ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 04 No. 02. October-December 2025.Page# 3203-3215
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

Surveillance Technologies and Human Rights: Reassessing Privacy and Life Protections in Pakistan

(Analysing Risks under Articles 6 and 17 of ICCPR and the HRC's 2024 Concluding Observations)

Hafiz Muhammad Asad Ali
Ph.D. Scholar Law,
International Islamic University, Islamabad
Email: 01993phdlawf25@student.iiu.edu.pk

Abstract

The rapidly growing surveillance economy of telecommunication interception services, platform surveillance, biometric identification, and safe city infrastructures in Pakistan has far exceeded the rights protecting legislative framework and proper regulation in Pakistan. In a broader perspective of the implications of the current data protection mechanisms in Pakistan in the framework of the concept of privacy and the right to life in respect of Article 17 (privacy) and Article 6 (right to life) of the International Covenant of Civil and Political Rights (ICCPR), this article provides the posteriorizing of the privacy and life protection in this country with reference to the Concluding Observations of the UN Human Rights Committee (HRC) on Pakistan issued in 2024. It states that the main human rights danger is not so much more surveillance, but surveillance on the basis of indefinite legal permissions, insufficient ex-antes judicial perforations, little independent auditing, and shrouded technical constructions circumstances that not only permit invasions of privacy, but also augment the stakes harms, which involve patterns of intimidation, targeting, and the conditioning environment in general of forced removals. It is based on the constitutional guarantees of Pakistan, and the analysis critically on the judicial posture of Pakistan itself, with its proceedings in 2023-2024 on the subject of illegal phone tapping, and the Lawful Interception Management System (LIMS), where the judge becomes insistent on the concept of legality, due process, and constitutional accountability. The article suggests the pathway of reform of rights compatible: the reduction of legal foundations; restoration of judicial warrant, the rule; establishment of independent control and technical accountability; reinforcement of remedy and transparency; and adjustment of surveillance regulation to the HRC 2024 proposals, using Turabian notes bibliography style.

Keywords: *Pakistan; privacy; surveillance; right to life; ICCPR; Article 17, Article 6; Human Rights Committee; LIMS; lawful interception; enforced disappearance; constitutional law.*

1. Introduction

Surveillance has ceased to constitute a sporadic investigative tool and become a permanent structure of governance an ecosystem of technologies, institutional practices, procurement decisions, regulatory prescriptions, and judgement cultures that combined themselves to define what can be seen by the State, captured by the State, inferred by the State, and done with by the State.

In Pakistan, the transition is not disclosed in systematic form of transparency reporting or ongoing debate in parliament, it is exposed through the episodes of uproar: phone tapping scandals, repeated audio leaks, allegations of covert surveillance, and lawsuits compelling the State and its regulators to justify more or less how modern interception and data access actually functions. It has produced a regulative environment in which the authority to invade the privacy of life could be vast, and the law which purports to give it, and to limit it, is heterogeneous, disputed and hard to check.

The article is a reply to such a mismatch and provides a reassessment of the surveillance technologies in Pakistan within a two-fold human rights axis, the International Covenant of Civil and Political Rights, specifically Articles 17 (privacy) and 6 (right to life). The active focus on Article 17 is self-evident. The protection against illegal or unreasonable interference with privacy, correspondence, and home is directly involved, through surveillance by interception of communications, metadata collection, forced entry into subscriber information and by surveillance of online speech. However, surveillance governance cannot yet be considered a pure "privacy alone" issue in the current situation in Pakistan. Concluding Observations on Pakistan released by the Human Rights Committee (HRC) in 2024 put increased focus on surveillance and data practices by the state and still took the subject of forced disappearances and lack of accountability seriously. The implication of the normative is not that, surveillance is an equivalent of disappearance. It has the implication of structural conditionality: more state coercive capacities given conditions of secrecy, weak ex ante control, and weak independent oversight, the condition of protecting privacy in the rule of law ecosystem becomes the condition of making life protection services effective prevention, due diligence, investigation and accountability.

1.1 The definition of surveillance technologies in this paper.

In this article, the term surveillance technologies are adopted to find umbrella covering to a range of state enabled tools and systems that work at various levels of the communication and urban landscape. This can be encompassed at the telecom layer in lawful interception systems and network interfaces capable of providing access to voice and messaging content and related metadata, and less dramatic requests to subscriber and traffic data. At the layer of digital platforms, it involves surveillance, censorship, regulation of content and forced collaboration with law enforcers. On the urban security level, it consists of embedded camera systems, biometrics, and data fusion that have the capability of linking identities with movement, association, and location. The article does not presuppose that all the applications of such technologies are not legitimate. Nowadays, surveillance can be and is used legally under certain conditions, especially serious crimes prevention and national security by the states. Whether surveillance exists or not fundamental is the terms of governance within which surveillance is exercised: whether it is extraordinary or has been normalized; whether it is

circumscribed by any predictable law or it is liberalized by discretion and whether the surveillance can detect, deter and cure abuse is the putative question of control.

1.2 The reason why privacy and protection of life must be studied collectively.

This practice of viewing surveillance as a privacy matter is capable of generating an incomplete diagnosis that in certain situations is perilous. Harm to privacy has been characterised as intrusion, humiliation, damage to reputation or chilling effects. These harms have their own significance especially in the fact that the conditions to participate in democracy and exercise other rights are founded on privacy, dignity, and autonomy. Nonetheless, the governance malfunctions permitting criminal or arbitrary surveillance may likewise give portals into greater stakes harms, which involve life and body safety. There are three pathways which are particularly pertinent.

First, surveillance ability has the potential to heighten vulnerabilities referring to persons and organizations who are already brought into being at greater risk like journalists, lawyers, political figures, human rights defenders, witnesses and other discordant voices. The communication and metadata accessed can give information on the location of a person, the people they interact with, the networks they depend on, and the movements they intend to make. The HRC interpretation of the right to life states that states owe due diligence to prevent aggressions that are foreseeable and a special protective care is necessary when the individuals or groups are at a high risk.

Second, protective practices to minimize the risk of violence may be undermined by widespread perception of surveillance. When they suspect that their conversations are being listened to or their records might be disclosed, people fail to report the incidents, consult counsel or arrange their security, or pursue the law. Both Article 17 and Article 6 are concerned with this mechanism. Being a privacy degradation as it is a form of social association by intrusion, be it a life protection degradation since it undermines preventative ecosystems limiting real world threats. The framework a Covenant outlaws not only unlawful but also arbitrary interference which includes acts that may be reasonable in principle, but unreasonable or disproportionate in practice, particularly where protection mechanisms are weak.

Third, in jurisdictions where surveillance is conducted behind closed doors with impunity, it may enhance an overall governance culture with serious transgressions. The right to life carries with it the prevention and responsibility duties whereby states must have institutional structures that are sufficient to probe the abuses and hold them accountable. Non auditable surveillance systems, unclear access policies, and oversight that lacks the ability to require disclosure provide circumstances under which the State can assert its ignorance or inability, and in which victims and even the courts can barely procure evidence. In these cases, the issue of privacy and the issue of life have one institutional cause in common: untrammeled power and structural obscurity.

1.3 Judicial history of Pakistan as a diagnostic tool.

The recent judicial involvement by Pakistan in practices of phone tapping and interception provides an exceptionally diagnostic prism. The courts demanded unearned state guarantees, institution accountability and technical interpretation. It is important since it indicates what can be termed as a rule of law insistence in regards to surveillance governance. Mian Najam us Saqib v. The Islamabad High Court proceedings. An example

of such an attitude is shown by Federation of Pakistan which regards illegitimate interception issues as constitutionally urgent and by forcing institutional actors to consider the legal basis and responsibility. The judicial stance is relevant to this larger argumentative thesis of the paper: in a region where surveillance capabilities are potentially multiplying, the judicial self-assessment in Pakistan offers a rights-based way in which surveillance apparatus can be placed within legal limit, as opposed to viewing it as an exemptive mechanism of security.

1.4 Research question and argument direction.

It is in this context that the article poses the following question: How do the technologies of surveillance and practices of governance in Pakistan contribute to the creation of risk in the face of the ICCPR Articles 6 and 17, and how is the surveillance governance in Pakistan reflected in the best reconciliation with a treaty and constitutional claims with the context of HRC 2024 Concluding Observations.

The main idea of the article is that the biggest challenge facing Pakistan is never merely the expansion of the surveillance capacity, however, the lack of an operationally verifiable governance regime: crossing and expansive mandates, unstable application of warrants of judicial control, inadequate independent supervision, and ineffective development of remedies secures interferences with privacy that are unlawful or capricious and undermines the due diligence and accountability ecosystem needed to authoritatively safeguard lives.

The rest of the article goes ahead to relate international standards and institutional realities in the country. It describes the ICCPR tests applicable to privacy and life first and overlayed on the mapping of the surveillance ecosystem in Pakistan and the legal underpinnings of the same. Then it focuses on the judicial approach of Pakistan as a homegrown interpretive scheme that exposes gaps in governance and simultaneously indicates rights solutions to the same.

Lastly, it suggests revisions that are bringing legality, necessity, and proportionality within the bounds of institutional and technical protections in order that the power to control any type of surveillance, should it be exercised at all, would be limited by statute, subject to external scrutiny, and to be audited, and open to challenge in practice.

2. The surveillance ecosystem of Pakistan and legal foundations.

The surveillance environment of Pakistan can be described as multiple layers of authority as opposed to one law. Many avenues of law reflect telecommunications national security provisions, regime of special surveillance warrants, power to investigate cybercrimes, and licensing requirements which interrelate with technical systems which can centralize or broaden access.

2.1 Constitutional background: dignity, privacy, and liberty.

The Constitution of Pakistan has both overt and inferred privacy and security pillars. Article 14 safeguards the dignity of man and the privacy of the home and long tradition in the Pakistani courts have seen dignity as a core value in constitution. Article 9 (security of person) liberty guarantee has also been given a liberal interpretation in the jurisprudence of Pakistan which allows the courts to consider threats to life and bodily integrity as the right violation even in circumstances of harms due to systemic governance failures.

The constitutional meaning is two-fold. To begin with, every surveillance regime has to be within law and conformant with the fundamental rights. Second, the rights of the constitution do not simply mean of negative restriction (do not intrude), but of maximum structural obligations: to provide the means of a lawful procedure, control and remedies adequate to the safeguard of dignity and freedom.

2.2 Telecom interception powers and the national security powers.

One of the keys facilitating clauses is the Pakistan Telecommunication (Re organization) Act, 1996 which includes the provisions on national security that usually accommodate the use of interception and tracing of calls/messages in general terms. Secondary studies of the telecom regime of Pakistan have continuously criticized the scope of Section 54 and lack of any meaningful protection.

In 2024, government disclosure showing the federal government had given an authorization/notification to a leading intelligence agency to intercept or trace communications under the telecom national security law further caused growing questions on regulation and legality. The 2024 Concluding Observations of the HRC directly mention such an authorization as one of the sets of privacy concerns and use it as an indicator of the growing surveillance authorities with poor protection.

2.3 The Investigation Fair Trial Act (IFTA) 2013: 2013 model of a warrant (not utilized).

The most rights-congruent surveillance system, formally, in Pakistan is the Investigation for Fair Trial Act, 2013 (IFTA) providing a route of judicial warrant to interception/surveillance within the context of planned offences. The architectural design of the statute allowed authorities, ministerial vetting, judicial issue of warrants, and restricted time span is akin to ex ante type of protections which Article 17 jurisprudence requires.

However, litigation to the IHC has indicatively indicated a serious operational loophole: even where a warrant founded model is present, the agencies and regulators might seek corresponding technical or licensing founded interception capacities without resorting to the statutory warrant pathway, or without being capable of stating the legal basis of the capacities.

2.4 The powers of cybercrime legislation (PECA 2016) and the platform governance.

The Prevention of Electronic Crimes Act, 2016 (PECA) of Pakistan gives the power of investigation, offenses, and cooperation responsibilities applicable to the access of data and control of the platform. The HRC recommends PECA as a priority concern in balancing privacy (2024 Observations, specially targeting PECA) in specific attention to the areas that maybe allowing clandestine technology usage and data gathering with an insufficient judicial or other third-party checking (or awareness).

2.5 Technical infrastructures: between telecom interception and so-called surveillance centers.

Infrastructure also determines surveillance risk. Such measures as centralized monitoring technologies and network control practices such as interception / monitoring of the network and more comprehensive controls of digital processes are outlined in the reports providing information on Pakistan's use of these technologies as described by public sources such as a 2025 Amnesty International report.

More to the point of legal scrutiny, the courts of Pakistan themselves have reported the nature and administration issues in LIMS a Lawful Interception Management System allegedly bought and activated under

regulative guidance, which, furthermore, poses the inquiry of who obtained entry, how it functioned, and whether it was being operated lawfully.

The judicial mind of Pakistan: case-based outline and doctrine.

This part gives the subject matter needed by the "Pakistan judicial mind," the topic, what Pakistani courts have stated regarding surveillance and privacy as well as other rights in relation to them, and what tests arise before the law.

4.1 The basis of the Supreme Court: Mohtarma Benazir Bhutto (PLD 1998 SC 388).

One of the background cases which form the basis of surveillance and privacy in Pakistan is Mohtarma Benazir Bhutto and others v. Others (PLD 1998 SC 388), including the president of Pakistan, have often referred to the principle that the phone tapping and surveillance involves dignity and privacy and has to be performed legally and with protection. The case is important in two aspects. It did not consider privacy violations as some minor procedural issues but as a constitutional wrong. Second, it highlights the fact that constitutional protection cannot be displaced because of an executive convenience.

Even in what subsequently came to be regulated by statute, Benazir Bhutto acts as a constitutional corrective that interception is exceptional and must be justified, a theme subsequently taken to the IHC infrequently.

4.2 Islamabad High Court W.P. No. 1805/2023: unlawful phone interception, privilege and incapability of the state.

It is presented by the IHC in W.P. No. 1805/2023, which attempts to address allegations that private phone availability had been recorded and leaked unlawfully and that such acts threatened intimidation and blackmail committed by the IHC. Prior to appearing before the Court, the Attorney General indicated that no agency had been given the mandate to monitor or record telephone conversations or conduct surveillance under the telecom act or any other legislation, indicated privacy rights of the citizens, and indicated that such communications could be covered under attorney-client privilege.

Three indicators of judicial mindset come to the fore:

Surveillance as a constitutional crisis and not as a criminal investigation. The Court presented the case in such a way that it concerned the duty of the State with regard to entitlement to basic rights, such as privacy and dignity.

Catering to the legal authority and explanation. The Court asked the telecom regulator about what legal and regulatory framework could support the provisions of lawful intercept in licenses when no agency was authorized.

Responsibility of the stories of incapacity. The Court considered claims that the State was incapable of detecting those perpetrators or illegal surveillance as shocking to the Court, as incapacity that of the State in itself is unconstitutional.

This position is significant to the analysis of the ICCPR in that it is Article 17, which asserts the need to prevent unlawful interference effectively, and Article 6, which mandates the use of due diligence to combat foreseeable threats such as threats to life that arise where leaks in surveillance allow targets to be identified.

4.3 W.p. No. 2758/2023 The Islamabad high court Order (25.06.2024): LIMS, illegality, and misrepresentation of the regulator.

It should be highlighted that one of the most legally significant judicial interactions between modern interception infrastructure and Pakistan occurs through the 25 June 2024 order in the W.P. No. 2758/2023 case of the IHC. The Court outlined the underlying thing as the claims of unlawful surveillance and interception of personal phone calls as a means of intimidation and creation of charges.

The order then passed the abstract rights: it asked the questions of the government of a system itself. The Court expressed a preliminary opinion that installation and use of the Lawful Interception Management System was prima facie, and not under the law, instructed telecom licensees to make certain that LIMS did not access networks, and said that allowing access to networks contrary to constitutional guarantees and various laws would make telecom leadership criminally liable.

Above all, the Court also created a preliminary opinion that the Chairman and Members of the PTA lied regarding the existence of the LIMS, served show cause notices, and required a separate sealed reporting to the court concerning the operation of the system and its access, storage, retrieval, and destruction as well as a technical graphic depiction.

In theory, this is a legal action towards the direction of technical legality: legality cannot exist by calling a statute a statute; it must have traceable authority, must be controlled in its access, must be audit and must be shown to have safeguards. This is in relation to HRC expectations that the surveillance should be controlled with independent checks and balances, judicial sanction and responsibility.

4.4 Systemic risk, life, and dignity wider approach to the constitution.

In addition to the special cases of surveillance, the jurisprudence in Pakistan has interpreted the right to life so widely in terms of quality of life and the dimension of security as well. For example, Shehla Zia v. WAPDA (PLD 1994 SC 693) is extensively referred to as having broad conceptions of what life means, in the spirit of the intuition that such state policies which clearly puts individuals in grave dangers may contravene Article 9.

This is important since there are usually systemic risks that are created by surveillance governance that creates chilliness when the opposition is sought, the result of which can be intimidation, hence vulnerability of journalists/human rights defenders and not one-time evils. Preventative judicial interventions, rather than post hoc punishment can be sustained on the constitutional frame.

5. Article 17, ICPR: privacy and the non-arbitrariness test.

Article 17 safeguards against arbitrary or unreasonable interception of privacy as well as family, home and correspondence. As explained by the HRC in General Comment No. 16, even the interference that is within the law could be arbitrary in case it is unreasonable, disproportionate, or one that does not include sufficient safeguards.

5.1 Legality: visibility, openness and boundary.

Nothing is illegal unless the surveillance authorities are published, sufficiently specific, and limited to the extent that people can predict when and where the intrusion of the state can happen. The problem in Pakistan is not that there is no legal text, but rather there are general authorizations (in national security framing, in particular)

as well as shadowy operational processes (license-based intercept, centralized systems) which are not even transparently regulated.

Those cases of the 2023-2024 of the IHC point to a practical gap in the legality: government saying that no agency has power to intercept, but telecom licenses mandate the presence of lawful intercept, and systems such as LIMS are available, then the legality is simply incoherent.

5.2 Necessity and proportionality: the default of surveillance problem.

Article 17 imposes necessity and proportionality to surveillance, even where the purpose is legitimate (national security, crime prevention): use of surveillance must be too specific (preferably), preferably must be limited in existence, and any intrusion must not exceed what is necessary.

The HRC 2024 Concluding Observations are indicative of worry regarding the magnitude and secrecy of surveillance connected policies in Pakistan. The Committee raised the issue of mass surveillance and telecom/data monitoring which involved PECA-related measures, firewall proposals and authorizations that permitted interception. It had advised that Pakistan should make such a surveillance within legal, necessary, and proportionate limits and should be controlled by a check of third parties and remedial means.

5.3 Safeguards E. judicial authority, inspection, transparency, redress.

In HRC doctrine, protective measures are not perfumatory they are the ones that transform potentially lawful intrusions into practices that are rights compatible. Safeguards usually include:

- Ex ante independent warrant (preferably judicial warrant), with specified reason and period;
- Interdependent (parliamentary, judicial, or independent specialized body) access to information;
- Openness (at any rate, aggregate reporting, transparent legal standards, notification in any case);
- Remedy (capacity to contest surveillance and get redress).

The IFTA of Pakistan provides a warrant model yet the IHC proceedings indicate that the culture of operational surveillance can circumvent the warrant practices.

ICCPR Article 6: surveillance in the context of protection of life.

On the surface, the two articles tend to appear different (privacy, Article 17, and life, Article 6). The interpretation of Article 6 given by the HRC, however, regards the right to life as covered by positive obligations to safeguard against threats which are foreseeable, and to establish legal structures against unlawful interference with the right to life.

Pathways between surveillance and life risk 6.1.

Surveillance has the capability of implicating protections in life in a number of pathways:

Web attack and vulnerability generation. Location, networks and routines of human rights defenders, journalists, political actors, and witness groups are also much at risk, which can be recognized through surveillance and metadata access. General Comment No. 36 also highlights the special safeguard of the people who are at risk due to a particular threat such as defenders and journalists.

Chilling impacts that cripple safeguarding. In such situations where surveillance generates the fear of reporting, organizing, or accessing legal assistance, the effect of surveillance on the protective ecosystem that safeguards against violence and rights abuse may be detrimental.

Impunity atmosphere and forcible disappearance. In the case where surveillance systems are non-transparent and non-monitored, they will add to an environment of enabling disappearance practices through enhancing state capacity to locate/ monitor the targets without imposing similar accountability.

6.2 2024 Concluding Observations of the HRC: disappearances as a life issue (and a surveillance governance mirror).

The 2024 Concluding Observations of HRC audibly indicates the concern over the compelled disappearances and inefficiency of monitoring accountability. Articles 6, 7, 9, and 14 are typically applied to disappearances, but this category of governance is inseparably connected not only to secrecy, absence of control but also to insufficient remedies. Both issues that the Committee simultaneously addresses are mass surveillance and disappearances, this means that a diagnosis on governance: in case the coercive state capabilities extend without the checks they are weak in defending privacy and life.

Article 6: prevention, investigation, and accountability 6.3 Due diligence.

In the context of surveillance, General Comment No. 36 stipulates that the states should establish institutions and procedures to prevent deprivation of life, investigate the possible cases, prosecute and restore.

In this case, this means:

- avert illicit operations and breach of data which poses threats;
- researching on illegal interception and leaks successfully (not accepting incapacity);
- restricting the power of the intelligence and law enforcement to a legal level;
- empowering remedies and safeguards of the victims.

This due diligence logic is reflected in the insistance of the IHC in phone tapping litigation that required a strict and searching scrutiny, which puts state incapacity narratives in an unacceptable constitutional light.

Risk reassessment of Pakistan following the 2024 observations of the HRC.

This part summarizes the article 17 and Article 6 review into a risk review consistent with the HRC 2024 results.

7.1 Risk under Article 17: normal intrusions and weak protection.

Risk drivers

- General national security-wide interception rights and ambigious scope;
- Licensing and technical designs that permit entry with no legal control;
- Without severe judicial approval that is applicable to PECA interconnected information is used to command and manage platforms;

Cloudy systems such as LIMS with contentious governance, access and auditability.

Risk consequences

- Routine violation of correspondence and communications privacy;
- Too broad and has an insufficient protection;
- Coupling to the expression and association, which makes one even more vulnerable.

These issues are directly merged within the closing observation of the HRC 2024 recommending that legality/necessity/proportionality, independent oversight and remedies be adhered to.

7.2 Article 6: risk collapse through enabling environment and accountability: failure.

Risk drivers

- Hierarchy, lax control over coercive power;
- Hackers should not be completely investigated in terms of the existence of illegal surveillance or leaks (or denial-based regulation);
- Continuous trends of enforced disappearance and the lack of accountability (NGO warning signs).

Risk consequences

- Heightened susceptibility of target populations;
- Lower capability to preclude or retaliate against threats;
- Impunity cycles: These loot life.

In this case the HRC 2024 final remarks regarding disappearances and accountability overlap its surveillance issues: they represent failures in governance through constraints and oversight.

Reform agenda: streamlining the surveillance governance in Pakistan with Articles 6 and 17.

The reform should be both institutionally realistic and legally precise. The most vital direction to be taken has been already described by the courts of Pakistan particularly the IHC of legality, warrants, accountability and technical transparency.

8.1 Re revoke the default of judicial warrant.

Pakistan must view warrant-based interception under IFTA as being the default rule, and strictly constrain any provision on national security-based interception by incorporating:

- specific grounds;
- individualized targeting (except in defined cases of emergencies);
- time restriction and renewals;
- minimization rules (collection / retention limits);
- ex post analysis and notice where possible.

This is in line with Article 17 protections and in line with the IHC focus that surveillance should be done within the confines of the fair trial act with due regard to the state legitimate reasons.

8.2 Independency and technical auditing.

The oversight should be effective: logs of the system, acquisition agreements, lists of access controls, investigation capacity. The IHC requirement of a graphic presentation of the LIMS operation, and comprehensive reporting of storage/retrieval/destruction, should be made into a requirement of the compliance rather than a special court action.

8.3 Obligations of the telecom licenses which are subjected to the law.

There must be a legal foundation towards telecom lawful intercept requirements in licenses: licenses must not form a shadow law of surveillance. In the situation when the regulator is unable to substantiate the powers of interception obligation, legal reform should align the requirements of the license with the constitutional and statutory warrant provisions. The fact that the IHC is interrogating the failure by PTA to furnish a reasonable legal response is to be considered a red flag to the system.

8.4 Powerful remedies: the rules on standing, notification and evidence.

Article 17 should have a purpose and to do this it would require that people should have an opportunity to contest lawless surveillance. Reforms should include:

- clear standing rules (along with secrecy blocking proof by public interest petitions);
- post surveillance notification in which the same will not put in jeopardy legitimate investigations;
- suppression/exclusion principles on which the surveillance evidence is unlawfully acquired;
- monetary and organizational responsibility.

Article 6, 8.5 integration: protection tasks on at risk groups.

General Comment No. 36 is applicable in the present case by providing targeted action to the persons in danger (journalist, defenders, and witnesses). These measures include fast protective measures, serious investigation of threats and restrictions on surveillance practices that reveal the location or networks of the target.

8.6 Transparency and reporting

Pakistan must issue periodic disclosure reports on:

- number of warrants requested/acquired (aggregate);
- types of crime and incarceration periods;
- emergency intercept uses;
- oversight findings;
- complaints and remedies.

This is a direct reaction to the focus of such oversight and remedies that the HRC has, and it enhances the trust of people.

Conclusion

Surveillance is not merely a technological proliferation issue as in Pakistan, but it is self-governance. The HRC 2024 Concluding Observations recognize the privacy risks associated with mass surveillance and laws against cybercrime and restate some brutal concerns around the enforced disappearance and accountability practices that include implications on the right to life. The constitutional course of the Pakistani judiciary, particularly, via the 2023-2024 illegal phone tapping and LIMS proceedings in the IHC in its articulation has reflected a constitutional direction i.e., in the knowledge and implementation of surveillance, should be grounded on a legally expansive or narrow, independent oversight and technologically auditable, with actual remedy.

A reevaluation of privacy and life protections will both explain what is on the line, as invasion without protections may become a direct facilitator of intimidation and targeting, and it will also play a role in the impunity atmosphere of life-threatening abuses. There is a rights compatible way to go however this will entail abandoning secrecy-based capability building in favor of rule of law-based capability governance where legality is not aspirational but a reality that can be audited.

Bibliography

Amnesty International. *Shadows of Control: Pakistan's Mass Surveillance and Digital Repression*. 2025.
ARTICLE 19. *Review of Pakistan Telecommunications (Re organization) Act*. 2012.
Asian Development Bank. *Shehla Zia v. WAPDA (PLD 1994 SC 693)*. Case compilation/summary.
Constitution of the Islamic Republic of Pakistan. Article 14.
Human Rights Committee. *Concluding Observations on the Second Periodic Report of Pakistan*. CCPR/C/PAK/CO/2. 7 November 2024.
Human Rights Committee. *General Comment No. 16: Article 17 (Right to Privacy)*. 1988.
Human Rights Committee. *General Comment No. 36: Article 6 (Right to Life)*. CCPR/C/GC/36. 3 September 2019.
Islamabad High Court. *Mian Najam us Saqib v. Federation of Pakistan*. W.P. No. 1805/2023. Order Sheet, 20 December 2023.
Islamabad High Court. *Bushra Imran Khan v. Federation of Pakistan*. W.P. No. 2758/2023. Order dated 25 June 2024.
Mohtarma Benazir Bhutto and Others v. President of Pakistan and Others. PLD 1998 SC 388.
Dawn. "Govt allows ISI to intercept phone calls, messages." July 2024.
The Prevention of Electronic Crimes Act, 2016 (Pakistan). PDF compilation (Sindh Judicial Academy repository).
Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)* (1988).
Human Rights Committee, *Concluding Observations on the Second Periodic Report of Pakistan*, CCPR/C/PAK/CO/2 (7 November 2024), paras. 44–45, 24–25.
Human Rights Committee, *General Comment No. 36: Article 6 (Right to Life)*, CCPR/C/GC/36 (3 September 2019), paras. 22–27.
Human Rights Committee, *General Comment No. 36: Article 6 (Right to Life)*, CCPR/C/GC/36 (3 September 2019), paras. 22–27.
Islamabad High Court, W.P. No. 1805/2023, *Mian Najam-us-Saqib v. Federation of Pakistan*, Order Sheet (20 December 2023).
Constitution of the Islamic Republic of Pakistan, art. 14.
Asian Development Bank, *Shehla Zia v. WAPDA* (PLD 1994 SC 693) (case summary/compilation).
ARTICLE 19, *Review of Pakistan Telecommunications (Re-organization) Act* (2012), 15–16 (discussion of interception powers and safeguards).
"Govt allows ISI to intercept phone calls, messages," *Dawn*, July 2024.
Human Rights Committee, *Concluding Observations on Pakistan*, CCPR/C/PAK/CO/2, para. 44 (privacy and surveillance concerns), para. 45 (recommendations).
The Prevention of Electronic Crimes Act, 2016 (Pakistan), as compiled in Sindh Judicial Academy PDF repository.
Mohtarma Benazir Bhutto and Others v. President of Pakistan and Others, PLD 1998 SC 388.
Islamabad High Court, W.P. No. 1805/2023, Order Sheet (20 December 2023), para. 1 (Attorney General's statement).

Islamabad High Court, W.P. No. 2758/2023, Order dated 25 June 2024, pp. 1–2 (foundational issue and framed questions).
Asian Development Bank, *Shehla Zia v. WAPDA*, PLD 1994 SC 693.
Human Rights Committee, *General Comment No. 16*, para. 4 (unlawful/arbitrary interference).
CYRILLA, *Investigation for Fair Trial Act, 2013* (warrant provisions overview).
Human Rights Committee, *General Comment No. 36*, paras. 22–24.
Human Rights Committee, *Concluding Observations on Pakistan*, paras. 24–25 (enforced disappearances concerns).
Islamabad High Court, W.P. No. 1805/2023, para. 9 (strict scrutiny; state duty framing).