trust Challenge: Can It Be Fixed?

Bhatti, A., & Afraz, T. (2025). Digital Innovation, Data, And Rights: Reassessing Pakistan's Intellectual Property and Cyber Law Framework. *Data, And Rights: Reassessing Pakistan's Intellectual Property and Cyber Law Framework (November 28, 2025)*.

Burfat, A. R., Lanjwani, B. A., & Oad, H. (2026). Pakistan's AI governance framework and national policy (2025): A reappraisal. *Research Consortium Archive*, *4*(2), 1013-1025.

Center for International Strategic Studies (CISS), commentary on Pakistan's critical infrastructure cybersecurity vulnerabilities.

Digital Pakistan, Banks in Pakistan Gear Up for AI Regulations.

Digital Rights Foundation Tracker; The News (Pakistan); SCWorld; HackRead; Rankiteo; Pajhwok — reporting on the March 2026 PakSat/Geo News/ARY News/Samaa TV satellite hijacking incidents and subsequent PEMRA/NCERT advisories.

Digital Rights Foundation, DRF Analyses Pakistan's National AI Policy 2025 (2026).

DLA Piper, Data Protection Laws of the World — Pakistan (updated March 2026).

Fadhil, T. H., Al-Haddad, L. A., & Al-Karkhi, M. I. (2025). Legal accountability and UAV fault diagnosis explainable AI in aviation safety and regulatory compliance for liability challenges. *Discover Artificial Intelligence*, *5*(1), 410.

GenderIT.org, Between Privacy and Power: The Fine Line in Pakistan's Data Protection Bill.

HackRead, Pakistan-Linked APT36 Floods Indian Govt Networks With AI-Made 'Vibeware' (March 2026).

Karim, A. (2026). Cybersecurity Governance in Pakistan: Institutional Gaps, Policy Failures, and Strategic Reforms. In *Digital Transformation and Sustainability in South Asia* (pp. 221-245). Cham: Springer Nature Switzerland.

Khalid, U. (2025). The digital battlefield: A comparative analysis of AI-driven cyber warfare in the US and china and its implications for pakistan's national security. *ASSAJ*, *4*(01), 64-76.

Lexology, Year in Review: Privacy, Data Protection and Cybersecurity in Pakistan.

Malik, W, Gul, S, (2024). Cyber conflict and international security: Legal challenges and strategic solutions in cyberspace.

Malik, W., & Gul, S. (2024). Bridging the gap: Exploring the intersection of cybersecurity and human security in the digital age. *Competitive Research Journal Archive*, *2*(04), 195-202.

Malik, W., Gul, S., & Qureshi, G. M. (2025). Regulating artificial intelligence: Challenges for data protection and privacy in developing nations. *Journal of Social Signs Review*, *3*(05), 95-108.

Ministry of Information Technology and Telecommunication, National Artificial Intelligence Policy 2025 (moitt.gov.pk).

National Commission for Human Rights (NCHR), Report on PECA and the 2025 Amendment Act (2026).

Pakistan Information Department (PID), Finance Minister Chairs Virtual Meeting on Strengthening Cybersecurity Preparedness in the Financial Sector (2 May 2026).

PIDE Knowledge Brief, Will AI Transform Pakistan? Assessing the 2025 National AI Policy.

Profit (Pakistan Today), SBP to Finalize Guidelines for Responsible AI Use in Pakistan's Financial Sector (27 April 2025).

ProPakistani, NCERT Prepares Guidelines to Safeguard National Critical Information Infrastructure (2024); IT Ministry Issues Draft of National Cyber Security Policy 2021.

Rankiteo, Pakistani Government Entity Hit by Ransomware as Cyberattacks Surge in 2026 (PKCERT disclosure, Fortinet Security Day Karachi 2026).

Regulations.ai, Pakistan — National AI Policy (2025) and Pakistan — Electronic Crimes Amendment (II/2025) regulatory summaries.

SAHSOL, LUMS, The PECA Amendment 2025: A Critical Analysis; and Deepfakes and Digital Identity: What Pakistan Can Learn from Denmark's Deepfake Law.

Saleem, M. S., Malhooz, F., & Fatima, T. (2023). From Cyber-crimes to Cyber-Security: Exploring Legal Minefield of Artificial Intelligence in Pakistan. *Pakistan Research Journal of Social Sciences*, *2*(3).

Sohail, R. A. O. (2025). Pakistan's National AI Policy 2025: A Comparative Appraisal, Advantages, Risks, Execution Pathways, and Regional Benchmarks. *INNOVAPATH*, *1*(3), 12-12.

Srivastav, P., & Rohit, P. (2025). Artificial Intelligence-Driven Vulnerability Assessment and Automated Threat Mitigation in Modern Cybersecurity Systems. *Available at SSRN 7234398*.

State Bank of Pakistan, Cyber Shield: Cyber Resilience Strategy for SBP Regulated Entities (2025–2030), CRMD Circular Letter No. 01 (16 February 2026).

The Express Tribune, Adopting AI May Cut Banking Fraud (26 July 2026).

Ünver, H. A. (2024). Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights. *European Parliament, Directorate-General for External Policies. PE*, *754*.

Vaseashta, A., Bancilă, R., & Radu, D. (2025, November). Integrating Artificial Intelligence and Smart Materials into Critical Infrastructures. In *International Scientific Conference Civil Engineering and Buildings Services* (pp. 810-845). Cham: Springer Nature Switzerland.

Vinh, D. X., & Dat, N. Q. (2026). COMPUTATIONAL LEGAL DIAGNOSTICS AND THE LIMITS OF HUMAN LEGAL REASONING. *International Journal of Law, Culture & Society*, *2*(2).