Innovative Research Journal of **Artificial Intelligence** (IRJAI)
DOI: https://doi.org/10.62497/irjai.240

Review Article

The Right to Privacy in the Age of Artificial Intelligence: Evaluating Pakistan's Civil Law Protections against Algorithmic Surveillance and Data Misuse

Muhammad Zakir Khan[1]*, Fakhre Alam[2]
1 College of Humanities and Law, Chengdu University of Technology, 610059 Chengdu, China
2 College of Business, Chengdu University of Technology, 610059 Chengdu, China

Citation: Khan MZ, Alam F. The Right to Privacy in the Age of Artificial Intelligence: Evaluating Pakistan's Civil Law Protections against Algorithmic Surveillance and Data Misuse. Innov. Res. J. AI. 2026;4(1):1-19. Available from: https://irjpl.org/irjai/article/view/240

Article Info
Received: April 30, 2026
Revised: June 12, 2026
Accepted: June 24, 2026

Keywords
artificial intelligence; ai; privacy; data protection; algorithmic surveillance; civil rights; Pakistan; biometric data; automated decision-making

Copyright © 2026 The Author(s).

Published by Innovative Research Journals.

This is an Open Access article under the CC BY NC 4.0 license. This license enables reusers to distribute, remix, adapt, and build upon the material in any medium or format for noncommercial purposes only, and only so long as attribution is given to the creator.

Abstract

The concept of privacy has morphed in real life with AI. We have all seen the concept of Privacy evolve practically with AI. Modern surveillance does not rely exclusively on the need for certain people to be supervised in a certain place; it is the result of continuing flows of identity, location, biometric, financial, health and behavioral information that are gathered, connected and inferred. Article 14 of the Pakistan Constitution guarantees dignity and privacy of the home and case law has recognized eavesdropping and tapping of telephone conversations as constitutional violations in the country. But the regular civil law structure is still in disarray. The Prevention of Electronic Crimes Act, 2016 covers all aspects of unauthorized access, misuse of personal identity and interception; the Investigation for Fair Trial Act, 2013 covers certain types of warrants for investigations; the Right of Access to Information Act, 2017 covers disclosure of personal records; and general civil remedies include bringing in an injunction, action on a contract, defamation, and constitutional review. However, none of these tools provide an all-encompassing array of rights which regulate legal data processing, biometric monitoring, automated decision making, algorithmic explanation, auditing and compensation for the misuse of data. They apply doctrinal and comparative legal analysis to assess that gap in this article. It states that the constitutional commitment trumps the current legal framework of the Pakistan Constitution and, through its commitment to the protection of the rights of the people, it has introduced greater sanctity into the proceedings. It is not that the constitutional commitment is not superior to the present legal structure, as it can bring meaning to the interpretation of rights, but case-by-case litigation cannot replace a comprehensive law on data protection.

* ***Corresponding Author:***
Muhammad Zakir Khan
Email: advzakirkhan12@gmail.com

1. Introduction

The privacy law was designed to protect against the types of invasions that are easily observed, such as breaking into a home, making an interception, revealing a private fact, or accessing a private (confidential) record. That model is amped by artificial intelligence. An individual can be unidentifiable and be the subject of constant tracking via mobile identification, camera networks, platform usage, shopping habits, facial template recognition, and deductions drawn from facial template recognition. The date of collection, therefore, does not limit the extent of the injury. It can show up later when merged datasets are used; when a model is used to assign a risk score; or when a shared opportunity is not granted owing to an opaque prediction of the model. [24-29]

The initiation point of the Constitution of Pakistan is important. As per Article 14(1), the dignity of man and 'privacy of the home' is indispensable and 'subject to law'. Articles 9 and 10A affirm the principle of liberty, due process and equal protection; Articles 19 and 19A provide for a balance between expression, access to information and legitimate privacy interests. Articles 9 and 10A affirm the principle of liberty, due process and equal protection; Articles 19 and 19A provide for a balance between expression, access to information and legitimate privacy interests [1]. One of the main reasons why the Supreme Court's judgment in Mohtarma Benazir Bhutto v President of Pakistan has been pivotal is its notion of telephone tapping and eavesdropping supporting not only an invasion of privacy and dignity but also a technical irregularity [4]. So, the language of the Constitution is able to adapt to new technologies, but the principle and enforcement of the Constitution are not synonymous.

What the current challenge is, is an institutional and remedial challenge. Pakistani legislation includes provisions for cybercrime, surveillance rules, identity management laws, laws that deprive citizens of information, and for ordinary civil causes of action. They apply to various authorities, various levels of relief, and various types of protection. If an algorithmic decision does not have a specific justification, a citizen data's private file has been sold without their consent, or his application for a job is turned down by a biased model, maybe he won't be able to find a single action that not only will give him access to the data, but will also help him get clarity, have his data deleted and receive compensation. The law could punish a dishonest intrusion without having any controls for an organization that acquired data lawfully for a purpose but ultimately misapplied it for that or another.

The purpose of this article is to critique the civil-law protections currently in place in Pakistan and whether they are sufficient for algorithmic surveillance and data misuse. The main idea is that it is the Constitution which gives a norms-based norms, while the existing laws do not establish an exhaustive horizontal privacy regime for both public and private data controllers. The analysis also addresses the "bandying" of a legislative description that is made frequently. The now-passed Personal Data Protection Bill, 2023 was introduced as a private-member bill; however, according to the current bill record at the Senate, it does not appear on the records whether it passed or was rejected [13]. The MOTT in May 2026 told the National Assembly that they have completed a separate comprehensive Personal Data Protection Act 2026 bill [14]. There was no record of its enactment was found. Thus, Pakistan does not yet have an enactment of an 'all-in-one' personal-data legislation.

2. Research Questions, Method and Scope

This paper is broken down into four questions. One important question is how far we interpret Article 14 and other fundamental rights to apply to informational privacy, before going beyond the right to privacy in our homes? First, what is the extent of Article 14 and other fundamental rights that go beyond the physical home in applying to informational privacy? Second, what protection is currently provided by laws and regulations related to cybercrime, surveillance or access to information and the general civil law? Thirdly, in which ways is it deprived of remedies in algorithms, inference, or by private entities? Finally, how would the constitutional principle become real rights and remedies?

The approach taken is the doctrinal approach. It does

not consider the protection of data to be a standalone technology problem but looks at it in the context of the interplay of the Constitution, federal legislation, reported cases, as well as new policy instruments. It also has references to comparative benchmarks derived from the International Covenant on Civil and Political Rights (Article 19) [2,20-21,34-35] and the European Union's General Data Protection Regulation (GDPR) [2,22] as well as the European Union's Artificial Intelligence Act (AI Act) [2,23] and the Recommendation on the Ethics of Artificial Intelligence (EAI) [2,34-35] of the UNESCO. The aim of the comparison is not to replicate another jurisdiction's statute verbatim, but rather to isolate and list some of the legal gaps in the functions that presently exist in Pakistan.

The emphasis is on civil protection. An affected person affected by a criminal offence is considered, because such offences are part of the ongoing private sphere, but it is asked how far an affected person is brought that he can prevent the harmful processing, hear a report on what has happened, rectify the affected data and obtain meaningful compensation. National-security surveillance is only discussed insofar as it is relevant to the assessment of its legality, oversight and proportionality. This article is not designed to evaluate the market worthiness of any individual security program.

3. From Observation to Algorithmic Surveillance

Algorithmic surveillance goes beyond electronic surveillance. It is a series of activities that lead to the collection of data, connection of this data, analysis, and the transformation into a decision or intervention. This model could detect a face, create a relationship, predict default, rank an employee who has applied for a job, and/or alert a traveler to an unusual pattern. The process involved with each step can interfere with rights. The information could be collected more than necessary, or it could be linked to other information that obliterates the context in which the information was conveyed; the output might reproduce historical discrimination; the training data may lead to discrimination; or the affected individual may not even be told that an automated score played a part in the result.

This is important, as it is the typical rules of law that center on unauthorized access or interception. A privacy injury can be caused by another party (including AI) to data that has been granted formal permission to be collected but continues to suffer from its subsequent use, prolonged storage, and sensitive inference or disproportionate use. If the agreement has been given, it might be hidden in the usual conditions and not rationalize all future use. A rights-based analysis also requires not only the question of acquisition of the data, but also the question of why they were processed, whether it was necessary to do so, whether alternatives to the use of more intrusive means were available, and whether the outcome was contested [25-26,33].

The greatest dangers occur when identity is long-term and course openers are not easily reversible. Unlike passwords, biometric templates cannot be changed. Association and worship, medical visits and politics are reflected in location histories. The administrative facts generated by predictive systems can convert probabilistic correlations into facts. On the level of population scale, even a slight error rate can put thousands of people up for a false match or misguided monitoring. Hence, three elements of privacy (interference by an opaque system), equality and due process (system of unjust discrimination against a group) come together in one, there is an opaque system that invades the privacy of individuals, discriminates against a group, and takes away an individual's due process to challenge the system [28-32].

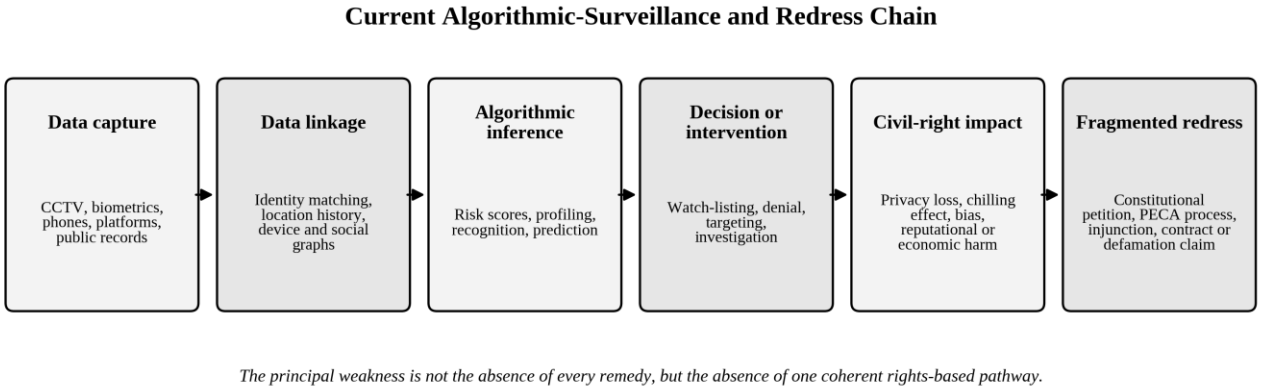


Figure 1: Current algorithmic-surveillance and fragmented-redress chain in Pakistan.

4. Constitutional Foundations of Privacy and Civil Rights

4.1 Article 14: dignity, home and informational privacy

The contemporary terminology of personal data, personal profiling and automation are not explicitly used in Article 14. Dignity and the privacy of the home are its object, subject to the law [1]. A narrow "literalist" interpretation could limit privacy to the realm of the home. It's very hard to believe such a reading in a digital society, where the home itself functions as a constant communications medium via phones, cameras, cloud services, and connected things. The Article brings together Privacy and Dignity, above all. Dignity does not belong to walls and doors, it belongs to the circumstances under which a person can establish relationships, communicate, ask for treatment, express their beliefs and make decisions without buttressing, disproportionate and uncalled-for scrutiny.

This is the logic of what the Supreme Court ruled in Mohtarma Benazir Bhutto. The Court said that a telephone call may not be heard by unauthorized users even if conducted over a telecommunications system [4]. It did not happen to be a protected interest to own the telephone line. It was the dignity of the citizen, freedom and his just and reasonable expectation that his private communication was not secretly and without lawful authority to be turned into state information. The principle of technological mediation does not do away with the constitutional right to privacy and should also guide the analysis of algorithmic monitoring.

The phrase 'subject to law' does not give the State an unlimited power to authorize surveillance. A law which restricts a fundamental right must be precise, must aim at serving a legitimate purpose and must be drafted in a non-arbitrary way. In the digital world, legality involves rules regarding the types of data, who is allowed to approve access, how long it lasts, how long it's kept, who can be part of the data to be shared, who authorizes independent review and remedies if misused. Vulnerability and sensitivity of the data to be processed may easily be undermined by a bare statutory power, without strictly proportionate limitations and protections.

4.2 Articles 9 and 10A: liberty, life and procedural fairness

According to Article 9, the right to life and the right to be left free from the state of death shall not be violated except according to the law; Article 10A, the determination of civil rights and obligations and the imputation of criminal charges must be based upon engaging in free and fair proceedings in accordance with the law. The guarantees are applicable to an algorithmic output when it has a 'material influence' on policing services, welfare services, license applications, employment, credit, education, travel. An adverse judgement cannot have any effect unless: the fact that the system exists is hidden, the deciding data is not shown, or the score logic is not made apparent. In most but not all cases, the disclosure of source code is unnecessary, but disclosure of intelligible explanations and the ability of the decoder to address material errors and to ask questions subject to review before a human decision maker are generally required.

The same is true for the association to freedom. There is no need for prosecution to change behavior, as long as there is a persistent monitoring system in place. People may opt out of lawful association, speech, worship and/or medical consultation due to the belief that these are being recorded and assessed. In this chilling effect, privacy, driven by a personal taste, becomes a structural condition for freedom in democracy [26].

4.3 Articles 19, 19A and 25: expression, information and equality

There needs to be a balance between the protection of privacy and freedom of expression and the right of access to information. Article 19 protects speech, except in constitutional matters, subject to constitutional restrictions. Article 19A guarantees the right to access information in matters of public importance, subject to regulation and reasonable restrictions [1]. The function of legislation doesn't require making all data confidential. It is for the balance between transparency in public power and the identification of individuals. Public authorities should be accountable for the use of AI systems that have significant impacts on or relate to the life of citizens in terms of their existence, purpose, and manner of procurement, as well as error rates and governance arrangements, and ensure that legitimate investigative detail is adequately protected while ensuring adequate protection of personal records.

The rights recognized in Article 25 are equality before law and equal protection of law [1]. Even if the system seems to be facially neutral, therefore, algorithmic bias may be a constitutionally protected problem. A model built using imbalanced training sets can subconsciously oppress women, religious minorities, people from specific areas, persons with disabilities, and people from economically neglected areas. An outcome test does look at whether discrimination was meant to be targeted, but it also should address data quality and institutional context through a rights-based lens [28-30].

Table 1: Constitutional and statutory provisions relevant to AI-related privacy harms.

Provision	Core rule	Relevance to AI/privacy	Principal limitation
Constitution, Art. 14(1)	Dignity and privacy of the home are inviolable, subject to law.	Constitutional foundation for communications and informational privacy.	Requires judicial interpretation; does not itself create detailed processing duties.
Constitution, Arts. 9 and 10A	Life/liberty according to law; fair trial and due process.	Supports notice, reasons, correction and review where automated outputs affect rights.	No general statutory procedure for automated decisions.
Constitution, Art. 25	Equality before law and equal protection.	Ground for challenging discriminatory algorithmic effects.	No general mandatory algorithmic-impact or equality audit.
PECA 2016, ss. 3-5	Criminalizes dishonest unauthorized access, copying/transmission and interference.	Useful for hacking, theft or manipulation of data.	Does not regulate all lawful-but-unfair secondary uses.
PECA 2016, s. 14	Offence of unauthorized use of identity information; blocking/destruction application.	Direct protection against identity misuse.	Narrow trigger and mainly offence/removal oriented.
PECA 2016, ss. 17-19	Unauthorized interception; dignity/privacy and intimate-image offences.	Protects communications, reputation, privacy and sexual dignity.	Not an omnibus data-processing regime.

PECA 2016, s. 36	Court-ordered real-time collection for a specific criminal investigation, limited in duration.	Introduces judicial authorization and necessity language.	Does not govern all public-sector analytics or retrospective data linkage.
Investigation for Fair Trial Act 2013, ss. 8-14, 27, 29, 34-35	Warrant process, review committee, complaints and offences for misuse/unauthorized surveillance.	Procedural control of specified surveillance and interception.	Secret process; limited public transparency and no algorithm-specific standards.
RTI Act 2017, ss. 7(g)-(h), 16(c)	Excludes or exempts records where disclosure invades personal privacy, subject to exceptions.	Balances public transparency with identifiable-person privacy.	Controls disclosure by public bodies, not the full lifecycle of data processing.
Specific Relief Act 1877, ss. 52-55; CPC, O. XXXIX rr. 1-2	Preventive and temporary/perpetual injunctions.	Can restrain continued disclosure, misuse or threatened harm where a cause of action exists.	Relief depends on fitting the claim within existing substantive law.
Contract Act 1872, s. 73	Compensation for loss caused by breach of contract.	Supports claims for breach of confidentiality or agreed data-use limits.	Protects parties to a contract; weak for bystanders and non-negotiated consent.
Defamation Ordinance 2002, ss. 3, 8-9	Civil action and remedies for defamatory publication.	May address false algorithmic statements that damage reputation.	Does not remedy accurate but intrusive profiling or secret scoring.

5. Existing Statutory and Civil-Law Protections

5.1 Existing Statutory and Civil-Law Protections

Pakistan's privacy and data-governance framework remains fragmented. The Constitution 1973 provides the main rights-based foundation through dignity, privacy, due process, expression and information rights, but lacks an express informational-privacy guarantee. PECA 2016 criminalizes cyber offences and interception but does not comprehensively regulate data processing or provide broad data-subject rights, while IFTA 2013 establishes judicial safeguards for targeted surveillance but offers limited protection against bulk or algorithmic surveillance. The Right of Access to Information Act 2017 protects personal information from public disclosure but does not regulate internal data use, profiling or analytics. The National AI Policy 2025 and draft National Data Governance Policy 2026 provide important policy direction, including responsible AI and public-sector data rights, but remain non-binding and limited in scope. Existing civil and constitutional remedies are available but fragmented and inadequate for modern data harms. The proposed PDP Bill 2023/2026 would provide comprehensive data-protection rights and independent oversight, but since it has not been enacted, Pakistan currently lacks a unified, enforceable data-protection regime.

Table 2: Comparative summary of Pakistan's legal instruments governing privacy, surveillance and data protection.

Instrument	Scope	Strengths	Key Gaps
Constitution of Pakistan 1973 (Arts. 9, 10A, 14, 19, 19A, 25)	Fundamental rights applicable to State action; dignity, privacy of home, due process,	Normative foundation; Supreme Court interpretation extends to telephone surveillance;	No express informational privacy right; requires judicial interpretation; limited direct horizontal

	expression, information, equality	rights-based orientation; applies horizontally through State obligation	application to private actors; no statutory enforcement mechanism
Prevention of Electronic Crimes Act 2016 (PECA)	Cybercrimes including unauthorized access (ss. 3-5), identity misuse (s. 14), interception (s. 17), online privacy offences (ss. 18-19), court-ordered collection (s. 36)	Criminalizes data theft, hacking and identity misuse; provides blocking/removal remedies; judicial authorization for real-time collection	Offence-centered model; no comprehensive processing duties; does not regulate lawful-but-unfair secondary uses; no universal data subject rights; weak civil compensation
Investigation for Fair Trial Act 2013 (IFTA)	Judicial warrant procedure for specified surveillance and interception; review committee; complaints mechanism (ss. 8-14, 27, 29, 34-35)	Warrant framework; judicial authorization; oversight committee; misuse offences	Designed for discrete interception, not algorithmic surveillance; no bulk data safeguards; limited transparency; no algorithm-specific standards
Right of Access to Information Act 2017	Limits public disclosure of personal privacy records (ss. 7(g)-(h), 16(c))	Protects identifiable personal data from public disclosure; balances transparency and privacy	Governs external access only, not internal processing; no regulation of public-sector analytics, linkage or profiling; no data subject rights
National AI Policy 2025	Ethical, responsible and transparent AI; human rights recognition; coordination with data protection	Express commitment to rights; acknowledges need for regulation; policy direction	Policy only, not legally enforceable; no specific rules; acknowledges absence of regulatory provision
National Data Governance Policy 2026 (draft)	Public-sector consent, access, correction, portability, erasure, sensitive data, breach reporting (federal public bodies)	Detailed administrative framework; privacy-enhancing technologies; retention rules	Applies only to federal public bodies; no private-sector coverage; policy not legislation; anticipated PDP Act not yet enacted
General Civil Remedies (Specific Relief Act 1877, Contract Act 1872, Defamation Ordinance 2002, Constitutional petitions)	Injunctions, contractual damages, defamation, constitutional review	Available tools; can restrain publication or processing; contractual protection	Substantive fragmentation; no general data protection causes of action; weak for non-material damage; no representative actions
Personal Data Protection Bill 2023 / Proposed PDP Act 2026 (not enacted)	Proposed: Commission, lawful processing, data subject rights, erasure, AI transparency, cross-border rules, sensitive data	Would address most identified gaps; constitutional orientation; independent regulator	Not enacted; disposed of by Senate committee (2023); 2026 bill finalized by executive but not passed by Parliament; citizens cannot rely on

			proposed rights

5.2 Prevention of Electronic Crimes Act, 2016

The most notable Federal legislation related to illegal acts involving information, systems and data is the Prevention of Electronic Crimes Act, 2016 (PECA) [7]. Dishonest access and copying or transmission; interference – Sections 3 to 5. Section 14 constitutes a criminalization of the unauthorized use of identity information and allows steps to be taken for the purposes of securing, destroying, blocking or preventing transmission of information affected by the inaccurate use of such information. Authorized interception is covered in Section 17. The dignity, privacy and sexual integrity in certain types of online publications (such as manipulated intimate material) are immunized under sections 18 and 19. Section 36 only allows real-time collection for a specific criminal investigation and is subject to restrictions as to necessity and in the original bill no greater than seven days.

Such provisions are relevant but are based on an offender-focused model. PECA is most effective when the perpetrator is dishonest, logs into a system without permission, takes possession of someone's identity, eavesdrops on a communication or posts content otherwise prohibited. Today's data harms are not of that nature. It is possible for a platform, employer, insurer or public body to have data lawfully, but to use it in a manner that is not compatible with the original purpose. May be able to hold information for years, may try to infer sensitive characteristics, may train without sufficient precautions or use an unexplainable score. This kind of activity is not necessarily illegal or "unauthorized access" as may be considered unconstitutional and unfair.

PECA is also not a general civil compensation scheme based on data harm. There is no general "right to be provided with their data", "right to correct their data", "profiling prohibition" or "loss of data control" under the Act; neither is there a right to notification on breach of the rights nor the prospect for "loss of control" or non-material damages. These are the kind of remedies that are called for where the damage is in the form of information and not matter.

5.3 Surveillance and interception statutes

The Pakistan Telecommunication (Re-organization) Act, 1996 allows interception or tracing to be authorized at the federal level on the ground of interest of the security of the country or apprehending any offence [5]. The Implementation of the Investigation for Fair Trial Act, 2013 governs investigatory warrants to a greater extent for the specified surveillance and interception mentioned in the Act. Our provisions cover such things as the application for a warrant, its review and issuance, and how long it can be issued for; a review committee, complaints concerning its misuse, and its liability for unauthorized surveillance or misuse of leaked information [6].

A warrant regime is better than the discretion of the executives, but algorithmic surveillance raises questions about its limits when the design is based on a discrete level of surveillance. Today's computer programmers can utilize bulk datasets, retrospective searching, automated facial recognition, association analysis, and continuous risk scoring. Today the question of whether a communication might be imperceptible to unauthorized parties is no longer the sole legal issue. It's also how many millions of records can be gathered together and then scanned, whether innocent people are subjecting themselves to repeated scans, and how the error rate is calculated and when it is OK that a person should be informed when there's no longer a need for keeping the anonymity.

Therefore, necessity and proportionality need to be as part of both the acquisition and analysis phase of the governing standard. Having made a lawful initial collection does not imply that every subsequent algorithmic use is likewise lawful. Judicial authorization must include data sources, the class or persons to be targeted, the method to be applied for analysis, the duration, the time period for which it is retained, restrictions on who can use it and who can audit it. Confidentiality is justifiable for national security, but should not preclude independent supervision or effective complaint processes once a decision has been made for security [2,34,35].

5.4 Right of access to information and public-sector data

Private-esteem is restricted public disclosure as enounced in the Right of Access to Information Act, 2017. Records of personal privacy and a private document handed over to a public body express or implied as being confidential are excluded from Section 7. They include Section 16(c) exemptions for information that would otherwise infringe upon an identifiable person's right to privacy (as long as the information is disclosed with consent), allow for the release of "garden leave" information, and permit release of information under certain public-official-function exceptions [8]. This distinction will correctly separate public accountability from unchecked disclosure of personally-held information.

However, the former subject is access to records and not internal processing. A public body can agree to the demand for external use as they do use the records internally for linkage, profiling or automated allocation but refuse the request for an external use. The law thus guards against one mode of exposure but not whether the underlying analytics is lawful, necessary and accurate or contestable.

5.5 Identity systems, digital government and policy instruments

The National Database and Registration Authority Ordinance, 2000 establishes Pakistan's central identity infrastructure [9]. The Digital Nation Pakistan Act, 2025 expands institutional capacity for digital government, data exchange and national digital transformation [10]. These instruments make data governance more urgent, not less. When identity credentials become the key through which multiple services are accessed, linkage can produce efficiency but also function creep: information collected for identification may be used for eligibility, policing, scoring or commercial verification in ways the citizen did not reasonably anticipate.

The National Artificial Intelligence Policy, approved in July 2025, endorses responsible, ethical and transparent AI and expressly recognizes the need to preserve human rights and coordinate with proposed data protection legislation [11]. Its action matrix nevertheless acknowledges the absence of a current AI regulatory provision. The Data Governance Policy issued in draft form in 2026 is more detailed. It addresses public-sector consent, access, correction, portability, erasure, sensitive data, children's data, breach reporting, retention and privacy-enhancing technologies [12]. Yet it applies to federal public bodies and associated processors, does not govern private-sector personal data, and describes the Personal Data Protection Law as anticipated. These policies are valuable administrative direction, but policy cannot provide the certainty, independence and enforceable remedies of primary legislation.

5.6 General civil remedies

Pakistan has a central identity infrastructure called the National Database and Registration Authority Ordinance, 2000 [9]. The Digital Nation Pakistan Act, 2025 further envisages capacity building of institutions on digital government, digital data exchange and national digital transformation [10]. These tools drive that needs for data governance forward, not back. Linkage can generate efficiency while also acting as something creepy: while the data needed for identification can be linked to other services for citizenship eligibility, governance and scoring, it can also be used in a way the citizen never thought it was being gathered for.

The National Artificial Intelligence Policy, adopted in July 2025, supports responsible, ethical, and transparent uses of AI and explicitly mentions the importance of upholding human rights and commends the ongoing development of new data protection laws [11]. The action matrix, however, shows that there is no current AI regulation provision. The Data Governance Policy in draft in 2026 has more detail. It covers public sector consent, access, correction and portability, erasure, sensitive data, children's data, reporting on breaches, retention and privacy-enhancing technologies [12]. But it does not cover private-sector personal data; it does not apply to federal public bodies and processors, and it anticipates the Personal Data Protection Law. These policies are important administrative guidelines, but policies cannot give the assurance, separability, and enforcement mechanisms of Primary Laws.

Table 3: Illustrative AI uses, civil-right risks and currently available remedies.

Use case	Data processed	Primary civil-right risk	Possible current route	Unresolved gap
Facial recognition in public spaces	Facial template, location, time and association	False match; continuous tracking; chilling of assembly	Article 14/199 petition; surveillance-law challenge; injunction where maintainable	No general statutory threshold, public register, accuracy duty or deletion right
Automated hiring	CV, education, identity, video or behavioral features	Sex, disability, class or regional discrimination; opaque rejection	Contract/employment remedies; Article 25 where state action exists	Private-sector equality and explanation duties are uncertain
Credit or insurance scoring	Financial, device, location and social data	Exclusion based on proxies; inaccurate profile; price discrimination	Contract, sectoral complaint and ordinary civil claim	No universal access, correction or human-review right
Predictive policing or watch-listing	Crime data, identity links, travel and communications metadata	Feedback loops; false suspicion; liberty and due-process harms	Constitutional review; IFTA/PECA safeguards	Model logic, data quality and error rates may remain undisclosed
Health or welfare analytics	Health, disability, family and income information	Sensitive inference; denial of benefit; stigma	Constitutional and administrative review; confidentiality duties	No comprehensive sensitive-data or automated-decision regime
Generative-AI profiling and data scraping	Public posts, images, voice, inferred preferences	Loss of context; impersonation; intimate or reputational harm	PECA ss. 14, 18-19; defamation; injunction	Lawful scraping, model training and inferred data remain uncertain

6. Comparative International Perspective: Selected Jurisdictions

Understanding Pakistan's position benefits from a concise comparison with how other jurisdictions address algorithmic surveillance and data protection. This section examines three models—the European Union, the United Kingdom, and Singapore—to identify transferable legal functions and international best practices.

6.1 European Union: The GDPR and AI Act

The EU has adopted the most comprehensive two-tier framework. The General Data Protection Regulation (GDPR) of 2016 establishes a unified data protection regime with a broad territorial scope and strong individual rights. Article 5 requires lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality. Article 22 grants individuals the right not to be subject to solely automated decisions with legal or significant effects, while Articles 13-15 require transparency about processing, including automated decision logic. Article 35 mandates data protection impact assessments for high-risk processing.

The EU AI Act (2024) supplements the GDPR by classifying AI applications by risk. "Unacceptable risk" systems are prohibited; "high-risk" systems (e.g., critical infrastructure, education, employment, law enforcement) must comply with requirements for risk management, data governance, technical documentation, transparency, human oversight, accuracy and robustness. Biometric identification in public spaces is strictly limited. Infringements attract substantial administrative fines up to €35 million or 7% of global turnover.

Relevance to Pakistan: The EU demonstrates that data protection and AI governance can coexist through distinct but complementary statutes. Pakistan's proposed framework could similarly separate general data protection from AI-specific rules, with high-risk AI triggering enhanced safeguards.

6.2 United Kingdom: Post-Brexit Adaptation

The UK's Data Protection Act 2018 implements the GDPR with domestic modifications. The UK GDPR retains core protections including lawful bases, data subject rights, and the Information Commissioner's Office as independent regulator. The UK's National AI Strategy (2021) and regulatory approach favor sector-specific adaptation rather than omnibus AI legislation. The government has proposed a "pro-innovation" framework that relies on existing regulators (e.g., the Information Commissioner and the Competition and Markets Authority) to interpret and apply principles to AI.

The UK also enacted the Investigatory Powers Act 2016, which regulates bulk surveillance, interception, and retention of communications data, and requires judicial warrants and oversight by the Investigatory Powers Commissioner.

Relevance to Pakistan: The UK shows that a common law jurisdiction can integrate data protection principles through a combination of statute, independent regulation and judicial oversight, even without a single AI-specific law. Pakistan could similarly rely on the Federal Investigation Agency, PTA and a future Data Protection Commission to coordinate enforcement.

6.3 Singapore: Asian Data Protection Model

Singapore's Personal Data Protection Act 2012 (PDPA), amended in 2020, establishes a consent-based framework administered by the Personal Data Protection Commission. It includes obligations for data protection, retention, transfer and accountability. The PDPA permits organizations to collect, use and disclose personal data for legitimate business purposes without consent in specified circumstances, balancing commercial innovation and individual protection.

Singapore's Model AI Governance Framework (updated 2020) provides voluntary guidance on internal governance, decision-making and transparency, complemented by sectoral regulatory experiments (e.g., financial services). The approach is less prescriptive than the EU, reflecting Singapore's priority on attracting technology investment while maintaining baseline privacy standards.

Relevance to Pakistan: Singapore demonstrates that a developing Asian economy can implement functional data protection legislation without stifling innovation. The PDPA's enforcement mechanisms, including directions, financial penalties and private rights of action—offer a model for a resource-constrained jurisdiction. Pakistan's proposed Commission could adopt similar graduated enforcement powers.

Table 4: Observations

Feature	EU	UK	Singapore	Pakistan (proposed)
Data protection statute	GDPR (2016)	UK GDPR (2018)	PDPA (2012, amended 2020)	None enacted (2023 bill disposed; 2026 proposed)
AI-specific legislation	AI Act (2024)	Sectoral guidance	Model Framework (voluntary)	None (AI Policy 2025 only)
Independent regulator	European Data Protection Board	Information Commissioner's Office	Personal Data Protection Commission	Proposed Commission (not established)
Data subject rights	Comprehensive (access, correction, erasure, objection, portability)	Comprehensive	Moderate (access, correction, withdrawal)	Proposed in 2026 bill

Automated decision safeguards	Article 22 (right not to be subject)	Section 49 (similar)	Limited	Proposed (AI transparency)
Administrative penalties	Up to €35M/7% turnover	Up to £17.5M/4% turnover	Up to SGD 1M	Proposed
Private right of action	Yes (Art. 82)	Yes	Limited	Proposed
Surveillance oversight	LED, privacy Directive	Investigatory Powers Act 2016	Cybersecurity Act	IFTA 2013 (limited)

7. The Legislative Position in 2026

Stating the absence of an Act in the aggregate should be done delicately. The Personal Data Protection Bill, 2023 introduced concepts such as 'lawful and Fair Collection' and 'Purpose of Collection', which are familiar to the data-protection concept. It was introduced in the Senate on 13 February 2023. The bill was not passed or rejected by the committee, but and was disposed of as provided by the standing order of the Senate [13] as appears in the Senate's current bill summary. Merely being listed as an ongoing bill should not, therefore, be characterized as an "active pending bill" without qualification.

There was an alternate development in 2026. The Ministry of Information Technology and Telecommunication submitted the draft of a comprehensive Personal Data Protection Bill 2026 in a written reply before the National Assembly on 14th May 2026. The answer included a proposed framework of the National Commission for Personal Data Protection, right to erasure, right to learn about the use of personal data in AI systems, and regulations for transfer across borders and sensitive data [14]. These features will directly overcome some of the gaps discussed in this paper. However, the finalization is not necessarily Parliament's enactment. Citizens should not expect that the rights outlined in a bill until enacted into law and signed by the President will be legal rights.

The law is in a transitional state, therefore. While the general constitutional principles have progressed to more detailed policy commitments, it has been a long time since Pakistan achieved enforceable center. That divide is especially pronounced as the deployment of public and private AI grows at a rapid pace, and legal obligations are spread out across a litany of legislation designed to solve other issues.

8. Evaluating the Protection Gap

8.1 No comprehensive legality framework for processing

Collegiate Law relies on distinguishable concepts of authorized and unauthorized use, and fails to adequately circumscribe the admittedly more nebulous notion of lawful processing. Comprehensive legislation ought to mandate that every controller must have a lawful basis, include a clear purpose, gather minimal data as opposed to the more necessary, provide for accuracy, limit the retention of data, and ensure security for the data. These responsibilities must be observed in order to ensure such processing either by manual or automated means, whether the controller is public or private [20]. If there is no fundamental responsibility, then its legality becomes possession or nominal consent.

8.2 Inferred and biometric data

The AI systems generate information that is not provided by the person themselves. A model may be a model that derives a health status, political proclivity, economic vulnerability, or emotional condition, or even a network of connections and relationships from regular information. The current statutes of Pakistan are not explicit in providing that a sensitive inference shall receive the same level of protection as a sensitive fact it infers. Biometric data poses yet another risk: Face and fingerprint templates, iris and voice data are all identifiers that last a lifetime. If you're breached, it can affect you for the rest of your life. In the context of enhanced safeguards, strict necessity requirements, explicit statutory authority or narrowly limited consent, and independent impact assessment and powerful deletion rules must be added.

8.3 Automated decisions and the accountability gap

In the case of a decision that has a legal or otherwise significant effect, the decision maker ought to inform the affected person that the decision was generated through the use of automation, provide a meaningful explanation why automation was used, and provide for a human review. It doesn't have to include all the technical bottom line. It has to have sufficient information to evaluate accuracy, relevance, discrimination, and legal authority. There is no general right of this nature provided in the current system of Pakistan. The resulting accountability dilemma is that the institution can state that it is a problem with the model, the developer can claim that the data sent to the model is the problem, and the citizen can somewhat be unaware of who did the choosing [29-31].

8.4 Equality and group harms

Data protection is presented as a personal right, but there are some algorithmic systems that can end up being a burden on groups. Neighborhood and language and device type or education history may be a proxy for protected or socially vulnerable characteristics in a model. A class of persons cannot be excluded from the exception right through the system and therefore be saved by individual permission. Representative complaints, the equality impact assessments, and investigations where those are initiated by regulators are then essential supplements to individual rights to access.

8.5 Weak civil compensation and collective redress

It is challenging to value harm to data. Anxiety, loss of control, reputational risk or greater exposure could result in harm to a person without financial loss. Traditional damages laws might leave people with such injuries under-compensated, and in particular cases many people may be affected, but each has monetary losses measured in the hundreds of dollars. A dedicated statute ought to include the recognition of material / non-material damage, the inference of damage in suitable situations, the possibility of representative actions, and distribution of liability between the controllers and processors based on their role in the business. Compensation should be the primary action taken, and administrative penalties should be second.

Table 5: Gap analysis against a rights-based data protection regime.

Legal function	Present position	Required rule
Lawful basis and fair processing	Fragmented; PECA focuses on unauthorized or dishonest conduct	Express bases for processing; fairness; necessity and proportionality for public bodies
Purpose limitation and minimization	Not generally enforceable across sectors	Use data only for specified compatible purposes; collect minimum necessary data
Sensitive, biometric and inferred data	Sectoral and offence-based protection	Enhanced conditions, impact assessment, strict access and retention controls
Transparency and access	RTI regulates public disclosure; no universal data-subject access right	Notice, access, source disclosure, recipients and retention information
Correction, erasure and portability	Limited blocking/destruction remedies under PECA s. 14 and specific policy commitments	General enforceable rights with defined exceptions and deadlines
Automated decision-making	No general right to explanation, objection or human review	Notice of automation, meaningful reasons, review and contestability
Bias and equality assurance	Article 25 applies constitutionally; no routine algorithmic audit	Pre-deployment and periodic equality testing for high-impact systems
Breach notification	No universal cross-sector duty to notify regulator and affected persons	Risk-based notification with clear deadlines and mitigation duties
Independent regulator	Functions dispersed among sectoral bodies and courts	Independent commission with audit, order, penalty and guidance powers

Civil redress	Injunction, contract, defamation and constitutional routes are partial	Direct cause of action, material/non-material damages and representative claims

9. A Rights-Based Civil Law Framework for Pakistan

A good statute would be oriented towards the constitution and be more than administrative. They should exist to put in practice dignity, privacy, liberty, due process and equality and allow for legitimate innovation. The framework should be broadened to cover public bodies, companies, non-profit organizations, and processors, exceptionally, with specific care taken to clarify what is meant by "household activity", "journalism" and "research" and "national security". Exceptions must be limited, reviewable and should not be a nullification of the fundamental security, accountability and independent oversight obligations.

9.1 Core processing principles

Legality, fairness and transparency: every processing operation must have a defined legal basis and be communicated in clear language.

Purpose limitation: information collected for one purpose should not be used for an incompatible purpose without a new legal basis.

Data minimization and proportionality: public and private actors should use the least intrusive data and method reasonably capable of achieving the legitimate objective.

Accuracy and contestability: controllers should take reasonable steps to correct data and permit challenges to consequential inferences.

Storage limitation: retention periods should be defined, justified and auditable.

Security and accountability: controllers should maintain technical and organizational safeguards, processor contracts, logs and governance records.

9.2 Data-subject rights

The law should provide the rights to notice, access to information, correction, restriction, erasure, portability and objection. These rights should cover implied information and useful data as to who the source is, who the recipient was, when it was retained and for what purpose. Erasure should not be complete: There are exceptions to the erasure principle for lawful archives, freedom of expression and legal obligations and necessary public interest processing. The bottom line is that refusal needs to be accompanied by justification and be subject to review.

9.3 High-impact and automated decision systems

High impact should not be evaluated by brand but by consequence when it comes to AI. Improved responsibilities should be placed on systems which are effectively used in policing, identity, credit, insurance, employment, education, health and welfare, migration, utilities and essential public services. The institution in charge must carry out a data-protection and civil-rights impact assessment before deployment that includes the following: legal authority, necessity, affected groups and data quality, security, error rates, alternative methods and mitigation. A summary should be issued unless there is a narrow-cast secrecy ground.

Decisions by an automated process with legal or similarly consequential ramifications should not be imposed on anyone without authorization and protective measures. Such safeguards shall incorporate notice, an intelligible description of the factors which will be decisive, an opportunity to present opposing information, and for review by a person of actual authority to modify the effect. [20,31] There must be a way for public procurement contracts to allow the audit of the controls and ensure that as the vendors negotiate the terms of the contract there is no possibility that they can create the illusion of trade secrecy or obscure the rigidity of the accountability system for the public.

9.4 Surveillance-specific safeguards

The chapter on algorithmic surveillance by the State is a separate one. Although, in principle, targeted surveillance should be subject to prior authorization by a court, such provisions ought only to apply to very narrowly circumscribed emergencies, to be followed by speedy scrutiny. Warrants should, at the very least, specify the objective, sources of data, analytical technique, scope, length of time and conditions for sharing and deletion. Statutory authorization, parliamentary scrutiny and

independent technical audit should apply to bulk/population-level systems. It is recommended that the use of facial recognition in public places be restricted to specific instances of serious risks, and only as limited and short as they can be.

The practice of post-surveillance notice should move to become the exception, rather than the rule, after notification is no longer a clear threat to an investigation or national security. An illegal target will likely never discover the violation, and the proper to a remedy will not be exercised. Reporting should be made annually and show the total number of applications made, approved, and rejected, etc., categories of offences, duration and data destroyed, without giving any operational information.

9.5 Independent supervision and civil remedies

An independent National Commission for Personal Data Protection ought to be subject to the principles of security of tenure, financial autonomy, multidisciplinary competence and a territorial scope that covers both public and private controllers. Should set codes, hear complaints, conduct audits of its own motion, access or delete information, suspend illegal processing, and impose proportionate administrative fines and refer criminal activities. All of its decisions shall be reasoned, open to judicial review and published, with appropriate redactions.

Civil courts should clearly be able to make declarations, interim and permanent injunctions, corrections, erasures, accounts of profits as relevant, and damages for material and non-material damages. Representative complaints from established public-interest organizations and collective complaints in circumstances where collective action has the potential to address a multitude of people are types of complaints the statute should accommodate. Internal workings of a secret system need not be proved for a claimant to obtain a disclosure: recording logs, model documentation and impact statements may be preserved and controlled by courts and regulators.

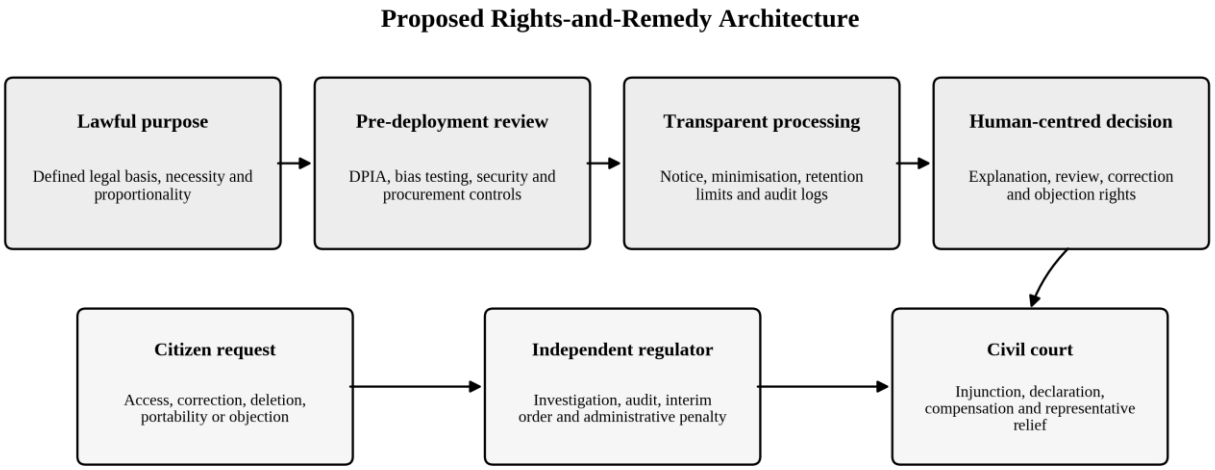


Figure 2: Proposed rights-and-remedy architecture for lawful AI processing and effective civil redress.

Table 6: Recommended statutory provisions and institutional responsibility.

Area	Minimum statutory content	Primary responsibility
Definitions	Personal, sensitive, biometric, inferred and de-identified data; controller, processor and high-impact AI	Parliament; regulator guidance
General duties	Lawful basis, fairness, purpose limitation, minimization, accuracy, security and retention	All controllers and processors
Public-sector processing	Express authority, necessity, proportionality, records of processing and procurement transparency	Public bodies; audit institutions
Automated decisions	Notice, meaningful explanation, correction, objection and human review	Deploying institution; vendor cooperation

Impact assessments	Mandatory before high-risk processing; publish non-sensitive summary; periodic reassessment	Controller; independent auditor; regulator
Biometric surveillance	Strict necessity; warrant or specific statutory authority; no indiscriminate continuous identification	Law-enforcement body; court; regulator
Children and vulnerable persons	Best-interests test, age-appropriate notices, restricted profiling and advertising	Controllers; regulator
Data breaches	Prompt regulator notification and affected-person notice where risk is significant	Controller and processor
Cross-border transfers	Adequacy, safeguards, enforceable rights and narrowly tailored localization for sensitive State data	Regulator; federal government
Remedies	Complaint, audit, interim order, injunction, erasure, compensation and representative action	Regulator and civil courts
Oversight of exemptions	Independent review, necessity records, sunset/review clauses and aggregate transparency	Courts, Parliament and regulator

10. Implementation Priorities

Is there a responsibility gap that can be filled only with legislation? Implementation to be staged starting with systems with the highest consequences. The first national inventory needs to include usage of high-impact AI by federal and provincial governments, a description of the legal authority, details on the types of data used, the vendor, deployment date, when the account will expire, and where complaints can be made. For a system with no clear purpose or owner, don't keep it going.

Second, of course, there is a need for the technical capacity of regulators and courts. As privacy disputes get more complex, data lineage, model documentation, security controls, and statistical evidence are paramount. Training at judicial academies and in the bar council, public prosecution, and civil service should be done to link these technical facts to well-known legal principles like relevance, reasonableness, proportionality, and burden of proof. Independent experts may be necessary, but expert help should be to comprehend the judicial task, not to supplant it.

Thirdly, public procurement should be a lever to control. Collaborate with courts and regulators; restrictions on vendor reuse, deletion on termination, incident reporting, accuracy and bias testing, and documentation should all be required of the contracts governing AI systems. A public authority cannot have its duty to uphold the Constitution outsourced. If there is inadequate transparency from the vendor, the system should not be used in decisions relating to rights.

Fourth, innovation should be allowed to take place by conducting trials and experiments within the framework. For regulatory sandboxes, one could imagine that they allow for testing, limited in time, using certain pre-defined datasets, participant protection, independent monitoring, and exit decision-making. A "Sandbox" should never be a space in which there is a lack of law. This is because the value of learning is exacerbated by a more rigorous view prior to the system being public.

Finally, reform must be Federally-led, but cooperative. Both data and AI systems span administrative jurisdictions and delivery may be at provincial or local levels. A sectoral state-level or provincial statute providing greater protection to the rights and transfers than the baseline provision could be enacted under a federal statute. Reduction of fragmentation by common technical standards and by having a streamlined and interoperable complaint process.

11. Conclusion: Implications for Responsible AI Governance

Pakistan is not a vacuum in itself. Dignity and the right to privacy of the home are guaranteed in Article 14, which creates a coherent civil-rights foundation with guarantees to life, liberty, due process, expression, information and equality. The judiciary have been grappling with whether constitutional privacy can be maintained outside of the home, as found in the treatment of unlawful monitoring with

telephones. Each of the provisions in PECA, the Investigation for Fair Trial Act, the Right of Access to Information Act and ordinary civil remedies provide valuable protection.

The problem is that these rules are for different questions. They can punish hacking, control specified interception, prevent record disclosure, prevent publication or compensate for contractual violations. They do not jointly form a full "personal-data processing law. In particular, they lack universal duties of purpose limitation and minimization, rights over inferred data and biometric information, protection for automated decisions, routine equality auditing, independent cross-sector supervision, notification of data breaches and a specific civil action for loss of control over personal information.

The policy guidance has now been focused. Ethical AI is acknowledged in the National AI Policy, 2025 and the Data Governance Policy, 2026. Thus, the executive's announcement of a comprehensive 2026 bill is important. But rights are real only as long as they are defined by Parliament, upheld by institutions and made effective by courts.

11.1 Implications for Policymakers

The analysis highlights for policymakers that the existing regulatory framework focusing on specific sectors is not sufficient to deal adequately with algorithmic surveillance. The implementation of an overarching Personal Data Protection Act is essential and should feature dedicated rules and obligations relating to AI and automated decision-making. The proposed Commission should be staffed with multiple disciplines beyond technical, legal and civil rights experts, as well as have financial and human resources. Pre-deployment impact assessments and measures that make it mandatory to publish tenderers and to make penalties commensurate to their impact should be built into legislation. The finalized bill for 2026 should be immediately provided to Parliament by the Executive, and Parliamentary committees should have expert inputs while analyzing the bill in detail.

11.2 Implications for Regulators

The framework indicates a need for a coordinated approach to its oversight regime, for regulators like the proposed Data Protection Commission, the Pakistan Telecommunication Authority and the Federal Investigation Agency. There is also a need to provide technical guidance, codes of practice for high-impact AI systems, and complaints handling processes for ordinary users to easily access. So Technical capacity-building is key; regulators need to be aware of data lineage, model documentation, bias testing and security controls to carry out a proper audit. There will need to be inter-register cooperation and MOUs to prevent the loss of fragments and forum-shopping.

11.3 Implications for Courts

In courts, the groundwork is already in place to extend privacy protections in the digital world. The rights protecting interim remedies provided by judicial interpretation of Article 14 and related provisions can be provided in advance of the enactment of legislation. Courts must be ready to impose impact assessment and provide explanations of automated decisions, and ensure compensation for non-material effects if the data processing is excessive and/or unlawful. Courts would have more assistance in assessing technical evidence and proportionality claims with judicial training in the implementation of AI and data protection at the Federal Judicial Academy. In addition, courts should relax standing requirements to allow for systemic algorithmic harms to be complained of in a public interest context.

11.4 Implications for AI Developers and Private-Sector Organizations

The uncertainty at the moment poses a danger and an opportunity to AI developers and other companies. This leaves you vulnerable to legal action; you could be sued in constitutional petitions, consumer-protection, defamation, or contractual cases. However, early adoption of good practices such as transparency about the use of AI, minimization of data, adequate human involvement, accuracy testing, and mechanisms that obtain consent can help to foster trust and decrease the cost of compliance later. Organizations should start performing voluntary privacy impact assessments, log data flows and decide on the model logic, and get vendor contracts to maintain audit rights. The proposed framework provides a clear pathway; businesses that develop sustainable and responsible

use of data nowadays will be stronger when the legislation is put into force.

11.5 Responsible AI Governance as a National Priority

The governance matters in the use of AI are not just a technical or legal issue they are a question of national policy and of democratic accountability. Policies and practices that involve algorithmic systems which impact access to credit, employment, welfare, healthcare, policing and migration must not be allowed to continue outside the limits of law. What Pakistan needs to do next is not to ban AI, but to draft a Technology-neutral AI policy in a state of fear for AI. It should be a "durable civil-law structure" that holds all powerful data processing to the law's standards: the necessity rule, proportionality, equality and respect for human dignity. The commitment to constitutionalism is clear, and the statute book has now to follow.

References

1. Constitution of the Islamic Republic of Pakistan, 1973, arts. 9, 10A, 14, 19, 19A and 25.
2. International Covenant on Civil and Political Rights, 1966, art. 17. Pakistan ratified the Covenant in 2010. Available from: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
3. United Nations. Universal Declaration of Human Rights. 1948; art. 12. Available from: https://www.un.org/en/about-us/universal-declaration-of-human-rights
4. Mohtarma Benazir Bhutto and others v President of Pakistan and others. PLD 1998 SC 388.
5. Pakistan Telecommunication (Re-organization) Act, 1996, s. 54. Available from: https://www.pta.gov.pk/media/telecom_act_1996.pdf
6. Investigation for Fair Trial Act, 2013, ss. 8-14, 27, 29, 34 and 35. Available from: https://www.na.gov.pk/uploads/documents/1385547808_508.pdf
7. Prevention of Electronic Crimes Act, 2016 (Act XL of 2016), as amended, ss. 3-5, 14, 17-19 and 36. Available from: https://www.nacta.gov.pk/wp-content/uploads/2020/05/PECA-2016.pdf
8. Right of Access to Information Act, 2017, ss. 7(g)-(h) and 16(c). Available from: https://www.na.gov.pk/uploads/documents/1506079961_175.pdf
9. National Database and Registration Authority Ordinance, 2000. Available from: https://www.nadra.gov.pk/wp-content/uploads/2020/04/NADRA-Ordinance-2000.pdf
10. Digital Nation Pakistan Act, 2025 (Act I of 2025).
11. Ministry of Information Technology and Telecommunication. National Artificial Intelligence Policy. Islamabad: Government of Pakistan; 2025. Available from: https://moitt.gov.pk/national-ai-policy
12. Ministry of Information Technology and Telecommunication. National Data Governance Policy. Islamabad: Government of Pakistan; 2026. Available from: https://moitt.gov.pk/data-governance-policy
13. Senate of Pakistan. The Personal Data Protection Bill, 2023: Bill Summary and Legislative Status. Islamabad: Senate Secretariat; status accessed 12 June 2026. Available from: https://www.senate.gov.pk/legislation
14. National Assembly of Pakistan. Written reply concerning safeguarding privacy and digital rights, including the proposed Personal Data Protection Act 2026. Proceedings dated 14 May 2026. Available from: https://www.na.gov.pk/proceedings
15. Specific Relief Act, 1877, ss. 52-55.
16. Code of Civil Procedure, 1908, s. 9, s. 151 and Order XXXIX, rr. 1-2.
17. Contract Act, 1872, s. 73.
18. Defamation Ordinance, 2002, ss. 3, 8 and 9.
19. Qanun-e-Shahadat Order, 1984, art. 164.
20. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 5-6, 9, 12-22, 25, 32, 35 and 82. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj
21. European Union. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Available from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
22. Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence. Paris: OECD; 2019, updated 2024. Available from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
23. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO; 2021. Available from: https://unesdoc.unesco.org/ark:/48223/pf0000381137
24. Solove DJ. A taxonomy of privacy. University of Pennsylvania Law Review. 2006;154(3):477-564. doi:10.2307/25041270
25. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press; 2010. doi:10.1515/9780804772891
26. Richards NM. The dangers of surveillance. Harvard Law Review. 2013;126:1934-1965. Available from: https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/
27. Zuboff S. The Age of Surveillance Capitalism. New York: PublicAffairs; 2019.
28. Barocas S, Selbst AD. Big data's disparate impact. California Law Review. 2016;104(3):671-732. doi:10.15779/Z38BG31
29. Citron DK, Pasquale F. The scored society: due process for automated predictions. Washington Law Review. 2014;89:1-33. Available from: https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2/
30. Selbst AD, Boyd D, Friedler SA, Venkatasubramanian S, Vertesi J. Fairness and abstraction in sociotechnical systems. Proceedings of FAT*. 2019:59-68. doi:10.1145/3287560.3287598
31. Wachter S, Mittelstadt B, Floridi L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law. 2017;7(2):76-99. doi:10.1093/idpl/ipx005
32. Kelly CJ, Karthikesalingam A, Suleyman M, Corrado G, King D. Key challenges for delivering clinical impact with artificial intelligence. BMC Medicine. 2019;17:195. doi:10.1186/s12916-019-1426-2
33. Mantelero A. AI and big data: a blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review. 2018;34(4):754-772. doi:10.1016/j.clsr.2018.05.017
34. United Nations Human Rights Committee. General Comment No. 16: Article 17 - Right to Privacy. 1988. Available from: https://www.refworld.org/docid/453883f922.html
35. Office of the United Nations High Commissioner for Human Rights. The right to privacy in the digital age. UN Doc A/HRC/48/31. 2021. Available from: https://undocs.org/A/HRC/48/31
36. United Nations. Guiding Principles on Business and Human Rights. New York and Geneva: United Nations; 2011. Available from: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
37. Qazi R. Ethical deliberations in artificial intelligence. Innovative Research Journal of Artificial Intelligence. 2025;3(2):1-9. Available from: https://irjpl.org/irjai/article/view/240
38. Floridi L, Cowls J. A unified framework of five principles for AI in society. Harvard Data Science Review. 2019;1(1). doi:10.1162/99608f92.8cd550d1
39. Radanliev P, Santos O, Jones A, Joinson A. Ethics and responsible AI deployment. Frontiers in Artificial Intelligence. 2024. doi:10.3389/frai.2024.1234567

Disclaimer: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.