



RESEARCH PAPER

Digital Government Readiness and Legal Preparedness for Artificial Intelligence Adoption in Pakistan's Public Sector

¹Saad Bin Sarfraz and ²Seerat Fatima

1. MPhil Public Policy, Centre for Public Policy and Governance (CPPG), Forman Christian College (A Chartered University), Lahore, Pakistan
2. BA-LL.B (Honours), The Shaikh Ahmad Hassan School of Law (SAHSOL), Lahore University of Management Sciences (LUMS), Lahore, Pakistan

***Corresponding Author:** saadchaudhry144@gmail.com

ABSTRACT

This paper assesses whether Pakistan's public sector has adequate digital governance and legal preparedness to responsibly deploy artificial intelligence (AI). Pakistan has articulated digital transformation goals in the Digital Pakistan Policy (2018) and Draft National AI Policy (2023), yet institutional and legal readiness lags. Using a qualitative assessment of policies, laws, and peer-reviewed research, the paper examines Pakistan across four interdependent dimensions: digital government readiness, institutional capacity, legal preparedness, and governance and accountability. Pakistan has developed identity infrastructure through NADRA and articulated a coherent digital governance vision, but lacks institutional coordination and legal frameworks for responsible AI deployment. The Prevention of Electronic Crimes Act (2016) omits algorithmic accountability, the Personal Data Protection Bill (2023) remains unenacted, and no independent oversight body specifically mandated to oversee public-sector AI exists. Key recommendations include enacting the Personal Data Protection Bill, expanding its Commission's mandate to cover algorithmic decisions, consolidating coordination under one institution, and publishing a public AI registry.

KEYWORDS Digital Government, Artificial Intelligence Governance, Legal Preparedness, Institutional Capacity, Data Protection, Administrative Law, Pakistan Public Administration

Introduction

Artificial intelligence has evolved from an experimental technology into an increasingly important instrument of public administration. It influences the way the state conducts public service, distributes resources, and makes decisions about the welfare of the people (Wirtz et al., 2019; Zuiderwijk et al., 2021). Across jurisdictions, AI is increasingly adopted to improve administrative efficiency, reduce discretion-based corruption, and deliver more responsive public services (Wirtz et al., 2019). Yet these potential benefits obscure a more fundamental question: Are there proper institutional and legal frameworks in place to use such tools?

Pakistan's public sector has pursued digital transformation intermittently since the early 2000s, up until the formulation of the Digital Pakistan Policy of 2018, where digitalization was positioned as a central pillar to economic competitiveness and public service delivery (Government of Pakistan, Ministry of Information Technology and Telecommunication n.d.). In more recent times, the Ministry of Information Technology and Telecommunications (MoITT) issued a Draft National Artificial Intelligence Policy in May 2023 for public consultation, marking the government's attempt to harness AI in order to aid national development (Government of Pakistan, Ministry of Information Technology and Telecommunication, n.d.). Nevertheless, policy ambition has consistently outpaced institutional and legal preparedness in the path of digital governance in Pakistan (Nazeer & Gil, 2023), and AI governance appears unlikely to depart from this broader institutional

pattern. A persistent gap in previous assessments, both in Pakistan and elsewhere, is the tendency of assessing preparedness using digital infrastructure alone, neglecting the role of institutional coordination (Fukuyama, 2017; Migdal, 1988) and legal instruments (Yeung, 2018) that enable responsible utilization of such infrastructure.

This article addresses three research questions. Firstly, to what extent are Pakistani public sector institutions ready for AI adoption, in terms of their technological infrastructure, manpower, and organizational readiness? Secondly, is the existing legal and regulatory regime in Pakistan, which includes cybercrimes laws, data protection laws, constitutional provisions, and e-governance laws, sufficient to ensure responsible AI implementation in the government sector? Lastly, what changes need to be brought about before the adoption of AI?

This paper contributes in three ways. First, it synthesizes two distinct public administration and technology law lenses that are often examined in isolation in the literature on AI governance: how administrative capacity (Fukuyama, 2017) and legal enforceability (Yeung, 2018; Levi-Faur, 2013) determine, rather than independently predict, readiness. Second, it proposes a four-dimensional interactive framework which includes digital government readiness, institutional capacity, legal preparedness, and governance and accountability. It is derived from Janowski (2015), Fukuyama (2017), and Gasser & Almeida (2017) and applies it to Pakistan through the analysis of verified government documents rather than hypothetical scenarios. Third, it provides a sequence of policy suggestions based on Pakistan's institutional reality, demonstrating why legal and coordinating efforts should come before infrastructure and enabling measures, in line with the sequence outlined by Gasser & Almeida (2017) and UNESCO (2021).

Literature Review

Digital Government and State Capacity

The development of digital government has been explained using different stage models over time; starting with the four stages of cataloging, transaction, vertical integration, and horizontal integration of government services by Layne and Lee (2001). Subsequent studies including the digital government evolution model by Janowski (2015) have elaborated on this process to include contextualization and personalization of government services and thus making digitalization a part of public sector reform in general and not a technological activity alone. The idea of Digital Era Governance as proposed by Dunleavy et al. (2006) has highlighted the fact that digitalization is a step away from New Public Management and involves reintegration of agencies, needs-based holism, and digitalization of administration.

These perspectives support the central argument of this article that digital government maturity is determined more by the administrative capacity of its coordination rather than the presence of technology itself (Dunleavy et al., 2006; Janowski, 2015). State building research conducted by Fukuyama (2017) identifies two factors, which are scope and strength of governmental institutions, with the former being more associated with governmental functions. According to his research, expanding governmental functions without increasing its strength will lead to weak governance outcomes. The research conducted by Migdal (1988) concerning state capacity was similar to this one and showed that even though there might be formal state authority, there would still be no effective implementation of any policy due to its low administrative capacity. The same can be applied to the process of AI implementation, because expanding the scope of automation without increasing the strength of governmental institutions will lead to an unreliable outcome regardless of the technical progress (Fukuyama, 2017; Migdal, 1988).

Regulatory governance literature provides another perspective on this issue. According to Levi-Faur (2013), the theory of regulatory governance highlights the fact that successful regulation requires a well-established ability to make rules, monitor activities, and enforce sanctions that is not tied to the institutions that are being regulated, which becomes especially important in case where the government becomes the agent of regulation and the user of AI tools.

Artificial Intelligence in Public Administration

Recent scholarship has examined the implications of AI for government in particular. Specifically, Wirtz et al. (2019) have considered the uses and issues related to the application of AI in government organizations, with data availability, technical proficiency, and organizational preparedness being some of the barriers to adoption identified in such settings. Likewise, Zuiderwijk et al. (2021) have investigated the implications of applying AI technologies in public governance, noting that AI technologies lacking necessary transparency measures could negatively affect public trust in situations when citizens are unable to challenge automation-based decisions. Yeung's (2018) arguments regarding algorithmic regulation have also drawn attention to the conflict of interests associated with the implementation of automated governance and procedural requirements in public administration.

At the international policy level, the recommendation by the OECD (2019) in terms of "the Council on Artificial Intelligence" emphasized principles of transparency, accountability, and human oversight to serve as guiding rules for member and non-member countries in the governance of AI, whereas the "Recommendation on the Ethics of Artificial Intelligence" by UNESCO (2021) introduced similar principles while explicitly considering issues related to human rights and the developing countries. Floridi et al. (2018) suggested an AI4People model in which beneficence, non-maleficence, autonomy, justice, and explicability were suggested as fundamental principles of AI governance, all of which have been followed by various nations in their national AI strategy (OECD, 2019; UNESCO, 2021). In addition, Gasser and Almeida (2017) recommended a model of three-tiered governance of AI that includes technical, ethical, and social tiers of AI governance; it was argued that development of legal and regulatory framework should be concurrent to that of technical abilities.

Pakistan-Specific Literature

Research regarding Pakistan's AI policy governance readiness is relatively scarce but insightful. For example, Nazeer & Gil (2023) have investigated the issues related to the implementation of artificial intelligence technology by government agencies in Pakistan, suggesting institutional fragmentation, technological constraints, and lack of regulatory frameworks as key impediments to responsible integration. Indeed, this result is in line with previous research regarding Pakistan's progress towards e-governance, which has traditionally been marked by a number of donor-led pilots unable to be scaled up (Nazeer & Gil, 2023).

Existing commentaries on the draft national AI policy itself have been largely negative about the policy's consultative and implementation process. It has been highlighted that the policy document sought public opinion without engaging stakeholders in the policy drafting process as advocated by best practices globally and that it includes some unrealistic objectives, such as workforce upskilling and establishment of National AI Fund, without a clear roadmap. Such a trend is reflective of the Digital Pakistan Policy 2018 as well, which had some innovative ideas and e-government goals but were implemented unevenly in the federal ministries and provinces (Nazeer & Gil, 2023).

This research finds that the governance of artificial intelligence in Pakistan is an issue that does not pertain mainly to technology, but institutionally and legally, relating to the ability of governmental institutions to coordinate the implementation of policy (Fukuyama, 2017) and having access to legal tools able to control and steer the process of algorithmic decision making in the government context (Yeung, 2018). What has been overlooked by the existing literature and is attempted in this article is to bring these two observations into one cohesive framework through which to examine Pakistan's institutional and legal experience.

This study employs an approach that combines four dimensions of analysis based on the theories of state capacity (Fukuyama, 2017; Migdal, 1988), digital age governance (Dunleavy et al., 2006; Janowski, 2015), and the literature on technology law concerning algorithmic accountability (Yeung, 2018; Gasser & Almeida, 2017). The multidimensional analysis differs from traditional AI readiness indexes that tend to combine measures related to infrastructure, skills, and policies into a single index, because the four dimensions are seen as necessary in combination rather than substitutable. In other words, the state can have good digital infrastructure but be ill-prepared to employ responsible AI unless there is legal enforcement or institutional coordination in place. At the same time, legal design cannot replace institutional capacity or digital infrastructure.

Digital Government Readiness refers to the technological and infrastructural platform necessary for providing digitalized public services including connectivity, interoperability of government databases and digital identification. Digital Government Readiness is based on the stage models provided by Layne and Lee (2001) and Janowski (2015) and represents the precondition for AI readiness.

Institutional Capacity encompasses both Fukuyama's (2017) concept of scope and strength of state functions and Migdal's (1988) concept of state capacity as the one that depends on implementation and refers to the administrative capacities, coordination mechanisms and human resources of public organizations needed for implementation of digital and AI policies at the ministry level and beyond.

Legal Preparedness is connected to the presence of tools for data processing, decision-making algorithm control and cybersecurity risk management related to AI systems in government through the use of enforceable legal instruments and constitutions and regulatory bodies. The concept is rooted in technology law literature (Yeung (2018), Levi-Faur (2013)) and the layered governance model proposed by Gasser and Almeida (2017).

Governance and Accountability refer to the presence of oversight structures, transparency responsibilities, and redress channels available to individuals affected by AI-powered decisions, in accordance with the guidelines provided in the OECD (2019) Recommendation on Artificial Intelligence and the UNESCO (2021) Recommendation on the Ethics of Artificial Intelligence, along with the provisions of administrative law of procedural justice as provided for under the Constitution of the Islamic Republic of Pakistan (1973).

The framework treats these dimensions as mutually reinforcing. The deficiencies in institutional capacity hinder the process of implementing legal instruments (Fukuyama, 2017), whereas the lack of legal readiness prevents whatever the governance and accountability measures could deliver despite whatever infrastructure exists (Yeung, 2018). This interdependence distinguishes the proposed framework from conventional readiness assessments where infrastructure, skills, and regulation are considered separately and independently improvable.

Rather than treating these dimensions as independent variables contributing separately to AI readiness, this study conceptualizes them as interdependent governance

conditions whose interaction determines the state's capacity to deploy AI responsibly. The framework therefore serves not only as an analytical tool for assessing Pakistan's current position but also as a theoretical lens for explaining why progress in one dimension cannot compensate for deficiencies in another. This interactional perspective constitutes the principal analytical contribution of the study.

Material and Methods

This study employs qualitative documentary analysis of primary legal and policy documents together with secondary academic literature published up to September 2024. Primary sources consist of legislative and policy papers issued by the Government of Pakistan, such as the Constitution of the Islamic Republic of Pakistan (1973), Prevention of Electronic Crimes Act (2016), Right of Access to Information Act (2017), Digital Pakistan Policy (Government of Pakistan, Ministry of Information Technology and Telecommunication n.d.), Removal and Blocking of Unlawful Online Content Rules 2021 (Pakistan Telecommunication Authority, 2021), National Cyber Security Policy 2021 (Government of Pakistan, Ministry of Information Technology and Telecommunication, 2021), Draft National AI Policy (Government of Pakistan, Ministry of Information Technology and Telecommunication, n.d.), and Personal Data Protection Bill (Senate of Pakistan, 2023). Secondary sources include reports on digital government and AI governance from the OECD (2019) and UNESCO (2021). In addition, the peer-reviewed academic literature on digital government (Dunleavy et al., 2006; Janowski, 2015; Layne & Lee, 2001), public administration (Fukuyama, 2017; Migdal, 1988; Wirtz et al., 2019), and technology law (Yeung, 2018; Levi-Faur, 2013; Gasser & Almeida, 2017) were utilized.

The documents have been analyzed on the basis of four dimensions of the analytical framework. The emphasis was on the interaction between dimensions rather than their standalone assessment. The analysis is based on documentary analysis and literature review. This methodology is in accordance with the accepted qualitative policy analysis methodology that is used for institution and law-based analysis, particularly when there is no systematic primary data regarding government's use of AI in Pakistan

Results and Discussion

The following analysis applies the proposed four-dimensional framework to Pakistan's public sector. Rather than evaluating each dimension in isolation, the discussion emphasizes how interactions among digital government readiness, institutional capacity, legal preparedness, and governance and accountability collectively shape the country's readiness for responsible AI adoption. Throughout the analysis, evidence is interpreted through this interactional framework rather than as a descriptive assessment of individual policy domains.

Digital Government Readiness

The digital governance approach of Pakistan has been substantially shaped by the Digital Pakistan Policy 2018, released by the Ministry of Information Technology and Telecommunication (Government of Pakistan, Ministry of Information Technology and Telecommunication n.d.). Five major pillars were identified under this initiative that include access, digital infrastructure, e-government, digital skills, and innovation to help the country move towards an integrated digital economy (Government of Pakistan, Ministry of Information Technology and Telecommunication n.d.). One of the objectives of this strategy is the encouragement of innovation hubs for new technologies such as artificial intelligence, robotics, Internet of things, and to foster the startup environment in the country (Government of Pakistan, Ministry of Information Technology and Telecommunication n.d.).

Despite these institutional arrangements, its implementation has been rather uneven (Nazeer & Gil, 2023). Service delivery in the country still suffers from fragmented digital systems in federal, provincial, and local government. Hence, interoperability across government agencies remains uneven and fragmented (Nazeer & Gil, 2023). The biometric identity database system of NADRA is arguably one of the most developed parts of the digital government structure in Pakistan and was used to deliver services in social protection programs, but its use in relation to other government data systems useful for AI, such as those related to health, education, or judiciary, has been insufficient (Government of Pakistan, Ministry of Information Technology and Telecommunication n.d.).

This pattern reflects the trend found in the digital government literature that involves investment in infrastructures for flagship applications while remaining weak in terms of horizontal integration throughout the bureaucratic structure (Dunleavy et al., 2006). As per Janowski's (2015) evolutionary typology, the digital government maturity in the case of Pakistan seems limited to transactional digitization in selected high-profile areas like identity registration and filing taxes, and has not yet developed into contextualization and cross-organizational integration necessary for application of AI in contexts of service delivery, and automated eligibility checks, respectively (Janowski, 2015; Layne & Lee, 2001). These findings indicate the interactivity feature of the framework because there is infrastructural maturity in one field but legal and institutional immaturity in another, which means the first cannot replace the second (Fukuyama, 2017). Without integration and proper data governance policies, AI applications in government would run on incomplete and poorly-governed data, which could reduce the reliability and defensibility of the technology (Zuiderwijk et al., 2021; Yeung, 2018).

Institutional Capacity

Institutional capacity for the use of AI refers not just to having the technological know-how, but also to the means of coordinating the efforts to turn the policies into consistent administrative actions (Fukuyama, 2017; Migdal, 1988). At present, the institutional infrastructure of Pakistan for the purposes of digital and AI governance appears institutionally fragmented between various institutions. The Ministry of Information Technology and Telecommunication is the institution responsible for formulating policy in the area of digital transformation and has spearheaded the efforts to formulate both the Digital Pakistan Policy and the Draft National AI Policy (Government of Pakistan, Ministry of Information Technology and Telecommunication, n.d.). Nonetheless, there have been other players in the field as well, such as the Ministry of Planning, Development and Special Initiatives.

Fragmentation is not only an issue that creates administrative hurdles but also has significant consequences in terms of regulatory governance. According to Levi-Faur's (2013) conceptual framework for regulatory governance, a well-governed institution needs to have a well-established institutional capacity that holds the legitimacy and capacity to develop and enforce standards. When the responsibilities for the standards for data, cybersecurity, and policies related to artificial intelligence lie with different ministries without a coordinating lead, the regulatory governance mechanism is unable to impose any consistency in terms of the standards for the quality of data, testing of algorithms, and risk assessment of artificial intelligence in the public sector, and accountability becomes significantly diffused if these standards were violated (Levi-Faur, 2013). According to Nazeer and Gil (2023), fragmented mandate and insufficient technical capacity among the civil service cadres were identified as main hindrances to the implementation of AI, rather than lack of technology.

The civil service capacity is another aspect of institutional preparedness, with an institutional history peculiar to Pakistan. The civil service recruitment and training system in Pakistan is geared towards developing generic administrative skills rather than

developing digital and data governance skills. It is a practice with origins in the administrative design of colonial rule that has proved resilient in spite of various reforms to the civil service structure (Husain, 2018). Such a focus on developing generic administrative skills means that civil servants who are moved from one non-related job posting to another find themselves ill-suited to gain the specialized skills needed to regulate, audit, or challenge the output of the algorithmic systems (Wirtz et al., 2019). This concern is noted in the Draft National AI Policy, which calls for awareness and training programs for civil servants on AI and data protection skills, targeting all civil servants by 2025 (Government of Pakistan, Ministry of Information Technology and Telecommunication, n.d.).

Nevertheless, the policy document fails to identify the budget required for its implementation, the lead government agency responsible for its curriculum, and the verification process of adoption. It raises questions regarding the past digital governance frameworks in Pakistan, whether the set target is realistic in the given time frame (Nazeer & Gil, 2023). Without these administrative resources, even an effective legal structure for the regulation of AI will experience the implementation gap that repeatedly faced Pakistan's regulatory agencies in the past (Fukuyama, 2017; Levi-Faur, 2013).

Legal Preparedness

The aspect that stands out as having the most substantial weakness when it comes to preparation for responsible implementation of AI in government by Pakistan is legal preparedness. This is an instance where there is maximum importance of the intersection of legal form and institutional capacity (Yeung, 2018). The legal system in Pakistan that concerns digital governance has been largely created to cater to cybercrime and content regulation rather than algorithmic governance or automated decision-making and processing of information.

The courts of Pakistan have read the right to privacy into Article 14 of the Constitution which guarantees dignity and privacy as going beyond the physical privacy of one's own house to include informational privacy (The Constitution of the Islamic Republic of Pakistan, 1973). It is a constitutional base from which the legality of the government AI systems could be reviewed if they process information without proper safeguards in place. The right to a fair trial in the determination of civil rights and obligations as guaranteed under Article 10-A of the Constitution introduced by the Eighteenth Amendment in 2010 (The Constitution of the Islamic Republic of Pakistan, 1973) also applies to the proceedings of administrative tribunals and other public authorities making decisions about the citizens' rights.

Where automated systems decide whether someone is eligible for a public benefit, deny someone services, or single out an individual for further scrutiny, it may reasonably be argued that the right to a fair hearing provision in Article 10-A may be interpreted as requiring that the affected individual gets proper notice and the chance to defend himself or herself in a meaningful way, which means that the decision being made needs to be understandable. Currently, there is no legislative provision for the constitutional principle of right to an explanation of a decision based on automated systems in Pakistan, as the concept is only present at the level of constitutional doctrine and cannot be effectively operationalized within the realm of governmental automation. The right to information provided by Article 19A constitutes another example of a constitutional principle, while the Right of Access to Information Act of 2017 implements it.

The principles of administrative law, such as the rule that public agencies have to perform their tasks in accordance with powers delegated to them by statute and should exercise discretion properly, are affected by the possibility of AI-based decision-making processes (Yeung, 2018). In case where the statute gives a discretionary power to be exercised by the particular individual or body, the actual delegation of the discretionary

power to an automated process raises unresolved questions under Pakistani administrative law as to whether or not this delegation is possible without clear statutory provision and, furthermore, who will be responsible legally in case an automated recommendation is accepted without proper human consideration (Yeung, 2018; Zuiderwijk et al., 2021). These issues remain unaddressed in any Pakistani legislation passed to date and also in the case law as of September 2024, creating a substantive gap between principles of constitutionality and administrative law that could, in theory, limit improper AI use and practical means to make those principles work.

The Prevention of Electronic Crimes Act (2016) continues to be the main legislative framework regulating cybercrime in Pakistan. It provides provisions related to the prohibition of unauthorized access to information systems and cyberterrorism, among others. Despite the fact that the PECA Act defines several cybersecurity offences and authorizes the Pakistan Telecommunications Authority to tackle the problem of unlawful content online, the said legislation was not created to regulate the processing of personal data with the use of automated systems; it does not contain any provisions concerning the transparency of algorithms, algorithmic bias, and accountability of algorithms' decisions (Pakistan, 2016).

The absence of data protection legislation continues to persist in Pakistan. First proposed as a bill in 2020, this has undergone subsequent modifications, resulting in a new version of the Personal Data Protection Bill 2023, which includes the establishment of the National Commission for Personal Data Protection (NCPDP), whose mandate will be the supervision of data controllers and processors, along with issues such as consent, data breach notification, and prohibitions for cross-border transfers (Senate of Pakistan, 2023). As of September 2024, the Bill had yet to be enacted into law through the passage of Parliament, thereby failing to provide Pakistan with a legal regime that would regulate the collection, processing, and retention of personal data (Senate of Pakistan, 2023). This omission is particularly significant in the context of AI governance, where machine learning systems used in public administrations for decision-making around access to services or fraud detection involve massive data processing of citizens.

In the absence of a data protection law and a supervisory commission, there are no legislative measures requiring government organizations to carry out data protection impact assessment, confining data processing within designated purposes, or giving individuals the option to challenge automatic decision-making based on their personal data (Senate of Pakistan, 2023; OECD, 2019). Purpose limitation and proportionality being absent in enforceable forms are also important from the perspective of administrative law because these doctrines usually prevent public entities from processing any data which is not essential for performing a particular statutory function, and in the absence of a data protection law, the requirement only exists in the unenforceable form of a constitutional provision (The Constitution of the Islamic Republic of Pakistan, 1973). The National Cyber Security Policy 2021 ensures the protection of Critical Information Infrastructure and provides a governance framework for national cyber security that includes measures pertinent to protecting government information systems from attacks (Government of Pakistan, Ministry of Information Technology and Telecommunication, 2021). Although it improves the preparedness of one aspect of law related to AI, which is ensuring the security of the infrastructure on which data operates, it does not take into account the issues faced due to the nature of algorithms themselves such as biases, explainability, and liability for automated errors in decisions that affect citizens.

The Draft National AI Policy, released for consultations by MoITT in May 2023, is the primary policy instrument in Pakistan regarding the governance of AI (Government of Pakistan, Ministry of Information Technology and Telecommunication, n.d.). The draft has established its goals through several pillars, which include awareness and readiness, market enablement, and the creation of a progressive and trustworthy regulatory environment for

AI (Government of Pakistan, Ministry of Information Technology and Telecommunication, n.d.).

The Right of Access to Information Act (2017) offers a partial supplement to this scheme by providing the right to access records held by public authorities of the federal government, provided certain exemptions. While theoretically, this Act can help achieve transparency in government use of algorithmic technologies, since people would be able to access information about criteria and data behind automated decisions made, this particular Act was not adopted taking into account the need to provide for algorithmic transparency, and the exceptions include those connected with the issues of national security and policy-making which may be extensively used by the public authorities to deny the information regarding AI systems (Pakistan, 2017). Furthermore, while there is no general requirement for public authorities to state their reasons for administrative decisions imposed on the citizens in statute in Pakistan, such duty does exist in some comparable jurisdictions.

It is meant to be the eventual creation of ethics frameworks and a regulatory regime for AI. Nonetheless, as a non-binding policy instrument, it lacks any legal binding power, and even its wording recognizes the lack of any dedicated AI regulatory regime in Pakistan when it was formulated (Government of Pakistan, Ministry of Information Technology and Telecommunication, n.d.). Sector-specific laws, such as the National Cyber Security Policy 2021 and the cloud computing policy of Pakistan, mentioned in relation to AI risk management, were not conceived in view of promoting algorithmic accountability as a key purpose, hence keeping the legal preparation of AI in Pakistan on a pre-regulatory footing, based on constitutional provisions only.

Governance and Accountability

Accountability and governance structures for AI in the public sector of Pakistan remain largely underdeveloped in practice. No independent regulatory body has been established that is authorized to regulate algorithmic systems deployed by the government and to ensure that these algorithms are fair and reliable. It will be responsible for receiving and deciding citizen complaints about the automated administrative decision-making system. The National Commission for Personal Data Protection, which was suggested under the draft 2023 Personal Data Protection Bill, would constitute the closest equivalent to the regulatory body; however, the Bill must first be passed by the parliament, which it had not been as of September 2024.

Administrative laws and remedies for judicial review of administrative actions and the institution of ombudsmen in Pakistan serve as generalized means for contesting administrative acts which are arbitrary or unreasonable. However, these remedies have not taken into consideration the peculiarities of algorithmic decision-making and, therefore, do not solve certain issues associated with it, such as the difficulty faced by the citizens to ascertain whether a negative decision was made automatically and to get an intelligible explanation for the decision (Yeung, 2018; Zuiderwijk et al., 2021). The explicability principle of the AI4People framework (Floridi et al., 2018) and also OECD (2019) and UNESCO (2021) frameworks assume that the persons affected have access to the intelligible explanation of the automated decisions, which is not currently required of the Pakistani authorities despite their ability to fulfill such a requirement in light of the due process under Article 10-A (The Constitution of the Islamic Republic of Pakistan, 1973).

Government transparency on the use of AI technology is equally inadequate. There is no public record of AI systems used by any federal or provincial government organization in Pakistan, unlike in other jurisdictions, where there has been the recent emergence of the practice of publicly registering algorithms used by governments for automated decision-making processes (OECD, 2019). This lack of transparency not only limits public oversight but also academic and civil society evaluation that would otherwise enhance evidence-

based policy development (Zuiderwijk et al., 2021). Consequently, the role of the ombudsman and judicial review systems are inherently ineffective tools for accountability because neither of them can operate against an undisclosed use of automation in any particular decision affecting the concerned citizen (Yeung, 2018).

The cross-dimension analysis demonstrates that in Pakistan's case, there has been an ongoing tendency towards making digital governance ambitions more pronounced as compared to creating institutions and legislation for their proper realization (Nazeer & Gil, 2023). This is not a unique trend related only to the governance of AI technologies. Rather, it is a feature of Pakistan's public sector development which was characterized by the formulation of ambitious goals outlined in policies which faced later implementation challenges due to institutional disintegration and lack of resources (Fukuyama, 2017; Nazeer & Gil, 2023).

The interaction among these four dimensions explains why it is essential to understanding why partial success in one dimension cannot be translated into readiness on an overall basis, and it is this aspect that distinguishes the framework used in this paper from other approaches to measuring AI readiness. Composite measures used in comparative digital government research usually treat infrastructure, capabilities, and policy as separately weighted dimensions adding up to overall readiness (Janowski, 2015). In the case of Pakistan, this approach would certainly highlight the fact of some significant achievements, such as the biometric infrastructure developed by NADRA and the presence of both the Digital Pakistan Policy and the Draft National AI Policy (Government of Pakistan, Ministry of Information Technology and Telecommunication, n.d.), while overlooking the actual unreadiness revealed in this paper. Digital government readiness, represented by the NADRA system infrastructure, has made greater progress compared to legal and institutional arrangements necessary for the governance of its expansion into AI-powered solutions. The institutional capacity shortcomings, especially overlapping responsibilities of different ministers and lack of specialized knowledge among bureaucrats who have the generalist nature of civil servants, imply that even if there was some legal arrangement like the Personal Data Protection Bill passed into law, its successful implementation and enforcement was not assured without an adequately resourced and independent regulatory agency (Fukuyama, 2017; Levi-Faur, 2013). Legal readiness cannot make up for institutional capacity weaknesses because laws cannot ensure compliance without the administrative capacity necessary to enforce them (Levi-Faur, 2013). It is the key point of the analysis in the article where it is argued that the readiness assessment should be done in terms of the minimum, rather than average, across all four dimensions because the weakest one defines the actual readiness for responsible use (Gasser & Almeida, 2017).

This finding is particularly important in regards to accountability. Algorithmic systems that are implemented in public administration without any data protection laws being enacted, an oversight commission, and standard administrative procedures for making automated decisions would put the Pakistani public administration in a much more disadvantaged position than that envisaged by the international frameworks like the OECD (2019) AI Recommendation. The danger here is not just technical malfunction but the overall undermining of the credibility of digital government (Zuiderwijk et al., 2021), especially considering the fact that AI-assisted service delivery would primarily affect those areas of public administration where errors can have direct implications for the rights and entitlements guaranteed by the Constitution under Articles 10-A, 14, and 19A.

A further consideration concerns policy sequencing. The international framework, such as UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021), states that the process of setting up frameworks must take place before, or at least simultaneously with, the use of artificial intelligence technology, not after. The case of Pakistan, whereby the Draft National AI Policy is setting ambitious objectives for enabling its artificial intelligence

market, but the foundation law Personal Data Protection Bill has yet to be passed, represents an example of an inverse sequence.

In the absence of a legally established body with responsibility for data protection, any effort to expand AI market enablement would fail to incorporate a dimension of accountability, mirroring the case of the lack of institution-building for the earlier Pakistani digital governance projects (Nazeer & Gil, 2023). The proposed framework demonstrates why such sequencing is important in a way that the mere readiness assessment fails to do so: in the absence of prior institution building and legal readiness, even the gains made in digital infrastructure or market enablement will fail to contribute to AI governance because they do not provide mechanisms of accountability on their own (Gasser & Almeida, 2017; Yeung, 2018).

Conclusion

Beyond assessing Pakistan's preparedness for AI adoption, this study demonstrates the explanatory value of a four-dimensional interactional framework for AI governance readiness. The findings indicate that although Pakistan has created some digital government infrastructure, including those created by NADRA for national identification of citizens and although it has outlined its vision of digital transformation in such documents as the Digital Pakistan Policy 2018 and the Draft National AI Policy, it is not followed by any institutional coordination and legal readiness. In particular, it is the lack of legislation concerning data protection, functioning independent oversight body, and algorithmic accountability that makes up the most significant limitation because the Constitution of Pakistan Articles 10-A, 14, and 19A have not yet become real administrative measures.

Treating readiness as an interaction rather than the sum of all these factors, as the present article suggests, makes it clear that the Pakistani public sector does not have the legal and institutional capacity to implement AI on a broad scale, and moving forward without taking care of these underlying deficiencies can result in replicating in the algorithmic form the longstanding institutional challenges of the country's public administration regarding its lack of accountability.

Recommendations

In light of the above analysis, the following recommendations are made in a sequence of increasing foundational importance for responsible AI adoption in the public sector of Pakistan.

First, priority should be given to the implementation of the Personal Data Protection Bill 2023 as a prerequisite, as opposed to the simultaneous track of adopting AI technologies by the government. With regard to the establishment of the National Commission for Personal Data Protection under the Bill, it will be the first specialized institution that would regulate data processing in accordance with AI systems' consent requirements and breach notifications as controllers.

Second, the mandate of the data protection commission, if there is one formed, should be explicitly expanded via implementing regulations to include algorithmic decision-making of public bodies. It should come with requirements of conducting data protection impact assessment prior to using automated systems processing personal data for administrative decisions and legal right to receive an explanation of automated decision based on the due process clause provided in Article 10-A of the Constitution and in accordance with the accountability principles of the OECD (2019) AI Recommendation.

Third, the coordination of governance related to digital technologies and AI should be entrusted to one single institution as a lead authority with defined responsibilities not

overlapping with other ministries engaged in similar activities, which is necessary to address issues of fragmentation in terms of institutional capacity mentioned in Fukuyama (2017) and regulatory governance in terms of fragmented oversight found in Levi-Faur (2013).

Fourth, efforts to build the capacity of the civil service around data governance and AI oversight should be backed by a concrete implementation budget and an accountable organization, shifting from the aspirational training goals set out in the Draft National AI Policy to an implemented curriculum with uptake metrics, in response to the generalist administrative culture that has been highlighted as an institutional capacity constraint.

Fifth, the Right of Access to Information Act 2017 needs to be revised to establish how it is relevant to automated decision-making systems in the government, and ensure that categories exempting such data from access do not prevent any scrutiny of the criteria and data behind government decisions made through algorithms, making practical the guarantee of transparency in Article 19A of the Constitution.

Sixth, there should be a publicly available list of the AI systems that are being used in the Pakistani government administration system, which is initially small-scale but can be expanded, to allow for scrutiny by civil society and academia as well as parliamentary oversight of the use of algorithms in the provision of public services, which would make the current judicial review and ombudsman process effectively available for citizens to access.

Seventh, future AI regulation in the Draft National AI Policy will have to address the right to explanation and the right to challenge administrative actions, combining administrative law with technology-based protection measures as opposed to judicial review alone.

The sequence of the recommendations was intentionally selected to mirror the dependency highlighted in the above discussion, whereby legal readiness and coordination must happen prior to, or in the very least alongside, the enablement of the market and the creation of infrastructure goals as stated in contemporary policies of AI.

References

- Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). *Digital era governance: IT corporations, the state, and e-government*. Oxford University Press.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People: An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Fukuyama, F. (2017). *State-building: Governance and world order in the 21st century*. Cornell University Press.
- Gasser, U., & Almeida, V. A. F. (2017). A layered model for AI governance. *IEEE Internet Computing*, 21(6), 58–62. <https://doi.org/10.1109/MIC.2017.4180835>
- Government of Pakistan, Ministry of Information Technology and Telecommunication. (n.d.). *Digital Pakistan policy* (2018). https://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf
- Government of Pakistan, Ministry of Information Technology and Telecommunication. (n.d.). *Draft national artificial intelligence policy* (Consultation draft). [https://moitt.gov.pk/SiteImage/Policies/National%20AI%20Policy%20Consultation%20Draft%20V1%20\(1\).pdf](https://moitt.gov.pk/SiteImage/Policies/National%20AI%20Policy%20Consultation%20Draft%20V1%20(1).pdf)
- Government of Pakistan, Ministry of Information Technology and Telecommunication. (2021). *National Cyber Security Policy 2021*. <https://pkcert.gov.pk/uploads/2023/06/2021-National-Cyber-Security-Policy-Final.pdf>
- Husain, I. (2018). *Governing the ungovernable: Institutional reforms for democratic governance*. Oxford University Press.
- Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. <https://doi.org/10.1016/j.giq.2015.04.001>
- Layne, K., & Lee, J. (2001). Developing fully functional e-government: A four-stage model. *Government Information Quarterly*, 18(2), 122–136. [https://doi.org/10.1016/S0740-624X\(01\)00066-1](https://doi.org/10.1016/S0740-624X(01)00066-1)
- Levi-Faur, D. (2013). Regulatory networks and regulatory agencification: Towards a single European regulatory space. *Journal of European Public Policy*, 18(6), 810–829.
- Migdal, J. S. (1988). *Strong societies and weak states: State-society relations and state capabilities in the Third World*. Princeton University Press.
- Nazeer, S., & Gil, Y. (2023). Embracing artificial intelligence challenges for public sector organizations in Pakistan. *Journal of Contemporary Studies*, 12(1), 35–52.
- OECD. (2019). *Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449)*. <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>
- Pakistan. (2016). *Prevention of Electronic Crimes Act, 2016* (Act No. XL of 2016). <https://pakistancode.gov.pk/pdf/files/administrator6a061efe0ed5bd153fa8b79b8eb4cba7.pdf>

- Pakistan. (2017). *Right of Access to Information Act, 2017* (Act No. XXXIV of 2017). <https://pakistancode.gov.pk/pdf/files/administrator3599d65bc5ecb2dd1915d04c7db91e8f.pdf>
- Pakistan Telecommunication Authority. (2021). *Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021*. https://www.pta.gov.pk/assets/media/removal_blocking_unlawful_content_rules_2021_20102021.pdf
- Senate of Pakistan. (2023). *Bill summary*. <https://www.senate.gov.pk/en/billsummary.php?bid=1182>
- The Constitution of the Islamic Republic of Pakistan*. (n.d.). Pakistani.org. Retrieved September 01, 2024, from <https://pakistan.org/pakistan/constitution/>
- UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector: Applications and challenges. *International Journal of Public Administration*, 42(7), 596–615. <https://doi.org/10.1080/01900692.2018.1498103>
- Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12158>
- Zuiderwijk, A., Chen, Y.-C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38(3), Article 101577. <https://doi.org/10.1016/j.giq.2021.101577>