Research on Local Government Data Security Management in the Big Data Era

Hua Rui

Lab for Digital & Mobile Governance, Fudan University
790693032@vip.com

Abstract
Data Security is an inevitable problem in the process of data exploitation. The traditional "system-centered" management philosophy and mode have been unable to meet the needs of data in the circulation. Therefore, it is urgent to explore the status quo and mode of data security management under the framework of "data-centered" philosophy in order to better promote data exploitation. Drawing on the qualitative research tool Maxqda2020, this paper analyzes the relevant policy texts and responsibilities of government bodies, identifies the core value, organizational structure and the division of responsibility of local governments in data security management, and tries to summarize their management modes. The data security management has preliminarily achieved the mode transformation from "system and application-centered "to "data-centered". The balance between security and utilization has been recognized at the value level. But the corresponding organizational structure, management measures and means have not kept up.In the future, data security management needs to be optimized in terms of laws and regulations and top-level design

Keywords: *Data security; Public data; Management mode;*

1. INTRODUCTION

Data is regarded as a country's basic strategic resources[1], and the exploitation of it to the maximum is one of the principal lines of data governance. However, with the deepening of data exploitation, problems of data security have become increasingly prominent. The "Program of Action for promoting big data development ", issued by the State Council in 2005, mentioned that it is necessary to properly handle the relationship between innovation and security, so as to ensure data security.

The traditional "system-centered" data security management mode can no longer meet the requirements of data security management under the background of "public infrastructure construction, information system interconnection and complex data circulation". First of all, in the past, each public administration and service organization managed and protected its own data, and the boundary of rights and responsibilities was clear, while today the rights to use and manage data are changing with data collection and circulation. As a result, a new data security management system is in urgent need to define ownership and responsibility boundaries in data collection and circulation. Secondly, data sharing and exploitation has made the data in previously closed systems open and circulation. Meanwhile, data barriers among government departments, government and society, and enterprises have also been gradually broken down. Such an open and cyclic data ecology also demands on a better reconstruction of data security management mode and system. Therefore, it is necessary to identify the core values and internal operating mechanism of local governments in data security management, and try to sort out management models to provide suggestions and reference for future data security management path [7].

2. RESEARCH METHODS AND ANALYTICAL FRAMEWORK

2.1 Research Methods

Based on the Policy Document Database of the State Council and Legal and Regulatory Database of Peking University, "data security", "data security management" and "network security" are used as key words to search for policies and regulations, and a large number of policy documents and institutional functions and reform plans disclosed on the government's official website are taken as sample sources. According to the word cloud chart of all samples, words such as "safety", "institution", "organization" and "responsibility" shows a higher frequency of occurrence. Therefore, the sample source is highly correlated with the research subject of this paper.

S. A. R. Khan et al. (Eds.): ICMSSE 2022, AHCS 12, pp. 10–15, 2023.
https://doi.org/10.2991/978-94-6463-056-5_3

On this basis, with the help of qualitative analysis tool maxqda2020, this paper sorts out the core values, organizational structure and responsibility division of data security management by local governments, clarifies their business operation logic [8].

2.2 Analytical Framework

The applicability and validity of management modes are important links in the data security governance by government. Mode, basically means a reflection of management system, philosophy, operation and other elements of an organization in a normal and regular form. So in essence, data security management model is the principle orientation, responsibility division and inter-relationships among main bodies in an organizational system, reflected in a fixed pattern.

In this paper, current status of local data security management is analyzed through three dimensions, namely the core values, organizational structure and responsibility division. The core values refer to work principles and orientation of data security on the basis of system supply, which represents the value orientation of data security management. If we regard values and principles as targets, then conducts are the most direct way to understand the status quo of data security management. If we want to transform targets into conducts, then practice, that is, specific operation of an organization should be taken into consideration. The operation mechanism can be understood as the organizational and structural relationship formed in the process of data security management and the interaction among various subjects. In other words, it is the division of labor within the organization, the allocation of functions and interaction among all subjects, which can be characterized as the division of responsibilities and organizational structure.

3. CURRENT SITUATION OF DATA SECURITY MANAGEMENT BY LOCAL GOVERNMENTS

3.1 Value Orientation of Data Security Management

Value orientation affects the development trend and direction of data security management. The values mentioned here are usually presented in laws and policies in the form of "law principles". By analyzing the principles of data security management, we can better understand the value system behind laws and regulations, and identify the positioning and objectives of data security governance. In jurisprudence, "principle" is the transformation of "value", which can be seen as equivalent to value[11].At the same time, "principle" is usually compared to "rule". If rules represent the reality, then principles are an abstract ideal, a kind of target state to be achieved.

Through qualitative analysis of published policies, regulations and documents related with data security, we find the main expressions of the value principles of security management, as shown in Table1: both the central and local governments have mentioned "equal attention paid to security and development", that is to say, data exploitation should take into account the value orientation of data security. Looking at the local governments only, " equal attention paid to security and development " and "balance between management and technology" have been mentioned by all while "unified leadership", "unified power and responsibility", "division of responsibilities" and "hierarchical management" are rarely mentioned, which shows that clear lines of demarcation hasn't been drawn yet in the specific division of management and responsibility [9].

Table 1 Regulations of central and local governments on safety management principles

	Equal Attention Paid to Safety and Development.	Balance between Management and Technology.	Coordination and Cooperation	Unity of Powers and Responsibilities	Division of Labor with Individual Responsibility	Graded Administration
Binzhou	√	√	√		√	√
Guizhou	√		√			
Guiyang	√		√			
Hangzhou	√	√	√		√	√
Hainan	√	√				
Hefei	√			√		
lianyungang		√	√	√		
Ningbo	√		√			
Tongren			√		√	√
Tianjin	√	√	√		√	

Zhejiang	√	√	√		√	√
Zhengzhou		√	√		√	√

3.2 Evolution of organizational structure

Organizational structure with distinct layers and an efficient circulation of information or orders can not only clarify the division of responsibilities, but also help each department to examine its position in the whole right system and management structure, and prevent confusion of responsibilities, which is a powerful organizational guarantee for government departments in data security management. According to the relationships among basic elements such as vertical hierarchy and parallel departments in the organizational structure, it is concluded that the current organizational structure has the following characteristics:

3.2.1 The Rudiments of Interdepartmental Network Structure.

In the traditional security management mode, each department only pays attention to its own internal data security, which results in seriously closed and fragmented data, while data circulation and exploitation increasingly need collaborative governance across organizational boundaries[12] In some places, by setting up data security (work) leading groups and Security Commission (usually under the municipal government), an interdepartmental coordination mechanism has been established. The leading group has strong political power and can use administrative authority to realize effective security management, efficiently allocate resources such as manpower, material resources and financial resources, so as to facilitate overall communication and coordination among departments. Take Hangzhou, Lianyungang and Shenzhen for example, they have set up leading groups or professional committees by selecting professionals in relevant business departments, and have made them linked with other business departments, forming an interdepartmental network structure. The leading group can not only make professional decisions on data utilization and links in full data lifecycle, but also have administrative guidance in business management, which not only caters to the characteristics of data circulation and dispersion, but also strengthens the linkage among big data administration, cyberspace administration, public security bureau and other operating departments [10].

3.2.2 The extension of the organizational structure

On one hand, the utilization and circulation of data break the boundary of security management, and organizational structure is constantly extending to society and enterprises. Governments are establishing ties with enterprises and society in the form of business cooperation and outsourcing. For example, leaders of Zhejiang Province instructed to set up specialized data security enterprises and create one-stop data security services, providing omni-dimension data security solutions for digital transformation. In some other places, big data operation companies are set up to take charge of the security construction and operation and maintenance of public platforms and common platforms such as e-government. On the other hand, data security governance is for better data exploitation, while the ultimate goal of data opening and utilization is to realize the social and economic value of data. This process requires that governance subjects of data security should extend the internal government to enterprises and society, and only by doing so can the multiple-subject structure reflect the essence of data serving society [11].

3.3 Division of Responsibilities of Data Security Management by different governments

Based on the duty arrangement of each department in the existing policies and regulations and each department's division of responsibilities clearly specified on government official websites or publicly released institutional reform plans, data security management can be divided into four duty categories: macro decision-making, organization and management, business execution and supervision and safeguard, according to different responsibility subjects. As shown in Table 2, macro decision-making mainly covers overall leadership, system construction and standard planning and formulating. Organization and management can be roughly encapsulated as security management system, overall coordination and operational guidance. As for business execution, it can be divided into business management and operation and maintenance of platform technology. Supervision and safeguard mainly include security check and supervision and assessment.

Table 2 Division of responsibilities for local data security management.

Local Gov.	Macro Decision-Making			Organization and Management			Business Execution		Supervision and Safeguard	
	overall leadership	system construction	standard planning	security management system	overall coordination	operational guidance	business management	platform technology	security check	supervision & assessment
Chongqing				B		B			C	D
Binzhou				B		B				
Guangdong		B	B							E、C、D
Guiyang					C		B		D	C
Guizhou	A			B	C、B	C	B		D	
Hainan				B	C	C、G	B			G
Hangzhou		B	B	B		B	E	G		
Lianyungang						E	G	G	G	
Nanjing	A	B	B			C		F	F、D	C
Ningbo			B		B					B
Shanghai	A	C			C	C	E	F	F	F
Shenzhen	B	B			C	C		G	D	B、C
Tianjin				C	C		E		D	
Tongren				B	C	C	E		D	B
Wuhu		C、F		B		B		F	B	
Zhejiang	B	B	B		C		E			
Zhengzhou				B	B	B			C、D	

Note: Information in the table comes from government official websites and relevant policy texts.

For convenience of reading: A stands for provincial and municipal governments and their general offices; B indicates data governance institutions or competent departments; C represents Cyberspace Administration; D represents Public Security Bureau; E stands for Government Affairs Department and its business divisions; F represents Big Data Center; G stands for Information and Technology Department.

3.3.1 Macro Decision-Making

Macro decision-making department mainly involves Local People's Governments or their general offices and local data authorities (local big data bureaus), yet in a few places, it is the Cyberspace Administration that leads system formulation and strategic decision-making. Looking from specific division of labor, the three main aspects of this work are basically undertaken by the same department, and the allocation of functions is single and clear, which means there won't be any cross-sectoral problems. From the perspective of involvement, only a few local governments are fully involved in leadership, system and planning [12].

3.3.2 Organizational Management

Organizational management mainly involves local cyberspace administration and data authorities (usually big data bureaus). In other places, leading groups (usually under municipal government offices) have been set up to coordinate data security. Only a few number of local governments have covered all three responsibilities of organizational management, which may be due to the fact that data security management in those places is still in its initial stage, and the delimitation of each responsibility needs to be improved. From the perspective of coordination of duties, in most areas, these three responsibilities are undertaken by different departments or agencies. For example, in most cases, the establishment of security system is completed by local data authorities, while the overall coordination and business guidance are mostly undertaken by cyberspace administration. In addition, in some places, although cyberspace administration is responsible for data security coordination and business guidance as stipulated in policies and regulations, according to the organization reform plan or “three decide” stipulation disclosed by the local data management department, specific responsibilities of coordinating, guiding and supervising the data security work of each department are also specified, which is easy to cause "fights" among departments. What is the boundary of power and responsibility between data competent departments and cyberspace administration needs to be further clarified during practice.

3.3.3 Business Execution

In business execution, the big data center and information center are mainly responsible for issues regarding platform and technology security. In most cases, industry departments and public administration service institutions are responsible for its own data security while some places transfer the responsibility to data management departments such as Big Data Bureau. In many places, there is no hierarchical relationship between business executive departments and overall guidance departments, so the comprehensive coordination will be affected to some extent. For example, what if Cyberspace Administration, as the overall guidance department and Big Data Bureau for security

work lose relationships of administrative subordination and restriction? How to cooperate and coordinate?

3.3.4 Supervision and Safeguard

Regarding supervision and safeguard, significant differences among different places are shown. For instance, security check is often undertaken by public security organs, but in some places, data security competent department bears this responsibility together with the public security bureau, cyberspace administration and confidentiality departments. The responsibility of supervision and management also involves several divisions.

Additionally, data security management responsibilities at the central level are also distributed among different departments. For example, responsibilities such as promotion of information and technology application and network security coordination, originally belonging to the Ministry of Industry and Information Technology have been re-assigned to the Office of Central Leading Group for Cyberspace Affairs. However, no corresponding leading department has been formed in macro decision-making. Secondly, there is also a lack of leading data security management institutions nationally. Generally speaking, the prototype of data security management of all regions has basically taken shape, but it still needs to be improved in terms of comprehensiveness. Against the background characterized by data circulation, however, the coordination and division of labor in management and execution need to be further clarified and so do the responsibility of supervision.

4. CONCLUSIONS

At present, the data security management has preliminarily realized the mode transformation from network, system and application-centered to data-centered. In terms of value orientation and goals, more awareness has been gained on the importance of data utilization and balance between security and utilization. Organizational structure, management measures and means haven't kept pace; the internal system and workflow need to be further straightened out.

Specifically, in management department, the status of statutory institutions of data security management needs to be further clarified; the division of labor and status among various departments is not clear. There are several objects in management objects and contents, which generally focus on "Big Data Security", "Public Data Security", "Network Security", "Information Security" and so on. Target orientation is diversified. One part is safety management based on the marketization of data elements, aiming at economic development and industrial transformation. The other one is targeted at safety control. In the social subject participation, besides the market-oriented operation of statutory body mode, the degree of engagement of market subjects of the other two modes needs to be improved.

According to the above findings, the future data security management should be under the background of data exploitation. In addition to better arrangements of laws and regulations, it is also necessary to explore the management structure and mode that can not only facilitate data flow, but also assure security, so as to achieve linkage and cooperation between the upper and lower levels.

In terms of laws and regulations, specialized data security laws and policies should be issued, and its operational should be standardized according to the system. In the design of the top-level structure, an inter-department cooperation mechanism should be constructed, which is led by government departments and participated by enterprises and society. It is to achieve the pattern of government and society co-governing. On the division of management, from the central government to the local, it is necessary to specify the specialized data security department or person in charge; the department in charge of guidance and supervision should be separated from the executive department. We can learn from the "Middle-ground Concept" of enterprises and regard the safety management organization or leading group of public data as "Data Middle Office".[13] As the core layer of organizational structure system and resource allocation, it serves as data interface and closely combines the front-end and the back-end of data department, forming a collaborative management network.

REFERENCES

[1] Circular of the state Council on printing and distributing the action plan for promoting the development of big data. gf [2015] No.50 [EB/ol]. http://www.gov.cn/zhengce/content/2015-09/05/content _ 10137.htm.

[2] Kou Jinfeng, Zhang Yunyong, Tao Ye, Liu Yong, Yan Shuo. Data security management system of telecom operators based on data life cycle [J]. Information and Communication Technology, 2019,13(06):53-58.

[3] Ding Hongfa, Meng Qiuqing, Wang Xiang, et al. Analysis of data security and privacy protection countermeasures of government data opening for data life cycle [J]. journal of information, 2019, 38(7): 151-159.

[4] Sheng Xiaoping, Guo Daosheng. Research on Data Security Governance in Open Sharing of Scientific Data [J]. Library and Information Work: 1-12.

[5] Research on Data Security Governance in Scientific Open Data Sharing _ Sheng Xiaoping [J]. Library

and Information Work, 2020:1-12.

[6] Wu Weiming, Wu Li. Comprehensive information security and rational use of data —— A brief review of Data Security Law (Draft) [J]. Information Security and Communication Secrecy, 2020, (08): 23-28.

[7] Zhu Xuezhong, Dai Zhizai. Value and system orientation of Data Security Law from the perspective of overall national security concept [J]. E-government, 2020, 212(8): 82-92.

[8] Qing Guo, Lin Tong, Qiao Yuanbo, et al. The construction and evolution of big data management institutions of local governments in China —— A comparative analysis based on the eighth institutional reform [J]. E-government, 2020: 29-38.

[9] Zhangming. from administration-led to institutionalized coordinated advancement-Zhejiang practice and experience in the construction of government digital transformation promotion mechanism [J]. governance research, 2020, 36(03): 26-32.

[10] Wang Weiling: Accelerating the Implementation of Digital Government Strategy: Realistic Dilemma and Solutions, E-government, No.12, 2019.

[11] [Germany] translated by Robert Alexy, Zhu Guang and Lei Lei. Law, Rationality and Negotiation: Research on Legal Philosophy [M]. Beijing: China Legal Publishing House, 2011:213.

[12] Dawes S S, Cresswell A M, Pardo T A. From "Need to Know" to "Need to Share": tangled problems, information boundaries, and the building of public sector knowledge networks [J]. Public Administration Review, 2009, 69(03): 392-402.

[13] Yao hong. design and implementation of data management system based on data center [J]. science and technology innovation, 2020(35):74-75.