Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 12, 2025

ARTIFICIAL INTELLIGENCE AND DATA PRIVACY: A CONSTITUTIONAL PERSPECTIVE

Erum Iftikhar

Faculty of Law, University, of Karachi, Karachi Sindh, Pakistan

DOI: https://doi.org/10.5281/zenodo.18058687

Keywords
Artificial Intelligence (AI), Data Privacy, Constitutional Law, Pakistan, Algorithmic Surveillance, Proportionality Test, Right to Dignity, Comparative Law, GDPR, Safe City Project, Algorithmic Governance.

Article History
Received: 28 October 2025
Accepted: 12 December 2025
Published: 26 December 2025

Copyright @Author
Corresponding Author: *
Erum Iftikhar

Abstract

The introduction of state-controlled Artificial Intelligence (AI) and surveillance technologies into Pakistan, best exemplified by biometric databases and predictive policing systems such as the Punjab Safe City Project, presents a threat to the constitutional fundamental rights as never seen before. This paper demonstrates that the current constitutional and legislative system in place in Pakistan is urgently inadequate to regulate AI, which constitutes an algorithmic surveillance regime that functions in a vacuum of doctrines. Article 14 of the Constitution provides that the dignity and privacy should be inviolable, but the subject of law provision and the reactive and permissive approach of the statutes such as the Prevention of Electronic Crimes Act (PECA) 2016 make it possible to collect and profile mass data without the required protection of proportionality, transparency, and due process.

This study applies a doctrinal and comparative legal methodology and firstly, it diagnoses this constitutional gap by examining Pakistani jurisprudence on surveillance. It subsequently conducts a critical comparative analysis based on the transferable lessons acquired through the regulatory approach of the European Union based on rights (GDPR), fundamental rights jurisprudence in India (K.S. Puttaswamy), and the volumetric approach to digital privacy in the United States (Carpenter). The thesis argument is that in order to balance AI innovation and constitutional faithfulness, Pakistan should take a two-pronged approach of judicial reinterpretation and strong legislative change.

The main contribution made by paper is the proposal of a customized, justiciable, Algorithms Surveillance Test of Pakistani courts, which is based on a rigorous proportionality criterion (legality, legitimate aim, necessity, and balancing). This is a test which would give the doctrinal instrument to examine projects such as Safe Cities. Simultaneously, it states that the upcoming Personal Data Protection Bill should be supplemented with Compulsory Algorithmic Impact Assessments (AIAs), compulsory transparency and explainability conditions and an entirely independent National Commission with robust audit and sanction capabilities. Finally, the study can offer a real-life constitutional roadmap to Pakistan, and other jurisdictions in the Global South to go beyond a state of unregulated algorithmic governance to a state of responsible, rights-sensitive algorithmic regulation.

INTRODUCTION

The development of Artificial Intelligence and AI technologies in Pakistan, especially the field of state security and administrative services, is a critical threat to the constitutional rights, in particular, the right to privacy and dignity. Pakistan is actively implementing advanced AI technologies, such as provincial projects such as the Punjab Safe City project, which implements the Face Trace System (FTS) and Automated Number Plate Recognition (ANPR), which are AI-based technologies used to identify and track criminals (Lubna et al., 2021). Such deployments are requiring the systematic gathering, handling, and storage of enormous amounts of personal information that fundamentally changes the character of state surveillance as a method of targeted interception to non-consensual mass profiling (Hyder et al., 2025).

This fast changing of technology has left a vacuum in the constitution. Although the Constitution of Pakistan provides inviolability of human dignity and privacy of the home (Government of Pakistan, 1973), as far as the law permits, the Constitution of Pakistan is still in its early phases of interpretation and application in the digital world. Without a fully-fledged data protection legal framework, state agencies and other organizations will be left without binding restrictions concerning data processing, and constitutional protection of these privacy rights remains merely an ideal but not a binding priority (Sohail, 2025). The existing legal framework cannot be used to regulate informational flows thus permitting AI systems to violate the basic rights in a manner that classical jurisprudence never expected (DLA PIPER, 2025b). The report aims to fill the gap between the historical constitutional doctrine of Pakistan, which has traditionally been premised on the physical intrusion, and the contemporary need to safeguard the informational privacy and assure the fairness of the algorithms.

The study falls in the context of the scholarly discussion of algorithmic governance, constitutional law and Global South development policy. It is motivated by four overall research questions as follows: First, does the constitutional framework (text and jurisprudence) of Pakistan provide sufficient protection against AI-enabled data processing and algorithmic surveillance of privacy? Second, are there any legal loopholes in the statutory law and institutional capability to regulate the privacy effects of AI in Pakistan? Third, how have other jurisdictions balanced constitutional privacy rights and AI and what can be transferred to Pakistan? Lastly, what particular legislative, judicial, and administrative policies does Pakistan need to implement in order to ensure privacy and achieve legal AI innovation?

The main aim is to chart out the current constitutional and statutory safeguards and examine such doctrines of law as proportionality, due process, and transparency in the context of AI and data processing. Comparing foreign examples, namely the rights-based framework of the GDPR of the EU and the constitutional Puttaswamy jurisprudence of India (Afzal and Ghawaas, 2025, Mustafa, 2015, Dwivedi, 2021), the study shall seek to come up with practical, practical recommendations on creating a constitutional interpretation, legislation, and regulation design that suits the Pakistani context.

1.2 Overview and Expected contribution of the methodology

The approach uses a mixed-methodology with the focus on the doctrinal legal analysis. This includes textual and purpose interpretation of the Constitution (Article 14) and interpretation of the applicable statutes and case law (e.g. Supreme and High Court decisions on surveillance and the terms of PECA 2016 and the draft PDPB 2023) (Ahmed, 2022, Yousaf Amanat & Associates, 2025, MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023). This conceptual backbone is supported with a comparative legal study of some jurisdictions to draw the regulatory best practices and doctrinal instruments applicable in the legal system of Pakistan (Hecht-Felella, 2021).

The expected value of this research is the provision of the first unified doctrinal and comparative study in the specific case of the constitutional challenge of AI in Pakistan. More importantly, the analysis suggests a customized constitutional Algorithmic Surveillance Test based on the jurisprudence of Pakistan with the view of going beyond high-level

policy suggestions to tangible legislative templates and institutional design proposals that can be feasible and operational within the present governance framework of Pakistan (Jamil et al., 2025).

2. AI Harms and Governance Principles

2.1 Defining AI-Enabled Privacy Harms

Artificial intelligence radically changes the dynamic between the citizen and the state/corporation by changing the process of data gathering into data generation and predictive profiling. The privacy threat of AI is not limited to the loss of control over a certain piece of information; it is spread on both structural and societal damages that cannot be reduced through the use of personal data rights. These dangers involve the risk of increased surveillance, the secondary application of data, and the risk of increased identification that may be achieved through the combination of disparate data sets (King and Meinhardt, 2024).

AI systems allow complex profiling of the user that may result in uneven access to key opportunities, including employment, housing, credit, and education (King and Meinhardt, 2024). In their application in the state sector, e.g. in predictive policing or welfare targeting, the systems can perpetuate existing social inequalities by introducing algorithmic bias based on missing or historical trainings data (Hyder et al., 2025, Qayyum et al., 2025, Kerry, 2020). This institutionalized discrimination of these vulnerable groups such as people of color or religious minorities is not merely a violation of privacy but a profound violation of equality rights (Kerry, 2020).

The constitutional safeguard of the *"dignity of man"* in Article 14 (Government of Pakistan, 1973) in the case must, here, be understood to encompass the right to informational self-determination. The capability of AI to keep track of behavior, predict it and even possibly manipulate it due to extensive data sets is directly a threat to the autonomy part of human dignity. In such a way, AI is not supposed to be a threat to privacy, but a multi-right violating engine, i.e. it is not merely violating privacy. Art/14) and possibly also the freedom of movement and association (Arts. 15, 17), and equality (Art. 25) (Chaudhry, 2025).

2.2 Basic principles of Constitutional Data Protection

The constitutional data protection requires the adherence to the principles that limit the processing power of the states and corporations. The fundamental requirements are the lawfulness and restriction of purpose, i.e. data collection must be explicitly defined in the law and strictly limited to the mentioned purpose. Modern AI systems directly conflict with this idea, as they operate on data merging and with the non-consensual second usage of data many times over its original intent of gathering (Mühlhoff and Ruschemeier, 2025).

Moreover, the concept of data minimization, which assumes that the collected and stored amount of data must be no more than is necessary according to its purpose, and data quality are fundamental principles that have become a common standard in the world, especially in such regulations as the GDPR of the EU (Jhokio and Rehman, 2025) and the DPDP Act of India (Usha and Neeral, 2025). To apply these principles to the large-scale state AI systems, including facial recognition databases, we need to break down the operational belief that more data is better to include high standards of necessity assessment.

2.3 Theory of Algorithmic Governance

One of the key concerns of AI regulation is the issue of opacity that is also known as the black box problem. When complex algorithmic systems are used to make decisions in government or the private sector, the nature of decision-making process becomes veiled hence the citizenry and regulators cannot know how the decision was arrived at (Katzenbach and Ulbricht, 2019). This obscurity is immediately converted into a constitutional deficit, the Process Integrity Test, the right to hear, to submit evidence, and to receive a reasoned decision (Afzal and Ghawaas, 2025). When a person is unable to identify how an automated system refused to provide him/her a service or label him/her as a suspect, he is essentially denied a significant constitutional due process and redress systems (Livermore, 2025).

The theory of algorithmic governance points out that the loss of the natural democratic friction (the resistance to change and conflict between human

authorities) is inevitable when a human form of rule is substituted by automated systems (Livermore, 2025). This may create an atmosphere of algocracy, the rule of algorithm, in which citizens who are offended are powerless since the mechanisms are fully automated in ways that do not ensure any transparency and accountability. To overcome this lack of accountability, the legal systems should enforce transparency processes which will enable and permit independent examination, auditing and evaluation of the automated systems (Reisman et al., 2018). This is aimed at making sure that AI systems are implemented in a transparent, responsible, and ethical way that strengthens, and does not undermine, fundamental rights (Cheong, 2024).

3. Statutory Data Protection Framework

3.1 Article 14 and Interpretation of the Right to Privacy and Dignity

In Pakistan, the constitutional basis of privacy is based on the first being Article 14(1) of the Constitution, 1973 (Government of Pakistan, 1973). According to this provision, the dignity of man, and, within the law, the privacy of home, shall be sacred. The focus on dignity is also essential, which offers a normative foundation that the understanding of privacy is an indispensable element of individual autonomy.

The Pakistani higher courts have in the past extended the application of this right past the physical aspects of the "home" to the national borders themselves. The rulings of Mohtarma Benazir Bhutto Case brought about the fact that unlawful and indiscriminate surveillance, such as telephone tapping and eavesdropping, is illegal, unconstitutional and immoral and infringes upon the right to life (Ahmed, 2022). This jurisprudence became a good precedent concerning the impossibility of government intrusion and mass monitoring in the absence of specific data protection laws. More recently, the inviolability of mobile phone data has been identified by the courts that state that the extraction of such data without due process may constitute self-incrimination, which strengthens the safeguarding of digital contents (Aftab, 2024). These cases create a strict constitutional guideline of judicial limitation of state surveillance that is by theory applicable to contemporary algorithmic surveillance.

3.2 The Analysis of the Subject to Law Clause

The strength of Article 14 is considerably limited by the fact that the inviolability of the privacy of the home is restricted by the law (Government of Pakistan, 1973). This provision means that the legislature still has much power to pass laws which either define, restrict or control privacy. Any act which is undertaken under a duly passed Parliament law, even that which is harmful to digital privacy, possesses constitutional force, unless the law itself is successfully attacked as being manifestly arbitrary, unreasonable or unjustified under a bona fide state purpose (Aftab, 2024, Sohail, 2025).

The implication of such wording, along with the failure of law to act upon enacting an all-encompassing law on data protection is harsh: without a clear, substantial law on privacy, the surveillance culture remains under-regulated. Such a legislative loophole allows a wide interpretation of criminal and security laws by the executive or the agency through which the AI is implemented, so that AI uses that sometimes occupies a gray zone can have just too little restraint in relation to the rights of citizens (Sohail, 2025).

3.3 Statutory Instruments and Surveillance Power

Lacking a more all-inclusive law on data protection, the Prevention of Electronic Crimes Act (PECA), 2016 has been the main, though extremely controversial, statutory tool that has touched upon the digital rights (DLA PIPER, 2025b). PECA 2016 is essentially a law of cybercrime, which pays attention to the reactive retributions of the offence like hacking, cyberstalking, cyber terrorism, and electronic fraud (Arshad Khan, 2018). It does not strive to be a protection data regulation framework (Yousaf Amanat & Associates, 2025).

Although PECA indirectly addresses data confidentiality (Section 41 provides that confidentiality unless a legal obligation is established or consent given (Khan, 2025)) it has deep flaws in comparison to the international privacy principles:

Reactive Focus: It refers to the violation of breaches after they have occurred instead of proactive

standards on how data should be handled (Yousaf Amanat & Associates, 2025).

No Individual Rights: It does not provide the citizenry with clear rights to their personal data, including the right to access, amend, or demand their deletion (Yousaf Amanat & Associates, 2025).

Extensive Surveillance Authorities: PECA, in combination with telecoms regulations, allows extensive data collection, data retention policies (Jamil et al., 2025), and state surveillance technologies, including fiber optic cable tapping technologies and Lawful Intercept Management Systems (LIMS) (Ahmed, 2022). This condition is such that AI systems may be implemented in order to support the operations of mass surveillance without a solid constitutional need and proportionality control (Amnesty International, 2025).

This structural paradox is the formation of a regulatory paradox: the state strictly punishes unjustified access and theft of data by a person and is excluded by PECA, but the broad authorization provisions of the same or other laws may allow and even authorize a mass access by the state without any equal check, and proves the unequal protection of digital rights (Khan, 2025).

3.4 Prospects for Reform

The proposed Personal Data Protection Bill (2023) is a significant effort of the Ministry of Information and Technology and Telecommunications to seal the gaps in regulations (DLA PIPER, 2025b). The Draft Bill includes some of the basic concepts of data protection, such as principles of consent, data processing, notification of data breach, cross-border data transfer and is rather clearly charged with the responsibility of encouraging adherence to international standards (Khan and Khan, 2025, MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023).

The PDPB offers the creation of the National Commission of Personal Data Protection (NCPDP). Notably, the draft specifically covers the algorithmic processing, giving the data subject the right to object to decisions exclusive to automated processing such as profiling, which have an immense impact on them (Section 29). The NCPDP is suitably charged with the role of encouraging and governing this automated processing (MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023).

Although it compares to other international frameworks, such as the GDPR and CCPA, critics have argued that the PDPB could still be biased in favor of state interests to the detriment of citizens, potentially legalizing the mass surveillance practices formerly held unconstitutional by the courts (Amin and Hassan, 2024). Unless the PDPB, as it may look, is very liberal in its treatment of the Federal Government or security agencies (which is not uncommon in regional bills), the statutory reform will encapsulate constitutional infractions in the form of indiscriminate data processing under article 14's subject to law clause (PRS Legislative Research, 2023, Kalyar, 2021). The achievement of the PDPB will entirely depend on the scope of the final text on the exemptions of the states and the actual independence of the NCPDP (Kalyar, 2021, PRS Legislative Research, 2023).

3.5 Gaps to Institutional Capacity and Enforcement

The shift in the model toward a purely punitive one (PECA enforcement through FIA) and a full-scale regulatory and preventive model (PDPB enforcement through NCPDP) has considerable institutional issues (MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023). The suggested NCPDP should be turned into a statutory corporate authority that will have both operational and administrative independence. It has a critical role to play in terms of guaranteeing strong technical management of algorithmic systems through its composition which necessitates specialists in ICT/cybersecurity, law, policy, and civil society. But the ability to enforce and the political autonomy required to audit and punish influential actors in a state or large corporations is the main issue. The accomplished provisions of the PDPB regarding automated processing rights cannot be implemented without proper resources and political autonomy. The current legal environment can be listed as shown in the following table:

Table 1 Inventory of Pakistan's Statutory and Regulatory Instruments Impacting Data Privacy

Instrument	Constitutional or Legal Scope	Primary Function and Application	AI/Privacy Gap Identified	Source
Constitution (Art. 14)	Fundamental Right	Dignity and Privacy of Home; judicially expanded to cover digital communications and dignity.	Right is "subject to law," creating a legal loophole that broad statutes can exploit for surveillance.	(MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023)
PECA 2016	Statutory Law (Cybercrime)	Combating electronic crimes, regulating digital space, enabling certain data access/interception powers.	Reactive focus; lacks proactive individual rights, consent mechanisms, or specific AI governance obligations.	(Ahmed, 2022, Yousaf Amanat & Associates, 2025)
PDPB 2023 (Draft)	Regulatory Bill	Comprehensive data protection framework; proposed creation of NCPDP.	Status pending; potential state exemptions; lack of mandated algorithmic transparency and audit powers against state actors compared to international standards.	(Kalyar, 2021)
Telecom Laws / NADRA Ordinances	Sectoral Regulation	Data retention, biometric collection, and lawful interception requirements.	Facilitate mass data collection by state/private actors without robust independent oversight or necessity tests.	(Arshad Khan, 2018)

4. Constitutional Comparative Approaches

The flaws of the existing statutory framework of Pakistan warrant an analysis of how other jurisdictions, especially those that have a similar constitutional framework or have more developed digital economies have limited the power of algorithms.

4.1 The European Union Model

The General Data Protection Regulation (GDPR) of the European Union provides the international

standard of privacy regulations with a set of fundamental principles that are reflected in the EU Charter of Fundamental Rights. It represents the rights-based strategy with the focus on the individual control and high regulatory monitoring (Taylor-Hiscock, 2025, intersoft consulting, 2025).

Substantive Rights/Algorithmic Controls: The GDPR offers the rights which are specific and limited and which are direct counterparts of the algorithmic domination. Of paramount importance is the right of Data subjects in the Articles 22, that they have the right to object to decisions of automated processing including profiling whose results have legal consequences or whose impacts are otherwise of considerable effect on them. The other vital mechanisms are the right to restriction of processing, the right to erasure (right to be forgotten) and the right to the data portability (Taylor-Hiscock, 2025, intersoft consulting, 2025).

Regulatory Instruments: GDPR requires the creation of autonomous supervisory bodies (Data Protection Authority or DPAs) that have strong powers of investigation, enforcement, and imposing enormous financial fines in case of violation. Moreover, it entrenches procedural protective measures like the compulsory Data Protection Impact Assessments (DPIAs) of the high-risk processing activities. The ability of DPA to audit and issue binding orders is crucial to implementing the data protection principles on the mighty controllers, even deploying AI (Taylor-Hiscock, 2025, intersoft consulting, 2025).

4.2 The Indian Model: Fundamental Right and Proportionality

Pakistan has the Indian model that is most relevant in terms of the constitution because of the similarities in legal background and common development processes.

Puttaswamy Jurisprudence: Supreme Court decision in 2017 of K.S. Puttaswamy v. the Union of India was a landmark, in which the right to privacy has been unanimously identified as a fundamental right, constitutionally guaranteed right, inalienable to the right to life and personal liberty (Article 21). This decision made informational privacy constitutional, which has become a powerful doctrine to oppose mass surveillance and data collection efforts carried out by the states (Supreme Court Observer, 2025, Global Freedom of Expression, 2018).

The Proportionality Test: It is important to note that Puttaswamy provided a test that ensures that the right to privacy is not an absolute precept, but that a state action that violates the right to privacy must meet a strict test with four parts: (1) the lawful character of the act (i.e., it has a legal basis); (2) the existence of a legitimate state goal; (3) the reasonableness of the action (i.e. less obtrusive alternatives are possible); and (4) the proportionality of the action to the aim of the This standard of proportionality is vital since it compels the state to explain why surveillance must be conducted against a democratic principle, and goes beyond the fact of the existence of the law (Supreme Court Observer, 2025, Global Freedom of Expression, 2018, Dwivedi, 2021).

Digital Personal Data Protection (DPDP) Act 2023: The Indian DPDP Act that has been recently enacted is the continuation of this standard of the constitution. It puts in place high accountability and transparency responsibilities. Interestingly, the Act provides the Consent Managers, which are interoperable platforms operated by third parties where users can provide, revoke, or review consent. Bringing in this new Consent Manager idea, which enhances the right to revoke the consent (a primary principle of GDPR), would have a profound positive effect on the user control measures of the local PDPB draft in Pakistan (Supreme Court Observer, 2025, Global Freedom of Expression, 2018, Dwivedi, 2021).

4.3 The American Model: Sectoral Regulation and the Fourth Amendment

The United States follows a very different way with an intricate mosaic of sectoral federal and state legislations (e.g., HIPAA, state regulations such as CCPA) that does not have a single, broad federal legislation (Squire Patton Boggs, 2025, DLA PIPER, 2025a).

Adaptation by the judiciary: Surveillance protection is guaranteed in the constitution under the fourth amendment, which does not allow needless search and seizure. In Carpenter v. United States (2018), the Supreme Court decided that seven days of information on the location of cells are a search and

thus ought to be covered by a warrant. Such jurisprudence is very applicable as it defined a volumetric method over privacy as it was adopted that the sheer amount of aggregate collection of digital information created a reasonable expectation of privacy, whether one individual communication was physically intercepted or not (Hecht-Felella, 2021).

Transferability: The U.S. model shows how judicial modifications of classical rights can be made to limit the modern and bulk data surveillance technologies, and Pakistan should learn this critical lesson, where the superior courts need to do the same with the older precedents on phone tapping (Ahmed, 2022) to include the extensive data gathering of the systems such as the FTS and ANPR.

4.4 Transferability Analysis: Pakistan Lessons

The comparative analysis indicates the definite ways to make Pakistan stronger:

Doctrinal Tool: The judiciary of Pakistan ought to in the official sense, embrace the Puttaswamy four-part proportionality test. Proportionality presents an analytic clarity and methodical inquiry which is better than the current Wednesbury unreasonableness test of reviewing executive conduct violating constitutional rights. This doctrine compels the state to prove that their AI systems are needed and appropriate (Mustafa, 2015).

Institutional Design (EU): GDPR is the better institutional design to regulatory design, which focuses on an independent Data Protection Authority having sufficient technical expertise and mandates which can make companies accountable by audits and penalties (European Data Protection Board, 2024).

Conceptual Framework (U.S./India): To work effectively in protecting against AI, the volumetric approach to privacy should be explicitly embraced by the Pakistani courts as it takes into account that the magnitude of information that is processed by the AI-based system, including those in the Safe Cities, is incompatible with a reasonable expectation of informational privacy and therefore requires strict judicial control akin to the warrant provisions in Carpenter (Hecht-Felella, 2021).

The strategies of the comparative jurisdictions are summarized in Table 2:

Table 2 Comparative Matrix: Constitutional and Regulatory Responses to Algorithmic Privacy

Jurisdiction	Constitutional Basis for Privacy	Rights Against Automated Decisions	Primary Regulatory Tool for AI/Privacy	Transferability Lesson for Pakistan
EU (GDPR)	Fundamental Rights (Arts. 7 & 8)	Explicit right to object to profiling/automated decisions (Art. 22).	Independent DPAs, mandatory DPIAs, and high financial sanctions.	Model for strong independent DPA and specific rights/mechanisms.
India (DPDP Act)	Fundamental Right to Informational Privacy (*Puttaswamy* ruling, Art. 21).	Proportionality test for state action; strong consent requirements; Consent Managers.	Legislative framework built on constitutional doctrine; regulatory board oversight.	High-relevance doctrinal model for judicial interpretation of Art. 14 and proportionality standard.

U.S.	Fourth Amendment (Search & Seizure).	Sectoral/State regulation (CCPA, etc.); no comprehensive federal law.	Judicial intervention (*Carpenter* Doctrine) limiting large-scale data collection.	Model for judicial adaptation to protect aggregate digital data (volumetric privacy).
Pakistan	Article 14 (Dignity and Privacy of Home).	Minimal explicit statutory rights; generalized right to object in Draft PDPB.	PECA 2016 (Reactive); Draft NCPDP (Proposed regulatory body).	Urgency of judicially expanding Article 14 to informational privacy and imposing stringent judicial review (Proportionality).

5. Doctrinal Lapses and the Algorithms Crisis in Pakistan

5.1 The use of Constitutional Proportionality Test on AI Surveillance

To run AI under the confines of the Pakistani constitutional guarantees, the implementation of AI should be under strict judicial scrutiny. Any technological intervention, especially one that interferes with the basic rights, should meet three fundamental tests, which are modified based on the constitutional jurisprudence to be considered constitutional (Afzal and Ghawaas, 2025, Cox & Palmer, 2024):

Process Integrity Test: Technical procedures should not water down procedural rights, which means that individuals should be able to obtain rational decisions and appeal decisions. By definition, algorithmic opacity does not pass this test because the black-box quality of several AI models does not allow the citizens to interpret or question the decisions, and thus infringes the right to a fair process (Afzal and Ghawaas, 2025).

Equality Test: AI systems should not discriminate or be biased against any social, gender, or geographic group, as it needs to be transparent and courts should be capable of tracking the information. Algorithms are prone to algorithmic bias that incorporates biases in the society, thus it directly violates the right of equality (Article 25) (Chaudhry, 2025, Afzal and Ghawaas, 2025).

Proportionality Test: AI application should be equal to its purpose and any violation of privacy should serve a just cause and the results of the utilization should justify the consequences. This is because state surveillance is often unsuccessful because it is non-targeted and of a mass kind (Afzal and Ghawaas, 2025, Cox & Palmer, 2024).

5.2 Violation of privacy and rights in Safe City Projects

The constitutional crisis at the moment is demonstrated by the accelerated implementation of AI in law enforcement in Pakistan, especially the Punjab Safe City Project with its Face Trace System (FTS) and Automated Number Plate Recognition (ANPR). These systems are meant to monitor and detect the terrorists, suspects, accused persons and criminals within the country (Lubna et al., 2021).

The constitutional implication of these deployments is the basic fault of any mass and non-targeted surveillance. This is exactly the form of blanket surveillance that had been already considered illegal, immoral, and unconstitutional by the Supreme Court in the Mohtarma Benazir Bhutto Case and other rulings on unlawful telephone tapping and eavesdropping. The judiciary held that there is a need to specifically authorize and justify surveillance (Ahmed, 2022).

The existing surveillance regimes, usually sanctioned by insufficient laws such as PECA as well as being provided by foreign technology vendors, work against the constitutional provision of necessity. These programs are constitutionally wanting because of the use of general mandates and the lack of independent judicial approval on the collection of data. They do not pass the necessity test of the proportionality test

as the state is performing indiscriminate collecting in which there may be more specific, less intrusive options. The absence of a robust privacy law gives the AI-driven surveillance the ability to be used too freely, expediting the capacities of the state to limit rights (Amnesty International, 2025, Jamil et al., 2025).

5.3 The constitutional Implications of Opacity and Bias in State AI Systems

The lack of transparency of most AI models applied by state agencies suggests the further infringement of constitutional rights. In cases where the state makes decisions founded on hidden algorithms, e.g. in predicting criminality or in deciding whether someone is eligible for benefits, the asymmetry of knowledge between the state and the citizen is absolute. The citizen is deprived of the right to know the logic behind the inputs or the right to contest the inputs that resulted into a rights amending outcome. This transparency does not support the constitutional mandate of judicial review and redress that carries with it (Livermore, 2025).

Moreover, in case the datasets that are used to train the predictive policing models are biased in the past, the resulting algorithm will perpetuate and formalize discrimination, which is in direct defiance of Article 25 (Equality before law). The constitutional doctrine requires that AI tools employed by the state should be seen as being of the utmost standards of impartiality and non-discriminatory nature. The lack of mandating auditable datasets and transparent design of algorithms is that the state is possibly automating discrimination against the constitution, and hence it warrants the implementation of the Equality Test as a constitutional condition to deploy AI (Chaudhry, 2025, Afzal and Ghawaas, 2025).

5.4 Structural Checks of National Security and Financial Accountability

The mass surveillance by state actors is often explained by the national security and counter-terrorism. Although national security is realized as a lawful state interest in constitutional law, international law, especially the Puttaswamy decision in India, requires that such allegations must be under a close proportionality scrutiny (Global Freedom of Expression, 2018). The constitutional test in Pakistan should also be tuned to make sure that national security claims will not be a rationalization of institutionalized constitutional infractions. It will need legal approval, the establishment of independent control, and the strong enforcement of the postulates of data minimization, which will not allow the state to bypass the current restrictions on surveillance with the help of AI (Amnesty International, 2025).

Lastly, considering the enforcement problems faced by Pakistan, financial accountability should be incorporated as a core rights enforcement measure. Such international regulations as GDPR place a significant emphasis on imposing financial fines (penalties) to make companies accountable. The future NCPDP should also have the authority to levy serious financial fines to both the state and the commercial sector data controllers. This brings about an effective economic deterrence that the price of infringing the fundamental rights and the uncontrollable algorithmic processing is sufficiently high to force one to act and therefore accountability is real, not just formal (MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023).

6. Constitutional Interpretation, Legislation and Regulatory Design Recommendations

Pakistan needs a dual approach of reforming constitutional interpretation through the judiciary and strict rights-driven statutory legislation to respond to the radical constitutional and regulatory issues of AI.

6.1 Judicial Strategy

The Supreme Court of Pakistan needs to make doctrinal action now in order to constitutionalize informational privacy:

6.1.1 Adoption of the Proportionality Standard Formally

The four-part proportionality test (Legality, Legitimate Aim, Necessity, and Suitability/Proportionality) should be taken on board by the superior courts to review all the state actions that involve digital data processing, and the deployment and functioning of AI systems are not exceptions. This standard has to replace the less demanding Wednesbury unreasonableness standard

of examination over executive action that breaches fundamental rights (Afzal and Ghawaas, 2025, Mustafa, 2015).

6.1.2 Interpretation of Article 14 to the Digital Age

The court needs to expressly read Article 14 to be comprised of the inherent right to informational self-determination since the systematic processing and profiling enabled by AI necessarily infringe on dignity, unless essential and proportionate. In addition, the court ought to embrace the volumetric approach to privacy acknowledging the fact that massive and aggregate digital data gathering is a search or intrusion that should be scrutinized more, similar to the doctrine of Carpenter of the U.S (Hecht-Felella, 2021).

6.1.3 Refining the Subject to Law Clause

The interpretation of Article 14 by judicial review should be limited in the sense that it should be defined as much as possible. Any new law that violates privacy should not only be legal but follow strictly the international standards of human rights and should meet the proportionality test. The laws which give unlimited and unrestricted authority to surveillance organs should be considered as unconstitutional due to the lack of necessity and proportionality (Government of Pakistan, 1973).

6.2 Legislative Reforms

The ultimate adoption of the PDPB (or replacement laws) should include the major accountability provisions taken out of the best practices:

6.2.1 Compulsory Algorithms Impact Assessment (AIAs)

The legislation should require Algorithmic Impact Assessments (AIAs) or Data Protection Impact Assessments (DPIAs) of all high-risk AI systems deployed in the public and the private sector, especially those that are used in policing (FTS/ANPR), welfare, or other areas of high-stakes decision-making. Such AIAs should be made laws that will consider risks in terms of accuracy, fairness, biasness, discrimination, privacy and security. Vital elements of these tests ought to be publicly released (with closely focused national security exemptions), and this ought to be conducted in consultation with independent auditors (Marquenie and Quezada-Tavárez, 2022).

6.2.2 Transparency Requirements, Explainability Requirements

Laws should also force data controllers to keep records of data provenance (provenance and integrity of training data) and give effective means to clarify high-stakes automated decisions to individuals that are impacted. This guarantees that the state meets the transparency principle of the algorithmic governance principle, and passes the constitutional Process Integrity Test (Cheong, 2024).

6.2.3 Enhancing Accountability and Consent

The PDPB should consider novel means of achievement, including the Consent Managers of the Indian model to make sure consent is meaningful, transparent, and revocable (Chaudhary and Verma, 2025). The legislation should guarantee the clear legal statements that should exclude the use of data by AI systems to process it on a secondary basis without providing renewed and considered consent.

6.3 Institutional Architecture

The success of the future data protection regime in Pakistan is based on the powers and independence of the NCPDP (MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023).

6.3.1 Independence and Technical Resources.

The NCPDP has to be completely independent of the executive, this should be ensured with safe funding, secure term of the members and also an open appointment procedure. It should also have sufficient technical know-how in its make-up, very clearly with experts in ICT, cyber security, and algorithmic governance (MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023).

6.3.2 Audit and Enforcement Powers

The NCPDP needs to have clear legal mandate to enforce external, independent audits of algorithm on the high risk systems deployed by any organization including state agencies. More importantly, the

Commission should be given the mandate of issuing binding enforcement orders, requiring system changes and imposing high financial fines that will be needed to deter both public and private data controllers (European Data Protection Board, 2024, MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2023).

6.4 Procedural and Remedial Safeguards

In order to make rights enforceable in today automation world, procedural protection has to be incorporated in administrative law:

Human-in-the-Loop Requirements: The legislation should require that the decision-making of high-stakes, choices that alter lives (e.g. in criminal justice, welfare or administrative penalties) should never be limited to automated processing. Human review and override should be ensured to ensure that the right to appeal against the decision by the individual is not violated.

Redress and Whistleblower Protection: The laws should provide redress systems that are simple to access and fast in the case of persons who have been injured by the automated machines. Strong measures should be put into place to motivate the reporting of algorithmic failures, biases or privacy violations in state and private entities.

7. Conclusion

The constitutional law of Pakistan has given a solid doctrinal basis of digital privacy based on the sacrosanctity of human dignity and cemented by the judicial precedents supporting the illegality of illegal surveillance (Article 14). But the fact that Article 14 is subject to law is a fatal flaw to this basis and the statutory gap that PECA 2016 produces due to its narrowness. As a result, the mass profiling systems are systematically implemented with the use of AI, including the Safe City projects, which are currently not adequately checked by the Constitution and contradict the proven judicial principles of necessity and proportionality.

The discussion has shown that the optimal solution to the problem of protecting the digital rights of Pakistani citizens involves a two-pronged intervention: both a judicial pledge to implementing the robust Puttaswamy-style proportionality test of state action and explicit enforcement via legislative means, including mandatory Algorithmic Impact Assessments and an autonomous Data Protection Commission (NPPD) with real audit and enforcement authorities. Such coordinated constitutional and regulatory action is all that is needed to move Pakistan to the same direction of responsible AI adoption that does not violate any fundamental rights or human dignity.

8. Limitations

The weaknesses of this research revolve around the dynamism of legislative reform, the ultimate text and political intent regarding the approval of the draft PDPB 2023 is still unclear, and this aspect may significantly change the statutory environment. Moreover, institutional secrecy limits the availability of granular, operationally relevant information about states AI systems (e.g., FTS algorithms, training data bias), which would help with having an empirical audit of the state level of constitutional compliance.

Existing research gaps require the collection of empirical research regarding the real-life effect of predictive policing systems and its practicality in Pakistan and a comparative approach to the institutionalization and implementation efficiency of the suggested NCPDP without referring to the already known GDPR models. Further research is also required to come up with technical and legal frameworks of mandated explainability that is not only viable to the developers of AI but also in redressing the constitution.

REFERENCES

AFTAB, S. 2024. Right to Privacy and Freedom of Expression in the Constitution of Pakistan. *Comparative perspectives on the right to privacy: Pakistani and European experiences*. Springer.

AFZAL, M. & GHAWAAS, H. G. 2025. Reforming Civil Justice in Pakistan through AI: A Critical Study of Legal Technologies and Their Impact on Access to Justice.

AHMED, K. 2022. *Electronic Surveillance and Interception Laws in Pakistan* [Online]. Online: Research Society of International law (RSIL). Available: https://rsilpak.org/2022/electronic-surveillance-and-interception-laws-in-pakistan/ 2025].

AMIN, M. H. & HASSAN, M. 2024. Digital privacy in Pakistan: Ending the era of self-regulation. *LUMS LJ*, 10, 22.

AMNESTY INTERNATIONAL. 2025. *Pakistan: Mass surveillance and censorship machine is fueled by Chinese, European, Emirati and North American companies* [Online]. Online: Amnesty International. Available: https://www.amnesty.org/en/latest/news/2025/09/pakistan-mass-surveillance-and-censorship-machine-is-fueled-by-chinese-european-emirati-and-north-american-companies/ 2025].

ARSHAD KHAN, E. 2018. The prevention of electronic crimes act 2016: An analysis. *LUMS LJ*, 5, 117.

CHAUDHARY, V. K. & VERMA, D. 2025. THE NEW FRONTIER OF DATA PROTECTION: UNDERSTANDING INDIA'S DPDP RULES AND GLOBAL COMPLIANCE. *PANJAB UNIVERSITY LAW MAGAZINE-MAGLAW*, 4.

CHAUDHRY, U. N. 2025. Algorithmic Decision Making in Pakistan. Online: Institute for Responsible Artificial Intelligence & Human Rights.

CHEONG, B. C. 2024. Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*, 6, 1421273.

COX & PALMER. 2024. *Necessity and Proportionality: Balancing AI Innovation with Privacy* [Online]. Online: Cox & Palmer. Available: https://coxandpalmerlaw.com/publication/necessity-and-proportionality-balancing-ai-innovation-with-privacy/ 2025].

DLA PIPER 2025a. Data protection laws in the United States. Online: DLA Piper.

DLA PIPER 2025b. PAKISTAN - Data Protection Laws of the World. Online: DLA Piper.

DWIVEDI, P. 2021. Puttaswamy V. Union of India. *Available at SSRN 4069390*.

EUROPEAN DATA PROTECTION BOARD. 2024. *AI Auditing* [Online]. Online: EDPB. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-auditing_en 2025].

GLOBAL FREEDOM OF EXPRESSION, C. U. 2018. *Puttaswamy v. Union of India (I)* [Online]. Online: Global Freedom of Expression, Columbia University. Available: https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/ 2025].

GOVERNMENT OF PAKISTAN 1973. Fundamental Rights and Principles of Policy. *In:* PAKISTAN, G. O. (ed.).

HECHT-FELELLA, L. 2021. The Fourth Amendment in the Digital Age. Available: https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age.

HYDER, G., REHMAN, T. U. & SAEED, A. 2025. Predictive Policing and the Rule of Law: Evaluating AI's Role in Criminal Justice through Global and Pakistani Legal Frameworks. *The Critical Review of Social Sciences Studies*, 3, 1119-1127.

INTERSOFT CONSULTING. 2025. *General Data Protection Regulation (GDPR)* [Online]. Online: Intersoft Consulting. Available: https://gdpr-info.eu/ 2025].

JAMIL, M. S., DAYAL, A. A., BILAL, H. & QAISER, M. N. 2025. Privacy of Home to Privacy-by-Design: Article 14 of the Pakistani Constitution in the Age of AI Surveillance. *International Research Journal of Arts, Humanities and Social Sciences*, 3, 279-293.

JHOKIO, A. & REHMAN, T. U. 2025. Data privacy laws in Pakistan: A comparative analysis with the EU's General Data Protection Regulation. *Journal of Political Stability Archive*, 3, 870-882.

KALYAR, B. J. A. 2021. *Protecting the Data - A Comparative Analysis of Pakistan's Personal Data Protection Bill, 2020*, Media Matters for Democracy.

KATZENBACH, C. & ULBRICHT, L. 2019. Algorithmic governance. *Internet Policy Review*, 8, 1-18.

KERRY, C. F. 2020. Protecting privacy in an AI-driven world. *Brookings Institution*, 10.

KHAN, S. H. & KHAN, S. 2025. Data Protection & Privacy 2025. Available:

https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/pakistan.

KHAN, Y. A. 2025. The concept of authorisation under Pakistan's data protection laws against the backdrop of the EU General Data Protection Regulation. Available: https://www.ibanet.org/concept-of-authorisation-Pakistan.

KING, J. & MEINHARDT, C. 2024. Rethinking Privacy in the AI Era Policy Provocations for a Data-Centric World. *Available at SSRN 5446957*.

LIVERMORE, M. A. 2025. The Political Limits of Algorithmic Governance. Available: https://www.theregreview.org/2025/12/15/livermore-the-political-limits-of-algorithmic-governance/.

LUBNA, MUFTI, N. & SHAH, S. A. A. 2021. Automatic number plate Recognition: A detailed survey of relevant algorithms. *Sensors*, 21, 3028.

MARQUENIE, T. & QUEZADA-TAVÁREZ, K. 2022. Data Protection Impact Assessments in Law Enforcement: Identifying and Mitigating Risks in Algorithmic Policing. *Security Technologies and Social Implications*, 32-60.

MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION 2023. DRAFT OF THE PERSONAL DATA PROTECTION BILL, 2023. *In:* TELECOMMUNICATION, M. O. I. T. (ed.). Online.

MÜHLHOFF, R. & RUSCHEMEIER, H. 2025. Updating purpose limitation for AI: a normative approach from law and philosophy. *International Journal of Law and Information Technology*, 33, eaaf003.

MUSTAFA, H. 2015. Wednesbury, proportionality and judicial review. *LUMS LJ*, 2, 1.

PRS LEGISLATIVE RESEARCH. 2023. *The Digital Personal Data Protection Bill, 2023* [Online]. Online: PRS Legislative Research. Available: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 2025].

QAYYUM, H., NISA, M. U. & KHAN, S. 2025. Human Rights and the Era of Generative Artificial Intelligence–Assessing and Enhancing Pakistan's National AI Policy with an Insight into Global Perspectives. *Law and Policy Review*, 4, 44-67.

REISMAN, D., SCHULTZ, J., CRAWFORD, K. & WHITTAKER, M. 2018. Algorithmic impact assessments: a practical Framework for Public Agency. *AI Now*, 9.

SOHAIL, S. 2025. AI at the Crossroads: Pakistan's Regulatory Challenge. *Courting the law* [Online]. Available from: https://courtingthelaw.com/2025/10/03/commentary/blawgs/ai-at-the-crossroads-pakistans-regulatory-challenge/ 2025].

SQUIRE PATTON BOGGS. 2025. *Overview of Privacy & Data Protection Laws: United States* [Online]. Online: Squire Patton Boggs,. Available: https://www.privacyworld.blog/summary-of-data-privacy-protection-laws-in-the-united-states/.

SUPREME COURT OBSERVER. 2025. *Fundamental Right to Privacy - Justice K.S. Puttaswamy v Union of India* [Online]. SCO - Supreme Court Observer. Available: https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/ 2025].

TAYLOR-HISCOCK, R. 2025. Your complete guide to General Data Protection Regulation (GDPR) compliance. *onetrust* [Online]. Available from: https://www.onetrust.com/blog/gdpr-compliance/ 2025].

USHA, T. & NEERAL, G. 2025. Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023. *Legal Issues in the digital Age*, 87-117.

YOUSAF AMANAT & ASSOCIATES. 2025. *COMPARING PECA 2016 AND THE PERSONAL DATA PROTECTION BILL 2023: A CRITICAL ANALYSIS OF CYBERCRIME AND DATA PRIVACY LAWS IN PAKISTAN* [Online]. Online: Legal500. Available: https://www.legal500.com/developments/thought-leadership/comparing-peca-2016-and-the-personal-data-protection-bill-2023-a-critical-analysis-of-cybercrime-and-data-privacy-laws-in-pakistan/ 2025].