

Research on the Challenges and Countermeasures of Data Governance in Government Public Management in the Era of Artificial Intelligence

Yanfei Huang

School of Zhengzhou university, Zhengzhou 450000, China

ABSTRACT

In the process of the development and application of artificial intelligence technology in government public management, data has gradually become an important resource for realizing the modernization of government governance system and governance capacity, as well as improving the level of government intelligence. The article focuses on analyzing the data governance dilemma and its causes faced by government public management under the background of artificial intelligence, and discusses aspects such as data itself, technological support, management systems, and social concepts. Finally, corresponding countermeasures and suggestions are provided, such as creating a high-quality data resource environment, improving technical support and security levels, improving institutional norms and collaborative networks, and building a shared and friendly social atmosphere, in order to contribute to enhancing the data management level of Chinese governments at all levels, promoting the process of intelligent public management, and realizing the modernization of national governance capacity and governance system.

KEYWORDS

Artificial Intelligence; Government Public Management; Data Governance.

1. INTRODUCTION

In recent years, AI technologies represented by big data, machine learning, deep learning, etc. have begun and will be further widely and deeply applied in all aspects of social life. Government public management is an important component of the national governance system, and its operation mode, decision-making process, and service form are also undergoing profound changes in this AI revolution. Data is the "fuel" of AI and the "blood" of intelligent agents. It directly affects the effectiveness and scope of the government's intelligent application[1]. Good data governance involves both the optimization of internal government operations and the refinement of public services, intelligent risk warning, and scientific decision support for the public interest. However, the complexity of artificial intelligence technology, the explosive nature of data information, and the dynamic and variable nature of governance scenarios pose significant challenges to traditional data management models. Data quality issues, data property rights issues, data sharing issues, data security protection issues, data management system construction issues, as well as ethical dilemmas and public questioning in data use, have collectively become a practical threshold that hinders government public management from entering the intelligent era[2]. Therefore, examining the new challenges faced by government data governance in the era of artificial intelligence and exploring effective response strategies has important theoretical value and practical urgency.

2. DATA AS THE CORE ASSET OF GOVERNMENT GOVERNANCE AND THE FOUNDATION OF INTELLIGENT TRANSFORMATION

In traditional management models, government data is often seen as traces of government operations or internal information, and in this case, the value of the data has not been fully realized. With the advent of the era of artificial intelligence, the status and role of data have undergone tremendous changes. Data is no longer just a simple trace, but an important resource that can be deeply mined. It is a key resource for achieving the transformation of government functions and innovation in government governance.

Firstly, data is the "nerve endings" of the government's cognitive society and perception of the situation. By aggregating massive amounts of data in areas such as economic operation, social livelihood, environmental resources, and public safety, it forms a panoramic, real-time, and accurate understanding of the social individuals or groups it faces, breaking through the limitations of traditional understanding based on sampling surveys and local experiences; Secondly, data is an important supporting tool for the government to shift from an experience driven decision-making model to one based on data and model analysis. Artificial intelligence algorithms can learn and mine big data to determine potential social demand trends in the future, predict the effectiveness of certain policy implementations, and assess the differences in outcomes brought about by various intervention measures. This provides more objective data support and decision-making reference information from multiple perspectives for government decision-making. Thirdly, data is the foundation that supports the government in providing intelligent and precise public goods and services[3]. By studying and analyzing relevant data such as user usage habits and demand characteristics, it is beneficial for government departments to simplify their procedures, accurately push policies, and provide customized services, greatly improving the accessibility, convenience, and satisfaction of public services; Beneficial for promoting the supply side structural reform of government services and providing citizens with better public goods and services; Beneficial for promoting the modernization of the government governance system. Data is the "lubricant" for improving internal collaboration and operational efficiency of the government. Cross departmental and cross level data sharing and business collaboration are conducive to breaking down departmental barriers, optimizing administrative processes, and achieving seamless operation of the overall government. Therefore, establishing a sound data governance system to ensure the availability, usability, usability, and security of data is an indispensable prerequisite and foundation for the government to successfully harness artificial intelligence and achieve intelligent transformation[4].

3. DATA GOVERNANCE CHALLENGES FACED BY GOVERNMENT PUBLIC MANAGEMENT IN THE ERA OF ARTIFICIAL INTELLIGENCE

However, in practice, there are still many complex issues for governments to effectively govern data to support AI applications, which are distributed throughout the data lifecycle and data governance system.

3.1. Challenges at the Data Foundation Level

Data is the foundation of artificial intelligence and greatly affects its effectiveness and credibility. The main problems currently exist are: firstly, the prominent issues of data fragmentation and islanding. The data held by the government is distributed across different departments, levels, and regions. Due to the fragmented management system, inconsistent technical standards, and considerations of interests, the willingness to share data among departments is low, and channels are not smooth, resulting in numerous data islands that cannot support intelligent applications that require the combination of multiple data sources. Secondly, the quality of data varies greatly. There are phenomena such as missing data, chaotic data formats, inconsistent data standards, untimely updates,

and even contradictions[5]. The entry of low-quality data will cause deviations or even errors in the output results of artificial intelligence models, known as "garbage in, garbage out". This directly restricts the scientificity of decision-making and the accuracy of services. The third issue is unclear data rights and responsibilities. The legal ownership of data, including ownership, usage, management, and revenue rights, has not been fully clarified. The rights and responsibilities between data providers, users, and aggregation platform entities are also unclear, which poses legal and practical challenges to data ownership, flow, transactions, and protection of data rights and interests.

3.2. Challenges in Technology Application and Security

In addition to efficiency advantages, the application of artificial intelligence also brings new technological and security challenges. One is the issue of algorithmic discrimination and decision fairness. The learning of artificial intelligence algorithms is based on existing data. If there is discrimination against specific groups of people (such as gender, region, income, etc.) in the past data, artificial intelligence may use this discrimination as its judgment basis and further expand this discrimination. One is to form discriminatory results in automated decision-making, which will affect social fairness and justice. The second is to increase the risk of data security risks and privacy breaches. The government has gathered a large amount of sensitive data related to national security, trade secrets, and personal privacy[6]. Artificial intelligence applications often require a large amount of data collection and analysis, increasing the possibility of data leakage, tampering, and abuse during the collection, storage, transmission, processing, and destruction processes. Advanced sustainability threat attacks and insider threats pose challenges to data security protection. The third is algorithm black box and accountability. Many cutting-edge artificial intelligence algorithms, such as deep learning, operate in a black box, making it difficult to clearly explain the specific operation process of the algorithm and how to make judgments and conclusions. Once automatic processing decisions based on such algorithms have a significant impact on the public or businesses, there will be management difficulties such as unclear accountability targets and ineffective accountability mechanisms.

3.3. Challenges at the Institutional and Management Levels

Thirdly, the current institutional mechanisms are difficult to match the new situation of data governance development in the era of artificial intelligence. On the one hand, relevant laws and regulations are relatively lagging behind. In the existing legislation such as the Data Security Law and the Personal Information Protection Law, there are many principled provisions, but there are still shortcomings in how to implement them in specific scenarios and how to carry out standardization construction, especially in issues such as public data open sharing and use, algorithm management, and automatic decision-making accountability. There is a lack of clear and operational legal provisions. One is the mismatch between organizational support and division of responsibilities. Many government departments have not yet established dedicated data governance agencies or chief data officer positions, with dispersed data governance responsibilities and a lack of unified leadership and top-level design. Insufficient horizontal linkage and asymmetric responsibilities, making it difficult to form a collaborative governance force[7]. Secondly, the standard rules and regulations are not perfect. There are no national or industry wide standards and specifications for data classification and grading, metadata, interfaces, data quality, algorithm ethics, etc., resulting in high data integration costs and low interconnectivity, making it impossible to achieve large-scale application of artificial intelligence.

3.4. Challenges in Social Cognition and Acceptance

The public's recognition and understanding of the government's use of AI data governance determine whether its use is legitimate and sustainable. One reason is that the public's data literacy and

willingness to participate are different. Some members of the public lack sufficient knowledge of data, algorithms, privacy and security, and are unable to effectively realize their data rights such as informed consent and participate in the supervision and feedback process of data governance, which poses a risk of widening the "digital divide". The second is the risk of public trust and acceptance[8]. The repeated incidents of information leakage, algorithmic discrimination, and technological black boxes will shake the public's trust foundation in government digitization and intelligent governance. If there is no open communication and full participation, the public will have resentment or even resistance towards the government's use of algorithms for decision-making, threatening policy implementation and social stability. The third is the contradiction between data application and privacy protection. While promoting data openness and sharing, and creating public value, the government should also protect citizens' personal information and privacy rights. How to strike an appropriate balance between the two, form governance rules that balance innovation and rights protection, and gain social recognition is an eternal topic.

4. COUNTERMEASURES FOR OPTIMIZING GOVERNMENT DATA GOVERNANCE IN THE ERA OF ARTIFICIAL INTELLIGENCE

Faced with the above challenges, the government needs to adopt a systematic, comprehensive, and forward-looking response strategy to build an agile, robust, and trustworthy data governance system that meets the requirements of the artificial intelligence era.

4.1. Consolidating the Data Foundation: Building a High Quality Government Data Resource System

Firstly, solve the problem of data infrastructure. One is to vigorously promote data aggregation and sharing. Introduce a responsibility list and negative list system for sharing government data resources, clarify the scope of data that should be shared and the situations where it should not be shared. Build and optimize national and provincial integrated big data platforms, data sharing and exchange platforms, and leverage their role as exchange hubs. The use of administrative negotiation, assessment incentives, economic compensation, and other methods is to promote conditional sharing of cross departmental data. Break down data silos between departments and achieve purposeful data sharing based on business needs. The second is to strengthen data governance throughout the entire process. Conduct quality assessment and inspection of the entire process of data collection and archiving to ensure data integrity and accuracy; Compile a list of data resources, recording information such as data ownership, type, update cycle, and quality status; Optimize data through methods such as data anonymization, integration, and cross validation. The third is to explore the establishment of a mechanism for separating data property rights. On the premise of adhering to the national ownership and public attributes of data resources, explore the implementation forms of equal distribution of public data usage rights, operation rights, and revenue rights, clarify the rights, responsibilities, and interests of all parties under the framework of the rule of law, and lay the foundation for promoting the market-oriented allocation reform of data elements[9].

4.2. Strengthening Technological Empowerment and Security Protection

Adhere to the combination of technological innovation and security guarantee. One is to promote the development of trustworthy artificial intelligence. Encourage the development and use of explainable artificial intelligence, federated learning, privacy computing, and other technologies to achieve value mining of data while ensuring data privacy and security, as well as improving the transparency and interpretability of algorithm decisions. Establish an algorithm impact assessment and filing system, establish an algorithm filing review and normalized evaluation mechanism, and carry out pre review and normalized dynamic monitoring of algorithms in important fields. The second is to establish a

security guarantee system for deep defense. Implement systems for network security level protection and critical information infrastructure security protection. Adopting technologies such as encrypted transmission, access control, data anonymization, security auditing, and threat perception to strengthen data security protection. Thirdly, we will establish a sound mechanism for preventing data security risks and emergency response, and regularly conduct security drills and attack and defense tests; The fourth is to strengthen independent research and development and use, increase investment in the research and development of artificial intelligence basic algorithms, chips, frameworks, and key data security technologies, reduce dependence on external technologies, and enhance supply chain security capabilities.

4.3. Improve Systems and Collaborative Mechanisms

Establish sound systems and collaborative mechanisms to ensure effective governance. One is to accelerate the improvement of the legal regulations and standard system. Promote legislation on public data, clarify the scope, conditions, procedures, and responsibilities for the open use of public data. Refine and implement the specific requirements of the Personal Information Protection Law and the Data Security Law in government settings. Accelerate the development of national and industry standards for data classification and grading, quality evaluation, interface specifications, algorithm governance, and other aspects. The second is to improve and perfect the data governance system. Promote the establishment of Chief Data Officers in government departments at all levels, establish specialized agencies to carry out data governance work, undertake the responsibilities of formulating and implementing local and departmental data development strategies, guiding data management, and supervising data security; Establish a data governance committee with the participation of various departments to study and promote the sharing, openness, and development of important data. The third is to build a new data governance system. Explore the collaborative construction of a data governance ecosystem among government, industry, academia, research, and application. Encourage joint enterprises, universities, research institutes, social organizations, etc. to collaborate in technology research and development, standard setting, platform construction, application development, and other aspects[10]. Explore the use of data sandboxes, innovative laboratories, and other methods to promote data fusion application experiments in a controlled environment.

4.4. Promoting Inclusive and Trusting Social Co Construction

The fundamental purpose of data governance is for the public interest and should be understood and supported by the public. Improve the data literacy and participation ability of the whole society. Carry out targeted public digital skills training and data knowledge promotion to enhance citizens' awareness of data rights and self-protection capabilities. Expand the channels for public participation in data governance, such as through hearings, public opinion surveys, open reviews, etc., to incorporate public opinions into data policy formulation and algorithm design evaluation. The fourth is to improve the transparency and accountability of government data governance. Proactively disclose information on non confidential data resource catalogs, data openness plans, algorithm application scenarios, and basic principles. Establish a convenient mechanism for querying, correcting, and appealing public data. Improve the review and manual intervention process for automated decision-making to ensure that citizens are not deprived of their right to access manual services under any circumstances. Seeking a dynamic balance between data utilization and privacy protection. Implement the principle of minimum necessary data and strictly limit the scope of data collection. Promote the concept of privacy design and embed privacy protection into system design and business processes. In the process of carrying out data openness and innovation, risks are avoided through anonymization, differential privacy, and other methods, and a classified and scenario based personal information protection mechanism is established through legislation, standards, industry self-discipline, and other means.

5. CONCLUSION

Under the background of artificial intelligence, how to effectively govern data has become an important issue in promoting government public management reform and innovation in the new era. Because data is the most important governance resource in the era of artificial intelligence, only by doing a good job in data governance can we fully leverage the advantages of artificial intelligence, promote the development of the government towards intelligence, and improve the level of government governance. This article explores the problems in promoting government data governance in the new era from four aspects: data itself, data security, data management systems, and social concepts. These problems are interrelated and coupled, and are a comprehensive system governance issue.

Cracking the above problems is not an overnight task, nor can it be solved by efforts in any aspect. It requires the formation of a systematic solution that includes building a solid data foundation, improving technological support, improving institutional linkage, and promoting social participation from multiple dimensions. This solution requires prioritizing quality and sharing leadership, placing equal emphasis on technology research and development as well as safety assurance, advocating for legislative amendments and standard setting simultaneously, calling for organizational change and cross-border cooperation, and ultimately committing to using transparent, participatory, and balanced methods to gain public trust and social consensus. The future government data governance is a constantly evolving and dynamically adjusting process, which requires the government to constantly explore new ways of data governance that conform to the laws of technological development, national governance needs, and public interest demands with a more open mindset, creative thinking, and a more responsible attitude. In short, only by establishing a fast, efficient, and reliable data governance system can we ensure the sustainable development of AI in the field of public management and better serve the creation of a public service-oriented government and society that satisfies the people.

REFERENCES

- [1] Engy Khalil, Fatmah Arif Al Ali. AI adoption in government public relations: Technology acceptance, social influence, and organizational dynamics in the UAE[J]. *Public Relations Inquiry*, 2026, 15 (1): 31-51.
- [2] Mansur Samadovich Omonov, Yonghan Ahn. Towards Smart Public Administration: A TOE-Based Empirical Study of AI Chatbot Adoption in a Transitioning Government Context[J]. *Administrative Sciences*, 2025, 15 (8): 324-324.
- [3] Luca Tangi, A. Paula Rodriguez Müller, Marijn Janssen. AI-augmented government transformation: Organisational transformation and the sociotechnical implications of artificial intelligence in public administrations[J]. *Government Information Quarterly*, 2025, 42 (3): 102055-102055.
- [4] M. Blair Thomas, Daniel Baracskey. Evolving AI policy and the public administrator: Initiatives across recent presidential administrations and transitioning into the second Trump presidency[J]. *Administrative Theory & Praxis*, 2025, 47 (3): 185-201.
- [5] Tiannan Zhang, Emilio Aguinaldo College, Manila, Philippines. Role of Artificial Intelligence in Public Value Creation in Local Government in Chongqing, China: Inputs to Improved E-Governance[J]. *Pacific International Journal*, 2025, .8 (3):
- [6] Michael Keating. Local governments are acquiring more public-safety technology, including transformative AI tools[J]. *Urgent Communications*, 2025,
- [7] Michael Keating. Local governments are acquiring more public safety technology, including transformative AI tools[J]. *The American City & County*, 2025,
- [8] Tan Evrim. Designing an AI compatible open government data ecosystem for public governance[J]. *Information Polity*, 2023, 28 (4): 541-557.
- [9] Department of Business and Technology , Korea Advanced Institute of Science and Technology (KAIST) , Daejeon , Republic of Korea, Department of Business Administration , Seoul School of Integrated Sciences and Technologies (aSSIST) , Seoul , Republic of Korea, Department of Business and Technology , Korea Advanced Institute of Science and Technology (KAIST) , Daejeon , Republic of Korea. Does public service delivery through new channels

promote citizen trust in government? The case of smart devices[J]. *Information Technology for Development*, 2019, 25 (3): 604-624.

[10] K. Prerakkumar. Monitoring Civic Project and Making Intelligent Decisions in Local Government using Geoinformation System[J]. *International Journal of Computer Applications*, 2018, 179 (9): 7-11.