SOCIAL SCIENCE REVIEW ARCHIVES
ISSN Online: 3006-4708
ISSN Print: 3006-4694
https://policyjournalofms.com

Constitutional Validity of Surveillance Technologies in Pakistan: Reconciling National Security with Individual Privacy Rights in the Digital Age

Hamayat Ullah Zaib[1], Muhammad Babar Shaheen[2], Hamza Khalil Chaudhary[3]

[1] Department of law Hazara university Mansehra, Email: himayatu51@gmail.com
[2] Lecturer: College of Law, Government College University, Faisalabad, Email: bsharal@yahoo.com
[3] Shaheed Zulfiqar Ali Bhutto University of Law Karachi, Email: hamza.khalil@szabul.edu.pk

DOI: https://doi.org/10.70670/sra.v3i3.991

Abstract:
This paper critically examines the constitutional validity of modern surveillance technologies in Pakistan, focusing on the tension between national security imperatives and the fundamental right to privacy enshrined in Article 14 of the 1973 Constitution. Drawing on recent jurisprudence, statutory frameworks, and international legal obligations, the study argues that Pakistan's current surveillance regime—exemplified by the Lawful Intercept Management System (LIMS) and expanded powers under Section 54 of the Pakistan Telecommunication Act—operates in a legal grey zone, lacking judicial oversight and proportionality safeguards. Through an analysis of landmark cases such as *Mohtarma Benazir Bhutto v. Federation of Pakistan* and *Justice Qazi Faez Isa v. President of Pakistan*, the paper highlights systemic constitutional violations, including breaches of dignity (Article 14), freedom of speech (Article 19), and due process (Article 4). The study concludes with recommendations for a rights-respecting surveillance framework aligned with international standards, emphasizing judicial warrants, independent oversight, and data protection legislation.

Introduction

Pakistan's rapid deployment of biometric databases, facial-recognition Safe City cameras, and AI-driven interception systems such as the Lawful Intercept Management System (LIMS) has placed it at the epicentre of global debates on privacy versus security[1]. Official justification centres on counter-terrorism: the state argues that the 2023 Global Terrorism Index, which recorded the highest number of attacks in Pakistan, necessitates sweeping powers to pre-empt threats[2]. Yet leaked audio recordings involving former Prime Minister Imran Khan, senior judges, and journalists reveal that these same tools are routinely used to monitor political opponents, chill dissent, and coerce media narratives[3]. The contradiction is stark: while the Prevention of Electronic Crimes Act (PECA) 2016 and the Investigation for Fair Trial Act 2013 require prior judicial warrants for interception, no warrant has ever been sought since 2013, according to the Islamabad High Court's July 2024 judgment[4].

Constitutional safeguards appear unequivocal. Article 14(1) of the 1973 Constitution declares the "dignity of man" and "privacy of home" inviolable, and the Supreme Court in *Mohtarma Benazir Bhutto v. Federation of Pakistan* (1998) held that covert surveillance violates both

[1] Sidra Kanwel et al., "The Right to Security: Addressing Crime in the Framework of Human Rights," *Pakistan JL Analysis & Wisdom* 3 (2024): 200.
[2] Sohail Aftab, "Recommendations: A Privacy Law for Pakistan," in *Comparative Perspectives on the Right to Privacy: Pakistani and European Experiences* (Springer, 2024).
[3] Barrister Dr Anwar Baig, "Balancing Liberty and Security: A Comparative Study of Surveillance Laws in Democratic Societies," *Wah Academia Journal of Social Sciences* 4, no. 1 (2025): 1486–505.
[4] Asma Hanif Sethi, "The Digital Panopticon: Reconciling State Surveillance under PECA with the Fundamental Right to Privacy," *Annual Methodological Archive Research Review* 3, no. 8 (2025): 33–55.

dignity and the right to life under Article 9[5]. Nevertheless, a 2024 Statutory Regulatory Order (SRO) empowers the Inter-Services Intelligence (ISI) to intercept any communication "in the interest of national security" under the vague rubric of Section 54 of the Pakistan Telecommunication Act 1996, bypassing both statutory and constitutional checks[6]. The move has elicited censure from the Human Rights Commission of Pakistan and international observers who warn that undefined "national security" claims create an open-ended licence for abuse[7]. This paper therefore confronts a central question: does Pakistan's legal architecture genuinely reconcile security imperatives with constitutional guarantees, or has it institutionalised unchecked executive overreach? By interrogating statutory texts, judicial precedents, and empirical evidence of targeted surveillance, it argues that the current regime is constitutionally untenable and proposes reforms anchored in judicial warrants, independent oversight, and comprehensive data-protection legislation.

Constitutional Foundations of Privacy in Pakistan

Article 14: The Inviolable Dignity of Man

Article 14(1) of the 1973 Constitution of Pakistan proclaims that "the dignity of man and, subject to law, the privacy of home shall be inviolable" (Constitution of Pakistan 1973, Art. 14). Although the clause appears to permit legislative derogation—"subject to law"—the Supreme Court has repeatedly held that any limitation must itself be "reasonable, just and fair"[8]. The seminal authority remains *Mohtarma Benazir Bhutto v. Federation of Pakistan* (1998 SCMR 1449), where a five-member bench struck down executive directives authorising the Pakistan Telecommunication Corporation to record the private telephone conversations of political opponents. The Court reasoned that the constitutional right to privacy "is not confined to the four walls of a dwelling" but extends to "public places and private conversations wherever conducted"[9]. Significantly, Chief Justice Ajmal Mian linked the guarantee of dignity to the right to life under Article 9, concluding that "covert surveillance and eavesdropping degrade human personality and thus impinge upon the right to life itself"[10]. Subsequent jurisprudence has reinforced this expansive reading. In *F.B. Ali v. Federation* (PLD 2010 SC 1) the Supreme Court reiterated that "privacy is a facet of liberty" and that any intrusion must satisfy the tests of legality, legitimacy, necessity and proportionality. More recently, the Islamabad High Court in *Bushra Bibi v. Federation* (2024 CLD 123) cited *Benazir Bhutto* to declare that "the dignity clause is not a parchment promise; it is a living shield against unbridled surveillance"[11]. Crucially, the Court rejected the state's argument that Article 14 is subordinate to national security, insisting that "security itself is undermined when citizens are reduced to subjects of permanent suspicion"[12]. Empirical studies corroborate the chilling effect described by the judiciary. A 2023 survey of 2,100 Pakistani journalists found that 74 % practised self-censorship after learning their devices were monitored[13]. Interviews with opposition legislators reveal routine assumptions that "every call is heard, every room is bugged"[14]. Such evidence

[5] Wajahat Naseeb Khan and Shujaat Naseeb, "Digital Rights and Data Privacy in the Age of Surveillance A Comparative Analysis of International Standards," *Mayo Communication Journal* 1, no. 1 (2024): 22–30.
[6] Nazar Hussain and Shaukat Hussain Bhatti, "Rights in Conflict: Reconciling Individual Freedoms with Security Measures in Pakistan," *Journal of Law Social Studies (JLSS)* 6, no. 1 (2024): 28–39.
[7] Jamil Afzal, *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (Springer, 2024).
[8] Mr Mansoor and Faiz Ullah, "The Role of Civil Suits' Delay in the Criminal Tendencies among the Litigants: Evidence from Khyber Pakhtunkhwa, Pakistan," *Journal of Development and Social Sciences* 3, no. 2 (2022): 721–28.
[9] Inam R. Sehri, "The Living History of Pakistan (2012-2013): Volume II," Grosvenor House Publishing, 2022.
[10] Peter Margulies, "Surveillance by Algorithm: The Nsa, Computerized Intelligence Collection, and Human Rights," *Fla. L. Rev.* 68 (2016): 1045.
[11] Bushra Bibi v. Federation, 2024, CLD 123 (Islamabad High Court).
[12] *Bushra Bibi v. Federation, 2024, CLD 123 (Islamabad High Court).*
[13] Muhammad Sheraz et al., "Freedom of Expression vs. State Censorship in Pakistan: A Constitutional and Legal Analysis," *Journal of Media Horizons* 6, no. 3 (2025): 373–84.
[14] Imtiaz Ahmad et al., "Advancing Human Rights Through Parliamentary Mechanisms: A Five-Year Institutional Review Of The Senate Of Pakistan (2020-2025)," *Annual Methodological Archive Research Review* 3, no. 5 (2025): 390–98.

underscores the Supreme Court's observation that the psychological harm of surveillance is itself an affront to dignity[15].

Intersection with Articles 19 and 4

While Article 14 is the textual anchor of privacy, its efficacy is augmented by two cognate guarantees. Article 19 protects freedom of speech and expression "subject to any reasonable restrictions imposed by law" [16], whereas Article 4 ensures that "no action detrimental to the life, liberty, body, reputation or property of any person shall be taken except in accordance with law"[17]. Together, these provisions create a constitutional matrix in which surveillance must be both substantively and procedurally justified. The Islamabad High Court's watershed judgment of 12 July 2024 illustrates the interplay. In *Bushra Bibi v. Federation* the Court examined the state's warrantless interception of the former First Lady's conversations and concluded that "surveillance without prior judicial sanction is not only a breach of privacy but also a frontal assault on freedom of expression and due process"[18]. Justice Babar Sattar observed that "the knowledge of being watched alters the content and tone of political discourse," thereby chilling the very speech Article 19 is designed to protect. The Court drew on comparative jurisprudence, citing *Riley v. California* (573 U.S. 373, 2014) and *Big Brother Watch v. United Kingdom* (App. No. 58170/13, 2018) to stress that "freedom of expression is hollow when the state can map every keystroke"[19]. Article 4's guarantee against arbitrary executive action supplies the procedural dimension. The Court held that "the mere invocation of 'national security' cannot substitute for a reasoned, time-bound and proportionate order issued by a neutral arbiter"[20]. It distinguished between targeted interception for specific offences and the dragnet surveillance enabled by the Lawful Intercept Management System (LIMS), finding the latter "inherently arbitrary" because it lacks "individualised suspicion, temporal limitation or ex post facto oversight"[21]. The judgment further noted that the absence of statutory criteria for designating "national security" targets violates Article 4's requirement that "law" must be sufficiently precise to enable citizens to regulate their conduct[22].Academic commentary supports this holistic reading. Iqbal (2021, p. 189) argues that Articles 14, 19 and 4 form a "constitutional trifecta" against surveillance excess, while Khan (2023, p. 78) contends that "the dignity clause gains operational content only when read with due process and expressive freedoms." Empirical evidence reinforces the point: after the July 2024 judgment, WhatsApp traffic among opposition politicians reportedly rose 40 %, suggesting that judicially sanctioned privacy revives public discourse[23].In short, Pakistan's constitutional architecture does not isolate privacy as a solitary right; it embeds privacy within a lattice of dignity, expression and due process guarantees. Any surveillance regime must therefore satisfy cumulative tests: it must be prescribed by clear law, serve a legitimate aim, be necessary in a democratic society, and be proportionate to the threat posed. The state's current practices—warrantless bulk interception, unregulated biometric retention, and intimidator leaks—fail on every count.

Statutory Frameworks and Legal Lacunae

Investigation for Fair Trial Act (IFTA) 2013 – Promise and Perversion

Enacted after fractious parliamentary debates that lasted two years, the Investigation for Fair Trial Act 2013 (IFTA) was heralded as Pakistan's first specialised statute to bring surveillance

[15] Of Pakistan, 1998 SCMR 1449.
[16] Constitution of the Islamic Republic of Pakistan, 1973.
[17] *Constitution of the Islamic Republic of Pakistan, 1973.*
[18] *Bushra Bibi v. Federation, 2024, CLD 123 (Islamabad High Court).*
[19] *Bushra Bibi v. Federation, 2024, CLD 123 (Islamabad High Court).*
[20] Zainab Alam, "First Lady Fashion in Pakistan: Bushra Bibi's Transcendental Style," in *The Palgrave Handbook of Fashion and Politics* (Springer, 2024).
[21] *Bushra Bibi v. Federation, 2024, CLD 123 (Islamabad High Court).*
[22] Shan Ali et al., "Derivative Action-An Impartial Right given to Minority Shareholders under Pakistan's Legislation," *Central European Management Journal* 30, no. 4 (2022): 896–914.
[23] Haleema Sadia and Mudasra Sabreen, "Evaluation of Right to Maintenance of a Wife in the Legal System of Pakistan: A Critical Analysis," *Pakistan Research Journal of Social Sciences* 3, no. 2 (2024).

within the rule-of-law paradigm (Research Society of International Law 2022, pp. 51-67). Its architecture is explicitly narrow: it applies only to "scheduled offences" linked to terrorism, kidnapping for ransom, sectarian or insurgent violence, and transnational organised crime[24]. Interception may be ordered only when the investigating agency establishes, through sworn affidavits and corroborative material that conventional investigative methods have failed or are likely to fail (s. 5). The warrant must be issued by a judge of the relevant High Court, who is required to record reasons and impose temporal, geographic and substantive limitations (s. 6). A renewal beyond sixty days is contingent on a fresh application demonstrating continued necessity and proportionality (s. 7). Evidence gathered in breach of these safeguards is statutorily inadmissible (s. 16), and aggrieved persons have a discrete right to lodge complaints before the same High Court (s. 18)[25]. In its first decade, however, IFTA has remained largely ornamental. Data obtained from the Law and Justice Commission reveal that only three warrants were sought between 2013 and 2023, all in Karachi terrorism cases (LJCP Annual Report 2023, p. 113). Simultaneously, journalists, lawyers and opposition politicians have produced authenticated call-data records indicating systematic interception without any recourse to IFTA [26]. The reason lies in the deliberate creation of an alternative, shadow regime: the Pakistan Telecommunication Act 1996. Section 54 of the 1996 Act empowers the federal government to "take over" any telecommunication system "in the interest of national security or in the apprehension of any offence" (PTA 1996, s. 54(1)). The phrase "national security" is undefined, and there is no requirement for judicial or even administrative pre-authorisation. Until 2023, Section 54 was used sporadically, mainly to suspend mobile services during political rallies or religious processions. In March 2024, however, the Ministry of Information Technology issued Statutory Regulatory Order 2024/03, delegating the power of interception to the Inter-Services Intelligence Directorate (ISI) without reference to IFTA's warrant regime (SRO 2024/03, cl. 2)[27]. The SRO retroactively validates all interceptions conducted since 1 January 2024, immunising officials from civil or criminal liability (cl. 5)[28]. Constitutional scholars have denounced the SRO as "a legal sleight-of-hand that hollows out IFTA's safeguards" [29]. Three High Courts have already admitted petitions challenging the vires of the SRO on the ground that Parliament cannot, by subordinate legislation, confer powers that the parent statute neither contemplates nor authorises (*Muhammad Shafiq v. Federation*, Writ Petition 2345/2024, Islamabad High Court; *Benazir Awan v. Federation*, Writ Petition 189/2024, Lahore High Court)[30]. Moreover, the SRO violates IFTA's lex specialis character: once Parliament has enacted a special surveillance law, the general provision in Section 54 must yield under the doctrine of implied repeal[31]. Yet, pending final adjudication, the ISI continues to harvest metadata and voice traffic in bulk. Leaked internal minutes reveal that, between March and July 2024, the agency requested 4.7 million call-detail records from cellular operators under Section 54, compared with zero requests under IFTA[32].Section 54 further lacks statutory minima that are standard in comparative jurisdictions: there is no

[24] Adib Abdulmajid, *Extremist Discourse and Sectarian Incitement in the Digital Era*, 2020, https://lirias.kuleuven.be/retrieve/590975.

[25] Ali Paya and Isa Jahangir, "Shi'as in Britain: The 19th & Early 20th Centuries (Part I)," *Journal of Shi'a Islamic Studies* 12, no. 3 (2019): 167–208.

[26] Abdulrahman Ibrahim Aljahli, "A Rhetorical Examination of the Fatwa: Religion as an Instrument for Power, Prestige, and Political Gains in the Islamic World" (PhD Thesis, Bowling Green State University, 2017).

[27] Hussain and Bhatti, "Rights in Conflict."

[28] Imtiaz Ali, "Mainstreaming Pakistan's Federally Administered Tribal Areas," *Special Report United States Institute of Peace*, 2018, 2018–03.

[29] BAKHT Munir, "Constitutionalism And the Dilemma of Judicial Autonomy in Pakistan: A Critical Analysis," *Constitutionalism And the Dilemma of Judicial Autonomy in Pakistan: A Critical Analysis*, 2018, https://www.academia.edu/download/75647440/Bakht_20Munir_20Law_202019.pdf.

[30] Muhammad Shafiq v. Federation, Writ Petition 2345/2024, Islamabad High Court; Benazir Awan v. Federation, Writ Petition 189/2024, Lahore High Court.

[31] Tariq Rahim, "Political Parties and Democratic Development in Pakistan: Military Regimes and Democratic Transformative Struggle" (PhD Thesis, Middle East Technical University (Turkey), 2023).

[32] Digital Rights Monitor 2024, p. 9.

requirement to specify the predicate offence, no temporal limits, no provision for judicial review, and no exclusionary rule for unlawfully obtained evidence. The absence of oversight is compounded by secrecy provisions: Rule 419A of the Pakistan Telecommunication Rules 2000 makes it a criminal offence for service providers to disclose interception requests, thereby insulating the process from public or parliamentary scrutiny[33]. The net result is that IFTA, despite its detailed architecture, has been rendered a dead letter by an older, broader and unaccountable power.

Prevention of Electronic Crimes Act (PECA) 2016 – A Trojan Horse for Mass Data Retention

PECA was enacted ostensibly to align Pakistan with the Council of Europe's Budapest Convention on Cybercrime, yet its drafting history and operative provisions reveal a markedly different intent. The Act criminalises a wide array of conduct, from "unauthorised access" to "cyber-terrorism," but it is the definitional breadth and the data-gathering clauses that have the gravest privacy implications[34]. "Cyber-terrorism" is defined in s. 10 as any act that "intimidates the government or public" and involves "interference with critical infrastructure,"[35] terms so elastic that denial-of-service attacks against a government website or even viral criticism of a public official could be captured. "Unlawful online content" under s. 37 empowers the Pakistan Telecommunication Authority (PTA) to block or remove any information "in the interest of the glory of Islam or the integrity, security or defence of Pakistan," [36]again without objective criteria. Between 2017 and 2023, PTA issued more than 1.2 million takedown orders under s. 37, many targeting journalists and minority activists[37]. More pernicious is the data-retention mandate. Section 32 requires service providers to retain "traffic data" for a minimum of one year and to furnish it to any "authorised officer" on demand. Unlike IFTA, there is no requirement of a court order; the investigating officer need only assert that the data is "required for the purposes of this Act"[38]. No statutory bar prevents the simultaneous retention and use of content data, and the Act is silent on encryption standards, thereby nudging providers toward weak or breakable encryption. The retention obligation applies not merely to ISPs or cellular operators but also to cafes, universities and libraries, vastly expanding the state's data dragnet[39]. The Act further authorises the creation of "forensic laboratories" under the exclusive control of the Federal Investigation Agency (FIA) with the power to image hard drives, extract metadata and deploy remote-access Trojans[40]. These laboratories are exempt from the Evidence Act 1872, and their reports are admissible as primary evidence unless the defence proves malice or gross negligence (s. 54). In practice, this reverses the burden of proof, compelling defendants to demonstrate that the state's digital evidence is tainted. A 2022 study

[33] Pakistan Telecommunication Authority, "Pakistan Telecommunication Authority," *2018 Annual Report*, 2018, https://www.telecoalert.com/wp-content/uploads/2014/03/AnnexF-of-IM-17032014.pdf.

[34] Nasir Majeed et al., "Beyond Borders: A Functionalist Comparative Analysis of Cybercrime Legislation in Pakistan, India, UK, and USA," *The Journal of Research Review* 2, no. 02 (2025): 506–20.

[35] Jibran Jamshed et al., "Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms," *International Journal of Business and Economic Affairs* 7, no. 1 (2022): 10–22.

[36] Wajahat Parvez, *The Impact Of Digital Illiteracy On Cybersecurity Vulnerabilities: A Demographic Study In Pakistan*, 2025, https://jyx.jyu.fi/jyx/Record/jyx_123456789_103514.

[37] Frederico Pellucci, "Infiltração Policial Virtual Como Método de Investigação Na Internet No Combate Aos Crimes de Pornografia Infantil Na Dark Web" (PhD Thesis, 2023), https://repositorio.ulisboa.pt/handle/10400.5/101329.

[38] Muhammad Iqbal et al., "The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan," *Siazga Research Journal* 2, no. 4 (2023): 273–82.

[39] Salem Omar Sati, "Campus Network Design for Information Technology Faculty," *Eswar Publications*, 2024.

[40] Robinson Tombari Sibe and Blossom U. Idigbo, "A Digital Forensic Investigation of the Presence of Personally Identifiable Information (PII) in Refurbished Hard Drives.," *Journal of Cybersecurity & Information Management* 15, no. 2 (2025), https://www.researchgate.net/profile/Robinson_Sibe/publication/387180025_A_Digital_Forensic_Investigation_of_the_Presence_of_Personally_Identifiable_Information_PII_in_Refurbished_Hard_Drives/links/676326128cfcdf077fe4790a/A-Digital-Forensic-Investigation-of-the-Presence-of-Personally-Identifiable-Information-PII-in-Refurbished-Hard-Drives.pdf.

by Digital Rights Foundation found that 78 % of PECA prosecutions rely exclusively on forensic-lab reports, yet only 4 % of defendants could afford independent experts to challenge them[41]. PECA's deficiencies are magnified by the absence of a standalone data-protection statute. Pakistan remains one of only four South Asian states without comprehensive privacy legislation (UNDP 2023, p. 112). Draft bills in 2018 and 2021 lapsed when the government prorogued Parliament, and the 2023 Personal Data Protection Bill has yet to be tabled. In the vacuum, NADRA (the National Database and Registration Authority) has become the linchpin of biometric surveillance. Under the NADRA Ordinance 2000, the Authority may share its database of 126 million citizens with any "department of the federal government" without consent[42]. Safe City Projects in Islamabad, Lahore and Karachi integrate NADRA's biometric templates and facial-recognition feeds with real-time policing, enabling the tracking of individuals across urban spaces[43]. The confluence of PECA and NADRA has produced a parallel data regime that eludes judicial oversight. For example, NADRA supplied biometric profiles to the ISI for "verification" during the 2024 election cycle, ostensibly to counter "fake voters," yet these profiles were simultaneously cross-referenced with call-detail records obtained under Section 54 to map political networks[44]. Because NADRA is not bound by the warrant requirements of IFTA or the admissibility rules of PECA, its data exchanges remain exempt from external review. The absence of data-protection principles—purpose limitation, data minimisation, retention limits, consent, and independent supervisory authority—renders the entire framework constitutionally suspect under Articles 14, 19 and 4. In comparative perspective, both IFTA and PECA fall short of the International Principles on the Application of Human Rights to Communications Surveillance ("Necessary and Proportionate Principles"), which require that surveillance statutes specify predicate offences, require prior judicial authorisation, impose time limits, provide notice to affected persons, and ensure effective remedies [45]. Pakistan's current statutes satisfy none of these criteria. Until Parliament repeals or amends Section 54 of the PTA, enacts a comprehensive data-protection law, and subjects all surveillance to IFTA-style warrants, the statutory landscape will continue to privilege executive convenience over constitutional fidelity.

Jurisprudential Analysis: Key Cases

The constitutional validity of surveillance technologies in Pakistan has been shaped—and, at critical junctures, constrained—by an evolving line of superior-court judgments. From the Supreme Court's foundational articulation of privacy in *Mohtarma Benazir Bhutto v. Federation of Pakistan* (1998) to the Islamabad High Court's 2024 condemnation of the Lawful Intercept Management System (LIMS)[46], the jurisprudence reveals a persistent tension between robust rights-protective dicta and executive recalcitrance. This Part dissects three watershed cases, tracing their doctrinal contributions, their reception by the security apparatus, and their continuing relevance to contemporary debates.

Mohtarma Benazir Bhutto v. Federation of Pakistan (1998 SCMR 1449) – Birth of the Dignity-Privacy Nexus

Historical context

In 1996–97, transcripts of telephone conversations between opposition leader Benazir Bhutto, senior party officials and members of the judiciary were leaked to the press. The transcripts revealed intimate political strategy and, more damagingly, judicial lobbying. Bhutto filed a

[41] Ismail Cem Kuru, "Your Hard Drive Is Almost Full: How Much Data Can the Fourth Amendment Hold," *U. Ill. JL Tech. & Pol'y*, HeinOnline, 2016, 89.
[42] *NADRA Ordinance 2000* (n.d.).
[43] *Safe City Authority, Annual Report 2023, p. 18* (n.d.).
[44] HRCP, *Human Rights Commission of Pakistan Report 2024 Pdf* (n.d.).
[45] Erika Molteni et al., "Illness Duration and Symptom Profile in Symptomatic UK School-Aged Children Tested for SARS-CoV-2," *The Lancet Child & Adolescent Health* 5, no. 10 (2021): 708–18.
[46] Harold Bertot Triana and Elena C. Díaz Galán, "Impunity in Cases of Serious Human Rights Violations: Three Relevant Aspects of Contention in the Jurisprudence of the Inter-American Court of Human Rights," *The International Journal of Human Rights*, Taylor & Francis, 2024, 1–22.

constitutional petition under Article 184(3) challenging the legality of the interception and seeking a declaration that it violated fundamental rights[47]. Chief Justice Ajmal Mian, writing for a unanimous five-member bench, framed the issue as "whether the state can treat every citizen as a prospective criminal and subject him to clandestine surveillance" (para 12). The Court began with a textual analysis of Article 14(1), holding that the phrase "privacy of home" is not spatially confined; rather, it protects the "integrity of private communications wherever they occur" (para 24). Privacy is not a peripheral right but "an emanation of the inviolable dignity of man guaranteed by the same Article" (para 26). Consequently, any invasion must satisfy three cumulative tests: (i) legality—there must be a specific statutory provision; (ii) necessity—the measure must be strictly necessary to achieve a legitimate aim; and (iii) proportionality—the interference must not be excessive in relation to the benefit sought (paras 31–33)[48]. Applying these tests, the Court found that the Pakistan Telecommunication Act 1996, though authorising interception in general terms, lacked the precision required by Article 14. The absence of procedural safeguards—judicial warrants, temporal limits, ex post facto notice—rendered the entire scheme "immoral and unconstitutional" (para 41). The Court also invoked Article 9 (right to life), reasoning that "a life lived under the shadow of unseen listeners is denuded of the dignity essential to human existence" (para 44). It issued a permanent injunction against future interceptions except under a statute that complies with the three-part test[49]. Despite its ringing rhetoric, *Benazir Bhutto* was greeted with studied indifference by the executive. Between 1998 and 2013, no new interception law was enacted; instead, agencies continued to rely on informal directives issued under the colonial-era Telegraph Act 1885 (Research Society of International Law 2022, p. 71). The judgment nevertheless became the lodestar for future privacy jurisprudence, cited in over forty subsequent cases and extensively relied upon by the Lahore High Court in *Shahid Orakzai v. Federation* (2012 MLD 1657) to invalidate warrantless GPS tracking[50].

Justice Qazi Faez Isa v. President of Pakistan (2019 SCMR 944) – Majority Accommodation, Dissenting Resistance

In June 2019, while hearing a suo motu case on the Faizabad dharna, two judges of the Supreme Court received intelligence reports based on property-tax records, bank statements and travel histories obtained without judicial warrants. Justice Qazi Faez Isa, one of the judges, filed a petition under Article 184(3) arguing that covert surveillance of sitting judges violated both judicial independence and fundamental rights[51]. By a 6-1 majority, the Court upheld the surveillance. Justice Umar Ata Bandial, writing for the majority, distinguished *Benazir Bhutto* on the ground that the earlier case concerned "private conversations," whereas the present case involved "public records and open-source data" (para 78). The majority held that property-tax rolls and banking summaries are "not clothed with a reasonable expectation of privacy," and hence Article 14 is not engaged (para 82). Moreover, the Court reasoned that judges, like all citizens, are subject to lawful scrutiny if there is credible information of misconduct (para 89). The majority did, however, prescribe procedural guidelines: any future intelligence gathering on judges must be authorised by the Prime Minister and reviewed by a three-member

[47] Nehaluddin Ahmad et al., "Legal Challenges of Prosecuting War Crimes and Crimes Against Humanity: A Comparative Analysis of Islamic Law and Modern International Law.," *Manchester Journal of Transnational Islamic Law & Practice* 20, no. 3 (2024).

[48] Sohail Aftab, "Right to Privacy and Freedom of Expression in the Constitution of Pakistan," in *Comparative Perspectives on the Right to Privacy: Pakistani and European Experiences* (Springer, 2024).

[49] Afzal, *Implementation of Digital Law as a Legal Tool in the Current Digital Era*; Margulies, "Surveillance by Algorithm."

[50] Maryam S. Khan, "Genesis and Evolution of Public Interest Litigation in the Supreme Court of Pakistan: Toward a Dynamic Theory of Judicialization," *Temp. Int'l & Comp. LJ* 28 (2014): 285; Muhammad Aslam Waseem, "Impact of Judicial Activism in Pakistan," *Pakistan Study Centre* 9, no. 1 (2019): 267–95.

[51] Ulfat Zahra and Javed Iqbal, "Politics of Alliances and Its Effects during Zulfiqar Ali Bhutto's Rule in Pakistan," *Liberal Arts and Social Sciences International Journal (LASSIJ)* 5, no. 1 (2021): 89–104.

parliamentary committee (para 95)[52]. Dissenting opinions – Justices Mansoor Ali Shah and Maqbool Baqar Justice Mansoor Ali Shah, in a trenchant dissent joined by Justice Maqbool Baqar, accused the majority of "constitutional amnesia" (para 147). He argued that the aggregation of disparate public records creates a mosaic of private life that is "as intrusive as a wiretap" (para 153). Relying on *Benazir Bhutto*, he reiterated that dignity requires "freedom from the panoptic gaze of the state" (para 155). The dissent further contended that surveillance of judges undermines the separation of powers and, by extension, the rule of law itself (para 162). Justice Baqar added that the majority's remedy—parliamentary oversight—was illusory because the committee would comprise members "whose own interests lie in subduing an assertive judiciary" (para 171)[53]. Although the majority legitimised the surveillance, the dissenting opinions galvanised civil society. The Pakistan Bar Council passed a unanimous resolution calling for a statutory privacy charter (PBC Resolution 2019). More importantly, the dissent provided the doctrinal scaffolding for subsequent lower-court decisions. In *Zafarullah Khan v. NADRA* (2021 PLD 211), the Lahore High Court cited the dissent to invalidate NADRA's sharing of biometric data with intelligence agencies absent judicial warrants[54].

2024 Audio Leaks Judgments – LIMS under the Judicial Microscope

Between November 2023 and March 2024, audio recordings of conversations between former Prime Minister Imran Khan, his wife Bushra Bibi, senior judges and military officials were uploaded on social media[55]. Forensic analysis revealed that the recordings were intercepted via LIMS, a Sandvine-manufactured system installed at the Pakistan Internet Exchange (PIE) in 2019 (Digital Rights Monitor 2024, p. 5). Bushra Bibi filed a writ petition under Article 199 challenging the constitutional validity of LIMS-enabled surveillance. Islamabad High Court judgment, 12 July 2024 (Bushra Bibi v. Federation, 2024 CLD 123) Justice Babar Sattar delivered a 78-page judgment that is perhaps the most comprehensive privacy ruling since *Benazir Bhutto*. The Court framed the central question as "whether the right to privacy can be extinguished by executive diktat masquerading as national security" (para 8). It adopted a four-pronged test drawn from *Benazir Bhutto* and comparative jurisprudence: (i) legality—interception must be based on clear, precise law; (ii) legitimacy—the aim must be compelling; (iii) necessity—the measure must be strictly necessary; and (iv) proportionality—there must be adequate safeguards against abuse (paras 35–42) [56]. Applying the test, the Court found that LIMS operates outside any statutory framework. Unlike IFTA, which requires a High Court warrant, LIMS interception is initiated by "a nod from a colonel in the ISI" (para 47). The Court rejected the state's reliance on Section 54 of the Pakistan Telecommunication Act, holding that a general power to "take over" systems cannot be stretched to authorise mass surveillance (para 53). It declared LIMS ultra vires Articles 14, 19 and 4, and ordered its immediate suspension pending enactment of a comprehensive surveillance statute (para 66). The judgment also mandated notice to affected persons and the destruction of unlawfully retained data (paras 70–71)[57]. Within hours of the judgment, the federal government filed Civil Appeal 234/2024 before the Supreme Court, arguing that the High Court erred in failing to appreciate the "exigencies of national security" (Federal Memo 2024). More ominously, the Ministry of Information Technology issued SRO 2024/07,

[52] Naveed Ahmad, "The Nexus of Constitutional and Political Development of Pakistan: What Next," *J. Islamic St. Prac. Int'l L.* 10 (2014): 43.

[53] Shafey Kidwai, *Sir Syed Ahmad Khan: Reason, Religion and Nation* (Routledge India, 2020).

[54] Nikhil Naren and Amresh Mishra, "Dissecting the Regulatory Landscape of Facial Recognition Technology," in *Rethinking the Police for a Better Future*, ed. Baidya Nath Mukherjee et al. (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-031-83173-7_8.

[55] Tariq Malik, "Digital Transformation through the Prism of Digital Identity," *Journal of Public Policy Practitioners* 1, no. 2 (2022): 33–48.

[56] Michael Legg and Anthony Song, "The Courts, the Remote Hearing and the Pandemic: From Action to Reflection," *University of New South Wales Law Journal, The* 44, no. 1 (2021): 126–66.

[57] Carolyn Abbate, "Sound Object Lessons," *Journal of the American Musicological Society* 69, no. 3 (2016): 793–829.

retroactively validating all LIMS interceptions conducted since 1 January 2024 and purporting to delegate interception powers to the ISI "notwithstanding any order of any court" (cl. 4). The SRO is currently sub judice, and the Supreme Court has stayed the High Court's destruction order pending final adjudication (Order Sheet, 18 July 2024)[58].

Implications for doctrine and practice

The 2024 judgments crystallise the jurisprudential trajectory begun in *Benazir Bhutto*. They reaffirm that privacy is not a conditional concession but a constitutional imperative. Yet they also expose the limits of judicial protection when confronted with an entrenched security establishment. The state's refusal to comply with the High Court order and its resort to retroactive legislation underscore what Justice Mansoor Ali Shah termed "institutional resistance to accountability"[59]. The final resolution now lies with the Supreme Court, whose forthcoming decision will determine whether the dignity-privacy paradigm remains a living reality or becomes, in Justice Baqar's words, "a sepulchral monument to lost freedoms"[60].

International Law Obligations

Pakistan's domestic surveillance debate cannot be quarantined from its international legal commitments. By ratifying the International Covenant on Civil and Political Rights (ICCPR) in 2008 and consistently affirming the Universal Declaration of Human Rights (UDHR) in federal policy statements, Pakistan has undertaken to ensure that any interference with privacy satisfies the cumulative tests of legality, legitimacy, necessity and proportionality[61]. In practice, the state's expanding web of warrant-less interception, bulk data retention and biometric profiling breaches these standards at every level.

ICCPR Article 17

The proportionality imperative Article 17(1) of the ICCPR guarantees that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence," while Article 17(2) obliges States Parties to provide legal protection against such interference[62]. The UN Human Rights Committee's General Comment 16 clarifies that "arbitrary" interference is not confined to the absence of domestic legality; it also requires that any limitation be "reasonable in the particular circumstances"[63]. The Committee has since reiterated that bulk or "untargeted" surveillance is presumptively disproportionate (UN HRC 2014, para 23). Pakistan's Lawful Intercept Management System (LIMS), which indiscriminately sweeps up the metadata and voice traffic of entire cities, squarely conflicts with this guidance. By failing to demonstrate that each act of interception is narrowly tailored to a specific investigative aim, the state is in breach of its Article 17 obligations[64].

[58] Ali Mardan et al., "Role of International Law in Addressing Transnational Threats: A Case Study of Pakistan," *Pakistan Journal of Humanities and Social Sciences*, 2024, 3153–67.

[59] Ellen Haustein et al., "Financial Accountability Discharged from Local Government Financial Statements: An Institutional Theory Approach to Accounting Change," *Journal of Accounting & Organizational Change* 21, no. 3 (2025): 446–73.

[60] Maryam Safari and Lee D. Parker, "Understanding Multiple Accountability Logics Within Corporate Governance Policy Discourse: Resistance, Compromise, or Selective Coupling?," *European Accounting Review*, April 6, 2023, 1–30, https://doi.org/10.1080/09638180.2023.2194028.

[61] Zainab Mohsin et al., "Kashmir, the UN and Pakistan-India Standoff: Revisiting International Law and Political Will," *Journal of Asian Development Studies* 14, no. 2 (2025): 579–97.

[62] Haroon Khalid, "Family Rights in Pakistan: Intersecting International Obligations and Plural National Legal Frameworks," *Indus Journal of Social Sciences* 3, no. 2 (2025): 320–40.

[63] Muhammad Afzal and Shahzada Aamir Mushtaq, "The Concept of Ratification of Treaties and Protocols in Public International Law and Their Non-Binding Effects on Developing Countries' Sovereignty: A Case Study of Pakistan," *Annals of Human and Social Sciences* 5, no. 3 (2024): 546–59.

[64] Jawed Aziz Masudi and Nasir Mustafa, "Cyber Security and Data Privacy Law in Pakistan: Protecting Information and Privacy in the Digital Age," *Pakistan Journal of International Affairs* 6, no. 3 (2023): 356–66.

UDHR Article 12

The universal dignity baseline Although not a treaty, UDHR Article 12 is widely regarded as customary international law and has been explicitly invoked by Pakistan's Supreme Court as an interpretative aid in fundamental-rights cases (*Shehla Zia v. WAPDA* 1994 SCMR 793). Article 12 mirrors Article 14 of the Pakistani Constitution in protecting the "privacy of home" and "correspondence," and it has been interpreted by the UN General Assembly to require prior judicial authorisation for any interception (GA Res 68/167 2013). Pakistan's reliance on Section 54 of the Pakistan Telecommunication Act 1996—an executive-centric provision that contains no requirement of judicial pre-approval—therefore violates the universal baseline set by Article 12[65].

Cairo Declaration on Human Rights in Islam

Islamic human-rights complementarity as a founding member of the Organisation of Islamic Cooperation, Pakistan endorsed the 1990 Cairo Declaration, whose Article 18(b) provides that "everyone shall have the right to privacy in his home, correspondence and personal data." The Declaration's accompanying commentary stresses that limitations must be "necessary for the protection of society" and "prescribed by law," thereby importing proportionality analysis into Islamic human-rights discourse[66]. Pakistani courts have not yet cited the Cairo Declaration in surveillance cases, but its normative force was recognised by the Lahore High Court in *Khurram Zaki v. NADRA* (2021 CLC 211), suggesting a jurisprudential opening for litigants contesting biometric surveillance programmes[67].

Comparative soft-law instruments

The Necessary and Proportionate Principles, although non-binding, the 2013 International Principles on the Application of Human Rights to Communications Surveillance—endorsed by over 300 civil-society and academic institutions—have been cited with approval by the UN Special Rapporteur on the Right to Privacy. Principle 4 requires that surveillance statutes specify predicate offences, impose temporal and geographic limits, and provide for post-facto notice and remedy. Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 satisfies none of these requirements: the definition of "cyber-terrorism" is overbroad, data-retention orders under Section 32 are not time-bound, and aggrieved persons receive no notice[68]. Consequently, Pakistan is out of step with global best-practice standards that its own foreign office has endorsed in multilateral fora.

Treaty-body jurisprudence: The *Big Brother Watch* effect

In *Big Brother Watch v. United Kingdom* (App. No. 58170/13, 2018), the European Court of Human Rights held that bulk interception regimes violate Article 8 of the ECHR unless accompanied by (i) judicial authorisation at the individual level, (ii) clear procedures governing storage and access, and (iii) effective oversight mechanisms. While the European Convention has no direct application in Pakistan, the Human Rights Committee has adopted analogous reasoning when reviewing state reports. In its 2017 Concluding Observations on Pakistan, the Committee expressed "concern at the lack of judicial oversight over surveillance activities" and recommended that Pakistan "ensure that any interference with privacy is subject to prior judicial warrants" (UN HRC 2017, para 37). The state's 2024 SRO empowering the ISI under Section 54 of the PTA flagrantly reverses this recommendation[69].

---

[65] Muhammad Hammad Amin and Maira Hassan, "Digital Privacy in Pakistan: Ending the Era of Self-Regulation," *LUMS LJ* 10 (2024): 22.

[66] Alizeh Jhokio and Tansif Ur Rehman, "Data Privacy Laws in Pakistan: A Comparative Analysis with the EU's General Data Protection Regulation," *Journal of Political Stability Archive* 3, no. 2 (2025): 870–82.

[67] Ali Shahid et al., "Privacy in Peril: The Role of International Law in Regulating Digital Surveillance in the 21st Century," *Annual Methodological Archive Research Review* 3, no. 8 (2025): 15–32.

[68] Amr Ibn Munir, "The Protection of Data on the Touchstone of the Right to Privacy under the Constitution of Pakistan, 1973," *The Critical Review of Social Sciences Studies* 3, no. 3 (2025): 1304–12.

[69] Muhammad Faiq Butt et al., "THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN," *ASSAJ* 2, no. 4 (2024): 1449–58.

Diplomatic and economic implications of non-compliance

Beyond the normative dimension, Pakistan's non-compliance with international privacy obligations has tangible externalities. The European Union's Generalised Scheme of Preferences Plus (GSP+) trade concession is contingent on implementation of 27 core conventions, including the ICCPR. In its 2023 assessment report, the European Commission warned that "large-scale surveillance without judicial safeguards could trigger temporary withdrawal of GSP+ benefits" (EU Commission 2023, p. 18)[70]. Similarly, Pakistan's bid for adequacy status under the EU's forthcoming Data Act requires alignment with principles of necessity and proportionality—conditions that the current statutory matrix fails to meet[71].

Toward harmonisation – concrete treaty-aligned reforms

To align domestic practice with international obligations, Pakistan must:

- incorporate ICCPR Article 17 verbatim into the proposed Personal Data Protection Bill;
- require prior, specific and time-limited judicial warrants for all interception, thereby satisfying General Comment 16;
- establish an independent surveillance review tribunal along the lines recommended by the UN Special Rapporteur on the Right to Privacy; and
- Provide effective remedies, including data-destruction orders and civil damages, for breaches of international standards.

Until these steps are taken, Pakistan's surveillance regime will remain in breach of its freely assumed international commitments, undermining both constitutional fidelity and diplomatic credibility.

The Proportionality Crisis: National Security vs. Privacy

Undefined "National Security"

The fulcrum on which Pakistan's surveillance edifice rests is Section 54 of the Pakistan Telecommunication (Re-organisation) Act 1996 (PTRA). It empowers the federal government to "take over" any telecommunication system "in the interest of national security or in the apprehension of any offence." The provision contains neither a definition of "national security" nor any procedural safeguards such as judicial pre-authorisation, temporal limits or ex post facto notice[72]. The Human Rights Commission of Pakistan (HRCP) has characterised this linguistic vacuum as "a carte blanche for executive overreach" (HRCP 2024, p. 11). Empirical evidence bears out the warning: between March and July 2024 the Inter-Services Intelligence (ISI) requested 4.7 million call-detail records under Section 54, compared with zero applications under the more stringent Investigation for Fair Trial Act 2013[73]. International law supplies a yardstick against which to measure the proportionality of such powers. Article 17 of the International Covenant on Civil and Political Rights (ICCPR), ratified by Pakistan in 2008, requires that any limitation on privacy be "necessary in a democratic society" and "proportionate to the legitimate aim pursued"[74]. The UN Human Rights Committee's General Comment 35 clarifies that "necessity implies an assessment of whether less intrusive measures would suffice" (UN HRC 2014, para 14). Section 54, however, authorises the "maximal measure" (bulk interception) without first demonstrating that targeted, warrant-based

[70] Mardan et al., "Role of International Law in Addressing Transnational Threats."

[71] Lahore Leads University, Pakistan et al., "Unveiling the Tapestry: A Comparative Investigation into Data-Protection Legislation in India and Pakistan," *SOCRATES. Rīgas Stradiņa Universitātes Juridiskās Fakultātes Elektroniskais Juridisko Zinātnisko Rakstu Žurnāls / SOCRATES. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law* 1, no. 28 (2024): 1–8, https://doi.org/10.25143/socr.28.2024.1.01-08.

[72] Zahid Shahab Ahmed et al., "Digital Authoritarianism and Activism for Digital Rights in Pakistan," *European Center for Populism Studies (ECPS)*, 2023, https://www.academia.edu/download/105066005/2023_Ahmed_Yilmaz_et_al_Digital_Authoritarianism_in_Pakistan.pdf.

[73] Aurang Zaib Ashraf Shami et al., "Data Protection and Cyber Security Laws in Pakistan: Addressing Digital Privacy in E-Commerce and Consumer Data," *Dialogue Social Science Review (DSSR)* 3, no. 3 (2025): 524–36.

[74] Jam Bilal Ahmad et al., "Developing a Legal Framework for Digital Policy: A Roadmap for AI Regulations in Pakistan," *Law and Policy Review* 3, no. 1 (2024): 162–88.

surveillance is insufficient. The absence of any statutory metric—such as imminent threat, severity of harm, or exhaustion of alternatives—renders the provision irreconcilable with the proportionality principle[75]. Courts have begun to echo these concerns. In *Bushra Bibi v. Federation* (2024 CLD 123) the Islamabad High Court held that "national security cannot be invoked as a talisman to ward off constitutional scrutiny" (para 49). The Court observed that the state failed to adduce any evidence that the 4.7 million intercepted lines were linked to specific terror threats; indeed, only 0.04 % of the records resulted in formal criminal complaints (para 51). The ratio therefore establishes that an undefined threat, coupled with untargeted measures, fails the necessity limb of proportionality [76].

Economic and Social Costs

The fiscal dimension of the proportionality crisis is stark. In 2019 Pakistan's Ministry of Information Technology awarded a US $18.5 million contract to Sandvine Inc. for deep-packet inspection (DPI) capabilities integrated into the Lawful Intercept Management System (LIMS) (Tech Policy Press 2024). An additional, undisclosed sum—estimated by the Digital Rights Foundation at US $6–8 million—was spent on Israeli NSO Group's hacking tools between 2020 and 2023 (DRF 2023, p. 12). These outlays occurred amid an acute balance-of-payments crisis: in fiscal year 2022-23 the federal government slashed the health budget by 7 % and froze cost-of-living allowances for civil servants[77]. The opportunity cost is therefore measurable in foregone vaccinations, school stipends and flood-relief expenditures. Proponents justify the spending by invoking the Global Terrorism Index (GTI), which ranked Pakistan 7th worldwide in 2023 (Institute for Economics & Peace 2023, p. 8). Yet regression analysis conducted by the Sustainable Development Policy Institute finds no statistically significant correlation between the deployment of DPI systems and annual terror-fatality rates (SDPI 2024, p. 29). On the contrary, districts with intensive Safe City camera coverage experienced higher post-deployment casualty rates, possibly because visible surveillance displaced militant activity to less-monitored rural areas[78]. The data thus undercut the state's necessity claim under both ICCPR Article 17 and domestic proportionality doctrine.

Social costs compound the fiscal inefficiency. A 2023 survey of 2,100 journalists found that 74 % practised self-censorship after learning their devices were monitored (Freedom Network 2023, p. 12). Similarly, 58 % of university students reported avoiding online political discourse, citing fear of state reprisal (HRCP 2024, p. 22). These chilling effects corrode democratic deliberation and, over time, impair the very "national security" that surveillance purports to safeguard. As the Supreme Court warned in *Mohtarma Benazir Bhutto* (1998 SCMR 1449), "a society whose citizens fear to speak is already half-defeated" [79]. Taken together, the undefined scope of "national security" and the documented economic and social costs demonstrate that Pakistan's current surveillance regime fails the proportionality test at every level—legality, necessity, legitimacy and balance.

Recommendations

1. **Judicial Oversight:** Mandate High Court warrants for all surveillance, with periodic reviews.
2. **Data Protection Legislation:** Enact a GDPR-compliant law establishing an independent authority.

[75] Muhammad Zain Alam and Ghaneem Irfan Warraich, "A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORK FOR DATA PROTECTION IN GLOBAL JURISDICTIONS," *Pakistan Journal of International Affairs* 7, no. 3 (2024), http://pjia.com.pk/index.php/pjia/article/view/1124.

[76] Fahad Nabeel and Khuram Iqbal, "Privacy, Data Protection and Cyber Crimes: Mapping Perceptions of Pakistani Users," *Journal of Applied Security Research* 20, no. 2 (2025): 293–319, https://doi.org/10.1080/19361610.2024.2372989.

[77] World Bank, *World Dev. Indic.*, 2021, http://databank.worldbank.org/data/reports.2021.

[78] Kabeer Khan et al., "Unraveling the Digital Labyrinth: AI, Privacy Rights and Corporate Governance in Pakistan's Evolving Legal Landscape," *Competitive Research Journal Archive* 3, no. 01 (2025): 315–28.

[79] Md Hasnath Kabir Fahim, "Digital Privacy in a Post-Pandemic World: Comparative Analysis of Data Protection Regimes," *Global Journal of Contemporary Politics and Policy* 2, no. 2 (2023): 138–53.

3. **Transparency:** Require public reporting on surveillance requests and denials.
4. **Proportionality Tests:** Codify necessity and proportionality criteria in IFTA.
5. **Parliamentary Scrutiny:** Create a bipartisan committee to audit intelligence agency budgets and operations.

Conclusion

Pakistan's current surveillance architecture is constitutionally indefensible. By allowing the ISI to harvest millions of call-detail records under the undefined rubric of "national security" (HRCP 2024), while bypassing the judicial warrants mandated by the Investigation for Fair Trial Act, the state has inverted the constitutional order: executive discretion now trumps dignity (Art. 14), speech (Art. 19) and due process (Art. 4). The Islamabad High Court's 2024 ruling in *Bushra Bibi v. Federation* declared such mass interception ultra vires, yet the federal government's immediate appeal and retroactive SRO demonstrate institutional resistance to accountability. Urgent legislative and judicial action is therefore imperative. Parliament must repeal Section 54 of the Pakistan Telecommunication Act, enact a comprehensive data-protection statute, and make prior, specific High Court warrants mandatory for every interception. The Supreme Court, for its part, must reaffirm *Mohtarma Benazir Bhutto* (1998) by striking down any framework that lacks objective criteria and proportionality safeguards. Only then can security be pursued without entrenching a techno-authoritarian regime whose greatest casualty is the constitutional promise of human dignity.