Research on Police Data Governance Process

Tuo Shi, Danyang Li*, Zihao Wang, Qi Zhang

Beijing Police College Department of Public Security Management, Beijing, 102202, China
* Corresponding author: Danyang Li

Abstract: In the information age, the police data of the public security organs are faced with the problems that the data is not known, the data is not desirable, the data is not controllable and the data is not connected, which results in the "barrier" of the police data presented by the public security organs among the various business departments, the lack of unified management and the lack of asset maps; Third, the lack of data standards, no effective integration, business system data can not effectively combine a series of problems. The above problems lead to a large number of police data can not be fully utilized, which seriously affects the efficiency of public security work. Therefore, it is the key to solve many problems to construct an effective data governance process. This paper discusses the application status of police data governance from the current situation of police data governance, and analyzes the current problems. This paper studies the police data governance process around the existing problems and police data governance objectives.

Keywords: police data; governance data; governance; process; governance frame; data; governance technique

1. Introduction

Today, data, as a source of important value, has become an important part of the overall battle effectiveness of public security and an important strategic resource. However, the huge data resources cannot be brought into play without effective data governance, which will affect the overall fighting capacity and modernization level of the public security team. The development of police data governance is an important link to deeply secure the practical business needs of public security work, conform to the social development trend of the "internet plus" era, meet the needs of public security organs' own business development, and create a modern police work.

2. Police Data Governance

2.1. Connotation of Police Data Governance

Currently, there is no unified concept of data governance, which is a set of management behaviors involving data use in organizations [1]. As the two concepts of data governance and data management are easily confused, domestic scholars studying data governance have clarified their differences and pointed out that governance and management are completely different activities, the former is the guidance, supervision and evaluation of management activities, while the latter is the implementation of specific plans, construction and operations based on the decisions made by governance [2]. Data governance has been applied earlier in enterprises, covering the entire enterprise's information position and construction. It provides a planning, design and implementation method for data management, clarifies the relevant roles, work responsibilities and work processes, and ensures that data assets can be managed in an orderly and sustainable manner over a long period of time. Moreover, it has a wide commercial extension, involving related projects in many enterprises, but it may appear in other forms.

Based on the relevant research basis, in this paper, it is believed that data governance should have the concept in a broad sense and a narrow sense. In a broad sense, data governance refers to the practice that relies on the accurate analysis of various data by modern information means to discover the value behind the data and the internal relationship between the data, and then obtain relevant conclusions to guide actual combat. In a narrow sense, data governance is more about governance of various types of data, that is, governance of data, in order to improve the quality of the data itself, and thus various governance data activities [3].

Police data, as an electronic record, has a wide range of amounts and categories. There is no need to govern data not related to police business, because only important data resources related to police work can be called "data assets". Therefore, "data governance" is not the governance of data, but the governance of "data assets" that can serve the police work. The police data governance studied in this paper should be a conceptual category of data governance in a broad sense, that is, police activities rely on data resources as an important means to improve the level of public security business and combat effectiveness, and use the connections between data and the problems reflected behind the data to solve the practical problems faced by public security work. In general, police data governance is a collection of management power and control activities to the full data assets of police departments, including planning, monitoring, implementation and other content, with the goal of realizing the effective integration of global data resources, and effectively solving the problems of public security power dispersion, resource segmentation, information island, operation closed, and finally breaking the departmental barriers and police barriers.

2.2. Elements of Police Data Governance

Police data governance includes three elements, namely "quality, sharing and application". First, the foundation of

police data governance lies in data quality, which directly affects whether and how much it can play a role. Collecting and processing data in the early stage of data governance is to improve the quality of data, so that the data can be further processed in the next stage to provide basic guarantee. Secondly, sharing is the key link of data governance. As an important strategic resource today, data can exert value in more positions and generate greater value if it spreads to more departments and fields [4]. The same data may seem useless in one department, but it may be a "treasure" to another, which is the problem that the public security organs are facing at present. However, there are high data barriers among various units. By police data governance, the data inside and outside the system can be summarized by building police cloud, intelligence center, big data center, etc., so as to make full use of modern new technical means, reverse the previous development ideas, and improve the police data governance process to realize the maximum value of data in the overall situation. Third, the application of data is the core of data governance. At the beginning of the governance of massive data, the purpose should be the application of data to serve the public security actual combat to solve practical problems.

3. Significance of Police Data Governance

As the business support in the big data era is facing the three major pressures of "operation, maintenance, management and appreciation", how to achieve cost reduction and efficiency improvement of data management through data governance, and to enhance the ability and value are the topics that all industries face in data governance. First, operation and maintenance pressure. At present, the total data volume of the support system has reached PB level or even EB level, coupled with the rising resource investment and operation and maintenance costs, the data quality and data security operation and maintenance are under pressure, and at the same time, the data is not effectively managed, which will cause great pressure on authorized access and support services. Secondly, management pressure. Scattered data sources, lack of effective management of data models, quantitative change to qualitative change brought by data expansion to business support, high-speed increase of global server data every year, and difficulty in carrying huge amounts of data in development, architecture and operation and maintenance systems, all of which bring huge challenges to platform support and system management capabilities. Third, pressure of appreciation. Data is the core value of an enterprise or organization. In the face of increasingly fierce competition, more and more enterprises and organizations begin to attach importance to the management and operation of data in order to enhance their business development capabilities. In the face of huge amounts of data, more and more attention is paid to how to effectively preserve and increase the value of data.

Similarly, the business support in the public security system also faces these three pressures. In detail, in public security work, the so-called operation and maintenance pressure is due to the pressure on data quality and data security operation and maintenance caused by the huge data volume of public security organs in various places and cities. Without effective governance, it will cause great pressure on authorized access and support services. The management pressure is caused by the lack of data control, the inconsistency of code and statistical standards of public security organs at all levels and places, and the problems of multi-head construction and repeated construction, resulting in unclear data governance process and difficulties in overall planning. The pressure of appreciation is due to the poor availability of data in the current public security system, which leads to the long online cycle of all kinds of information and analysis applications, the difficulty in establishing empirical models and the poor universality of data. In this regard, it is imperative to carry out police data governance, which has far-reaching significance.

3.1. Police Data Governance is Conducive to Breaking down Data Barriers and Smoothing Data Sharing.

Before police data governance, the data of various departments were used for their own purposes, and a large number of data were redundant, old, missing and scattered. Due to the lack of channels and data standards and other factors, the data quality of global application construction was uneven, the statistics were inaccurate, and a complete data quality management system was not formed, so it was impossible to share the data effectively with other police departments and units. Moreover, the established information systems were not connected in general, and the phenomenon of "data island" existed for a long time because it was necessary to communicate with each other before obtaining data. Through data governance, the barriers between data can be effectively broken down, data can be opened and shared. After the data governance, the data of public security, transportation, network security and other functional departments can be comprehensively collected and analyzed in terms of information such as people, vehicles, things, places, events and organizations, breaking the barriers between various police types, units and business departments, and promoting the transformation of all business departments to integration and overall linkage.

3.2. Police Data Governance is Conducive to Further Mining Data Clues and Enhancing Data value

Before police data governance, data work was mainly to meet local business needs, lacking overall and global considerations. "One system for one matter" occurred from time to time, and the data of each system was split, making it impossible to mine multi-level relationships. Data governance is conducive to multi-layer relationship mining, value clues mining, efficient analysis and collision comparison of data of various departments, and cross-data model analysis, so as to expand the connection between data and enhance data value.

3.3. Police Data Governance is Beneficial to Serving the Practice of Public Security Departments and Expanding the Results of Data

In view of the fact that the quality of data directly affects the effect of public security work in practice, data governance can comprehensively improve the quality of data to meet different business needs, which is conducive to the data close to practice, empowering actual combat, and realizing the availability and usability of data. At present, the public security informatization has become a comprehensive and comprehensive data analysis work to comprehensively improve intelligence judgment, early warning and prevention, risk perception, etc., because data governance can comprehensively perceive the informatization data results of different regions, police types and departments, and realize the integration of data and business, and at the same time can quickly test error mechanism through fusion calculation, so that more data can be generated from data, more valuable data can be obtained, and the data effect can be continuously expanded [5].

4. Current Situation of Police Data Governance

4.1. The Backward Concept of Policing Data Governance

For a long time, a deep-rooted public security work mode and thinking have been formed in public security organs in China, i.e., police data governance is a top-level design problem. Therefore, in addition to the top management, a large number of other police officers have not paid enough attention to the governance of police data in their concepts. There is a problem of insufficient understanding of police data governance, probably because of the lack of understanding and in-depth analysis of the characteristics of police data governance, and the lack of understanding of the great value of data governance, and the belief that data governance can only be mastered by technical departments in public security organs; or lack of enthusiasm and initiative for work, unwillingness to change the previous work mode, and reliance too much on habits and experience; or they are accustomed to the traditional case-handling mode, lack of active knowledge awareness of new technologies and methods, and continue the traditional working ideas and methods in actual work, which leads to the fact that police data governance has not been implemented and can't really play its role; or there is a preference of funds and construction to later maintenance and management, so that police data governance presents a formal and superficial problem [6].

4.2. Unclear Police Data Governance Process

At present, there is still no unified workflow standard and specification for data governance and a lack of scientific and unified top-level design, leading to various departments to carry out data governance in accordance with their own ways and methods. In addition, due to the absence of specific process specifications, each link and step of data governance are different, so it is difficult to achieve interoperability of data between departments and units, and it is difficult to predict whether governance can be effective or not.

Due to the lack of top-level design, lack of management norms, imperfect system, and lack of basic data planning, many basic data are repeatedly constructed in various business systems. Moreover, these systems adopt different standards and rules, resulting in scattered data storage and inconsistency due to redundancy. In addition, due to the lack of power and responsibility system for data governance, problems such as who should design the data planning, what work should be undertaken by the business department, and which should be undertaken by the information technology management department will arise, with unclear rights and responsibilities. In addition, data incomplete problems such as lack of key basic data, missing or incomplete part of auxiliary data, and serious historical data loss may even arise [7].

4.3. Insufficient Service Capacity for Police Data Governance

With the gradual improvement of the foundation of public security informatization and the continuous improvement of the thinking of "smart police" in various units and functional departments, all departments are eager to master the data services with wider scope, more types, quick response and accurate results. However, at present, there are some practical problems in the construction of data governance in public security organs, such as insufficient governance level and technical means, which leads to the fact that the service ability after data governance can't meet the actual needs. Due to the different technical levels of various departments of the public security organs, and the obvious deficiencies in the follow-up of the public security organs' governance techniques when compared with corporate data governance in the society, the collection, analysis and judgment of data resources cannot be carried out comprehensively and effectively in the governance process, and the governance activities of advanced technologies cannot be carried out, which makes the service capability of data governance difficult to meet the practical needs.

4.4. Unsatisfactory Depth of Police Data Governance

The police data governance of the public security organs needs to be further deepened, because the value of police data resources has not been given full play. However, at present, the public security organs' data governance in the application field of data resources is still at a low level and has not reached the proper governance depth, so the comprehensive utilization of police data and data value-added services need to be further strengthened. If the data can't be fully mined in depth after the data governance work, so that a large number of police data can be comprehensively analyzed to serve the actual combat business and public security decision-making, it will be meaningless. At present, each unit's failure to attach importance to data governance in thought and the lack of norms of data governance result in less attention and dependence on data governance departments. At the same time, data governance departments have no goals, which leads to ineffective governance and absence of in-depth governance.

5. A Study on Workflow and Business Frame Construction of Police Data Governance

Currently, the core goal of police data governance is to unify data resources. Specifically, it is required to form a "big reservoir" of public security data resources in accordance with the top-level design requirements of the general plan for big data construction of the Ministry of Public Security, which is "all resources, resources catalogued, catalogued globally and standardized globally", and obtain internal public security data in an all-round way and other social data resources such as internet enterprises, government departments, industry units and the like in accordance with the law and regulations in accordance with the principle of "doing everything according to the needs" and "not for everything but for use". The "six big databases" of original database, resource databases, subject databases, knowledge databases, business databases and business element index databases should be built to form a "big reservoir" of data resources to highlight the role of data governance in this process. No public-security organization or department is allowed to build a "small reservoir" of data resources.

Based on the current working practice of police data, it is believed in this paper that the working path of police data governance should focus on the realization of the landing of the "big reservoir" of police data resources. According to the idea of "data governance is the foundation", the problems of nonstandard, poor quality, weak timeliness, and low sharing of police data in public security organs will be solved steadily through phased data governance, and the data governance process oriented to data services should be constructed, laying a solid foundation for the landing of "big reservoir".

5.1. Work Flow of Police Data Governance

According to the workflow of general data governance, the police data governance process is put forward in this paper, as shown in Fig. 1. The police data governance needs to be steadily promoted by stages. To be specific, data governance work plan, task decomposition, project organization, template preparation, etc. are carried out in the preparatory stage of governance; the current situation of public security informatization, the actual demands of units or various police, and the network situation are understood at the stage of investigation and research on the current situation; multi-party argumentation is carried out, a data governance plan is formulated, and then the plan is strictly followed in the plan planning stage; systems, database tables, database fields, standards and specifications are sorted out in the stage of data sorting; the resources formed by combing are registered in time in the resource registration stage; the extracted data and data quality are judged in the data extraction stage; the data standard specifications are determined and the data are standardized according to the standard specifications in the data standardization stage; data governance organization and mechanism are established, and data governance is empowered in the functional stage of data governance; and the data service is developed and the data application is promoted in the application service and promotion stage.

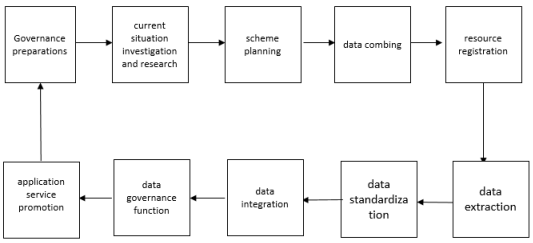

Figure 1. Workflow of police data governance

5.2. Business Frame of Police Data Governance

Police data governance, a complex and professional work, runs through the whole life cycle of police data. Its business framework is mainly based on ensuring data security and unifying data standards, and closely revolves around each link of the life cycle of police data in actual combat scenarios, namely, "data access-data processing-data organization-data service", which are designed to better meet the needs of public security business scenarios. The key points of data governance in each link will be discussed in the following.

5.2.1. Data access

Data access refers to the data reconciliation between multi-source heterogeneous data and the data provider by defining the process, method and circulation mechanism of data acquisition, processing, governance, organization and service at the initial stage according to the public security business requirements, and by accessing the data center according to data exploration and definition. In this process, data access with data governance as the core is divided into four steps: data exploration, data definition, data reading, and data reconciliation. Data exploration refers to multi-dimensional exploration on source data storage location, provision method, total amount and update status, business meaning, field format semantics and value distribution, data result, and data quality, so as to achieve the purpose of understanding data and provide a basis for data definition. Data definition refers to the process and method of data acquisition, processing, governance, organization and service in the initial stage according to the data exploration results and the public security business requirements. The data definition results are described and output in the form of metadata, which is dynamically maintainable and provides calling services. Data reading refers to extracting data from a source system or reading data from a specified location to check whether the data is consistent with the data definition. If there is any inconsistency, the access shall be stopped, the data shall be probed and defined again, further access shall be performed uniformly, necessary decryption and decompression operations shall be performed on the data, the record ID acting on the whole life cycle of the data shall be generated, and the data shall be subjected to character set conversion, etc. to form a format meeting the data processing requirements. Data reconciliation refers to the process of checking and verifying the integrity, consistency and correctness of the data of the data provider and the data access party at a certain reconciliation time node for the data access link. If the number of data

corresponding to the data provider and the data access party is inconsistent at a certain accounting point in time, it will be recorded as an exception in reconciliation, and an alarm will be given if necessary.

5.2.2. Data processing

Data processing needs to be carried out around the goal of data governance, and the core task is to realize data appreciation, data preparation and data abstraction for the big data features of huge scale, diverse types, high-speed flow, complexity and changeability, uneven quality and different value densities according to the data definition of data access links, with the data application as the guidance, and the data value density as the enhancement through standardized processing, and the data intelligent application as the data value increment, data preparation and data abstraction [8]. The data processing process is carried out in the order of data extraction, data cleaning, data association, data comparison, data identification and data distribution, as shown in Table 1.

Table 1. Introduction to data processing process

	Data extraction	Data cleaning	Data association	Data comparison	Data identification	Data distribution
Definitions	The destination format data is extracted from the source format data according to the result of data definition.	According to the data definition results, data filtering, de-duplication, format conversion, verification and other operations are performed to generate data meeting the standards and quality requirements. Data are reviewed and validated, non-compliant data are filtered, duplicate data are deleted, erroneous data are corrected, format conversion is completed, and data consistency is checked before and after cleaning.	According to the association rules or algorithms in the data definitions, the data are associated with other knowledge data, business data, and the like, and association information is output, so that association backfilling, association extraction and association analysis are supported.	In the process of data processing, structured data and unstructured data are subjected to the same comparison or similarity calculation according to the rules, and the data that hits the rules is output according to the output description, which is often used for information control and information subscription.	Based on the tag knowledge base, the tag engine is used to compare and analyze the data, calculate the model, and tag it to provide support for the upper application.	Based on different application scenarios, according to the distribution strategy defined by the data, the information such as association, relationship, labels and the data itself are processed synchronously or asynchronously, and the resulting data are distributed to the original database, resource database, subject database, knowledge database and business database.
Functions	Structured data extraction; Unstructured data extraction: text information extraction, video information extraction, audio information extraction and image information extraction.	Filtering, deduplication, format conversion, verification	Association backfill, associated extraction, association analysis	Structured comparison; unstructured comparison: keyword comparison, binary comparison, document comparison, multimedia comparison and biometric comparison.	Common and business tags, rule parsing, rule routing, rule compilation, rule execution	Task scheduling, distribution task queue, data distribution, distribution statistics, checking accounts, task monitoring

5.2.3. Data organization

As the key link to implement the goal of police data governance, data organization realizes the classification

and database building of data resources around the goal of building unified data resources, according to the data application requirements, and according to the organization scheme with unified standards and standardized processes defined by data, and further strengthens the internal connection of public security big data in the whole world and even the whole country, including original database, resource database, subject database, knowledge database, business database and business element index database.

(1) The original database is a collection of data used to retain the original data and reflect the original business scene, mainly including: public security law enforcement and duty data, Internet data, telecommunication network data, Internet of Things data, video network data, industry private network data and other data, etc.

(2) The resource database is a public collection of data that integrates the key elements of the establishment of various data resources, i.e. various identification attributes, such as citizenship number, license plate number, mobile phone number, etc., as well as the associations and relationships among the elements.

(3) Subject database is a collection of public data with multiple dimensions, which is established to facilitate work and accurately and quickly reflect the whole picture of the work object, and integrates all kinds of original data and resource data, and is accumulated for a long time around the subject object that can identify people (the theme of people), places (both offline and online), cases (basic files, case process, case handling, etc.), events (basic files, event process, event handling, etc.), things (vehicles, online terminals, guns, etc.) and organizations (non-governmental organizations, religious organizations, etc.), and information (public opinion information, harmful comments, etc.).

(4) Knowledge database refers to the collection of shared knowledge data and rules and methods in the public security field, including the knowledge data needed for data access, processing, governance, organization and service, the collection of various rules, methods and processes, and the knowledge data and general algorithms needed by various general models in the public security field.

(5) The business database is a database of businesses in various professional fields, which supports data in various professional fields, such as political security, terrorism and drug-related businesses, records business processes and provides data support for various business activities.

(6) Business element index database is a global index of key elements of business database, which is mainly used to solve business association and business conflicts.

5.2.4. Data service

To some extent, data service is one of the links to test the effectiveness of data governance. It refers to the access and management capabilities of various data resources, including original database, resource database, subject database, business database, knowledge base, metadata, data resource directory, etc. According to business needs, public security organs can develop various types of scene services.

(1) Query and retrieval service: It includes the query and retrieval interfaces of data resources, and various structured and unstructured data, supporting precise or fuzzy, classification, combination, batch and other query methods, supporting the return of statistical summary information of data, determining whether query keywords (entities) hit (exist), and data summary or detail information.

(2) Comparative subscription service: It is an information subscription service for one or more dynamic activities.

(3) Model analysis service: It refers to the data statistics, analysis, regular exploration, prediction, etc. according to the business needs and results return to support the complex and changing needs of the application layer business scenarios.

(4) Data push service: it is the basic core capability of data exchange and information push between nodes at all levels of the public security big data platform and between other departments inside and outside the public security network, mainly including data aggregation and data distribution. The former refers to collecting data resources from cities to provincial and ministerial data centers according to needs, or importing them from outside the public security network in one direction and collecting them to the corresponding data centers at all levels, while the latter refers to distributing data resources from provincial data centers to subordinate data centers according to needs.

(5) Data authentication service: It is the process of identifying the access rights of data based on the access control rules of data. Access control rules control resource permissions from four dimensions: content sensitivity, data source, data type, field and field relationship classification. Resource authentication uses data resource permissions of users and data authentication services to control access to data resources.

(6) Data operation service: It refers to operation interface services such as adding, deleting and modifying data and data tables [9].

(7) Data service management: It refers to the interface encapsulation of data governance and data service capabilities as needed to provide services for other application systems and other subsystems in the platform

5.2.5. Data governance

Data governance is the planning and design, process control and quality supervision of the whole life cycle of data resources. Standardized data governance can make data resources transparent, manageable and controllable, clarify data assets, improve data standards, standardize data processing processes, improve data quality, ensure the safe use of data, and promote data circulation and value refining [10]. This process includes seven contents: "data resource catalog, data classification, data lineage, label management, model management, data quality management, data operation and maintenance management", in which the data resource catalog includes:

catalog update, catalog registration, aggregation and distribution, and catalog query; data classification includes: examination and approval, classification management and authorization management; data lineage includes: data map, blood relationship analysis and influence analysis; label management includes label management, label model management and label life cycle management; model management includes: visual construction and optimization, model evaluation, algorithm management, training data management, model management and model publishing; data quality management includes: data quality evaluation dimension, quality check rules, data quality check, quality problem monitoring and early warning, problem handling and tracking, and data quality evaluation [11]; data operation and maintenance management includes: data resource monitoring, data processing monitoring, data service monitoring, data access monitoring, data quality display and abnormal alarm information.

5.2.6. Data security

In data collection, data access, data processing, data organization, data governance, data service and other aspects, corresponding security measures should be taken to ensure data security and the reasonable and compliant use of police data. In the process of data governance, the strategies, standards and measures of data security should be defined around the data security life cycle, and the data security construction should be carried out through data classification, data encryption, data desensitization and other technologies [12]. Data classification is the basic work of data security. It determines the degree of data sensitivity according to the multi-dimensional characteristics of data, and provides a support for the development of data resources opening and sharing strategy [13]. In the follow-up links, the corresponding security protection measures should be taken to ensure the data security depending on the data classification.

The methods of acquisition transmission security, acquisition equipment authentication and the like can be adopted in data acquisition link, reconciliation service access control, data read access control and the like can be adopted in the data access link, data distribution privilege account management can be adopted in the data processing link, data authentication, data authorization, data operation audit, highly sensitive data encryption and the like can be adopted in the data governance link, file encryption, database encryption and the like can be adopted in the data organization link, data service access control, data service, data authorization, data authentication, data leakage detection, data destruction, etc. can be adopted in the data service link to ensure the data security.

6. A Study on the Strategy of Promoting the Integration of Police Data Governance and Business Work

6.1. Improving the Concept of Modern Police Data Governance

In the entire public security system, everyone should strengthen the awareness of data governance, deeply understand the value of data, attach importance to data governance, establish the data governance concept of "using data thinking to help intelligent police to promote leapfrog development", and strive to achieve "more data exchange to reduce police leg work".

The concept of "jumping out of public security business and fully perceiving data" should be set up. From the perspective of comprehensive data services in various fields, public security is the police big data, which integrates police business data such as public security, transportation, intelligence and command with data from relevant government departments, data from various social fields and open internet data to form a police data lake.

The concept of "transformation from 'business data' to 'data business'" should be set up. Information systems in various fields, such as government data, social data, Internet data, etc., should be data-driven and data-converged with internal information systems of public security, forming a mode of data service support for actual combat, such as judgment and early warning, risk insight, emergency response, public security prevention, investigation and case solving, and realizing the transformation from "business data" to "data business" to better serve the practice.

The concept of "data speak for themselves" should be set up so that we can know early and ask "what data do we have, what data do we need and what can we do with data" all the time in the process of governance. For example, we can make the actual population collection more comprehensive by using social data to grasp the dynamic situation of rental housing use; we can avoid small incidents from evolving into large incidents by using population and case data to grasp the background of alarm, we can make the prevention and control effect more obvious by using track data to grasp the area of key personnel activities, we can organize diversion and guidance in advance by using traffic data to grasp the congestion of vehicle on the roads.

The concept of "data serving the policing practice and promoting continuous innovation" should be set up. In the process of data governance, the concept of "all for the actual needs" should be upheld and the actual application should always be taken as the lifeline of data governance. The purpose of data governance is to serve the practical business and continuously innovate, and continuously innovate under the existing mechanism to form new technology application, police service mode and social service.

The concept of "a new police service mode of coordination, precision and initiative" should be set up. In the process of data governance, data aggregation should be carried out in real time to push the intelligence information in real time, to enhance the ability of intelligence and service integration, and to make the cooperation between departments more collaborative. Holographic characterization of business characteristics should be conducted to analyze and mine high-risk personnel and groups to improve the efficient and accurate investigation ability, so that the investigation management is more accurate. Crime prediction results should be actively fed

back to the patrolling force for accurate deployment, to enhance the active fighting and prevention control ability, so as to make risk prevention more active.

6.2. Building a Professional Team of Police Data Governance Talents

As talents are the fundamental driving force of police data governance to a higher level, the training of talents for police data governance should be strengthened. In every link of data governance, professional talents are needed to support the entire process because the use of specialized talents in the process of data governance, that is, the composite talents who understand the practical business of public security and master the data governance technology, will directly affect the overall effect and level of police data governance. Therefore, the public security organs should focus on building a professional team of data governance talents, cultivate data governance talents through various channels, and form a public security human resources system matching with data governance by combining with the reform of police technology sequence, which not only reflects the attention to talents, but also satisfies the realization of talents' self-value, and enables them to better serve police data governance [14].

Talents should be trained through scientific research institutes. At present, the key link of police data governance needs to rely on external information technology enterprises, which will inevitably lead to enterprises' incomplete understanding of public security business, disconnection between research and development and the needs of public security business, and limited value in practice. Police data governance personnel should have professional knowledge and skills of big data, be familiar with public security business, have actual combat experience of public security, and be compound talents with technical development ability, public security business knowledge and industry application quality. Scientific research institutes should be adopted to cultivate advanced technical means of police in the field of data governance, organize and carry out purposeful, organized and planned professional training, and improve the quality level of police in this field, which can solve the current technical problems of police data governance from the source [15]. Talents should be trained through practical positions. In carrying out the police data governance, technological progress should not only be pursued continuously, but also be closely related to the policing practice, always adhering to the practice orientation. The technical personnel of data governance must have the experience of practical positions before they can understand how advanced technologies are related to practice, which technologies are needed in practice, which technologies are in urgent need of breakthrough at present, and so on. Only in this way can the data governance personnel be more specialized, the data governance team be more targeted, and the whole team can be mobilized to solve a series of problems of current data governance in a targeted manner, so as to achieve "integrating theory with practice" without breaking away from the actual needs of public security.

Talents should be introduced through market resources. Public security organs can recruit data governance professionals from the whole society. They can provide special resources that social enterprises cannot provide to form their own advantages and improve their competitiveness. Although the salary of management talents recruited by public security organs is not as good as that of society, it can provide a broader platform and corresponding development to make them more secure. According to Maslow's hierarchy of needs theory, people ultimately need to realize the need for respect and self-realization, and the public security organs can provide a broad platform to meet their self-realization needs. At the same time, the introduction of market talents will also inject fresh blood into public security organs. The original staff and newly introduced staff will communicate and cooperate with each other, stimulate the subjective initiative of the original staff, and enhance the overall combat effectiveness of the data governance team.

6.3. Improving the Organization System of Police Data Governance

The organization system of police data governance should be established and improved, and a data governance leading group with special leadership and responsibility, a data governance committee group composed of top-level public security managers, data managers and business managers, should carry out the top-level design planning of police data governance, lead lower-level business departments and units to carry out data governance work, open up the inter-departmental coordination and linkage mechanism, and form a closed-loop data governance business. At the same time, the institutional setup, functional allocation and operation mechanism of the current police data governance should be reformed and reorganized to define the functional boundaries of various departments, and build a data governance operation mechanism with clear responsibilities and efficient operation. The data standard group composed of the backbone of the business department of the public security organ, social information technology experts and data governance experts should be sound, the formulation of various standards of police data should be completed, and a complete police data industry standard should be formed, so that the data collected by each unit can have rules to follow.

At the same time, the multi-subject governance mechanism should be established to strengthen communication and coordination with social enterprises, so that enterprises can participate in the process of police data governance, promote the integration of police data and social data, learn and use advanced governance methods and perspectives in society, form a multi-governance mechanism of co-governance between police and enterprises, and constantly improve the level of police data governance.

According to the thinking of the police data governance organization system on the "strips", the respective perfect organization systems should also be constructed on the "blocks" of the four links of data acquisition, storage, use

and maintenance, so that each link has a separate organization system suitable for its own work, and the requirements on the "strips" of the organization system are ensured on the big thinking, and the data acquisition, storage, use and maintenance organization system meeting the work needs is established on the "blocks" of the governance link according to the actual work needs.

6.4. Establishing a Diversified Application System of Police Data

A standardized and global convergence mechanism should be established. Data collection and aggregation is the premise and foundation of data governance. The more types and dimensions of data are aggregated, the higher the value of the results will be. According to the principle of "collecting everything together", the internal data of public security organs should be consolidated, relevant mechanisms should be established, social data should be collected legally and in compliance, data sharing and exchange with other government departments should be expanded, and internet data collection should be strengthened in various ways, so as to achieve the real-time perception of "people, events, things and places" by public security organs.

An intensive and flat convergence system should be established. The public security private network or new channels should be established to build a flat data aggregation channel from the terminal to the cloud, so that the data perceived by the basic level can be aggregated to the core data center in real time, and the timeliness of data can be guaranteed. The newly acquired data can be deeply explored as soon as it is uploaded, so that the value of the data can be fully released immediately to serve the practice of the public security, which not only accelerates the efficiency of serving the public security business, but also ensures the timeliness of the data, and enables the speed of "devaluation" of the data to be in the hands of the public security organs.

A platform of extensive acquisition and rapid application should be established. A "data repository" or a unified data resource system should be constructed based on data collection, with resource integration as the means and application sharing as the goal. At the same time, different business requirements should be integrated to form a variety of thematic application databases such as comprehensive applications, vehicles, personnel and communication methods. Finally, the same platform should be integrated to ensure rapid application when actual combat requires.

7. Conclusions

Police data governance is not a temporary and phased work, but should run through the data work all the time. At present, the most important thing is to change thinking and look at data governance from a strategic overall perspective, change the original governance concept, follow the modern police data governance process, give strong support to the data governance work in terms of data standards, technical support, mechanism and system, and personnel team, and effectively improve the police data governance capability, so that multi-party data can play its value, truly serve the actual combat business of the public security, and realize the benefits of the police and the people.

Acknowledgment

Supported by the *Research on Blended Teaching Mode Based on OBE Educational Concept* (2021JYB06); *Evolution and Status of Capital Public Security Organs* (2021KZD10)

References

[1] Zhang Ning, Yuan Qinjian. Review of data governance research. Journal of Information, 2017, 36(05):129-134+163.
[2] Chen Xiaojun. Research on the Technology-Side Mechanism of Digital Transformation of Retail of Small and Medium-Sized Banks. Technology Wind, 2022(08):166-168.
[3] Research Group of Huzhou Public Security Bureau, Jiang Jianqiang. Some Thoughts on the Construction of Social Security Prevention and Control System Under the Condition of Data Governance Based on A Case Study of Huzhou Public Security Organs. Journal of Public Security (Journal of Zhejiang Police College), 2019(01):63-67.
[4] Research Group of Huzhou Public Security Bureau, Jiang Jianqiang. Some Thoughts on the Construction of Social Security Prevention and Control System Under the Condition of Data Governance Based on A Case Study of Huzhou Public Security Organs. Journal of Public Security (Journal of Zhejiang Police College), 2019(01):63-67.
[5] Zhu Xiaoyu, Zheng Ting. Research on Data Governance in Public Security Big Data Scenario. Journal of Public Security (Journal of Zhejiang Police College), 2020(03):113-117.
[6] Wei Guowei. Problems and Countermeasures of Public Security Informatization Construction under the Background of Big Data. Theory Observe, 2018(09):87-89.
[7] Yuan Ming, Gu Haiyan, Qian Hanwei. Challenges and Countermeasures of Data Governance in Police Colleges under the Background of Big Data. Journal of Jiangsu Police Officer College. 2018(06):118-121.
[8] Wu Xindong, Dong Bingbing, Du Xinzheng, Yang Wei. Data Governance Technology. Journal of Software. 2019(09):2830-2856.
[9] Zhou Dingtian. Construction and Empirical Study of Evaluation Model of Smart Police Data Governance. Xiangtan University, 2020.
[10] Dong Chunpu. The Historical Change of Police Operation Mode in New China. Journal of Jiangxi Public Security College, 2019(02):43-47.
[11] Zhou Dingtian. Construction and Empirical Study of Evaluation Model of Intelligent Police Data Governance. Xiangtan University, 2020.
[12] Zhu Xiaoyu, Zheng Ting. Research on Data Governance in Public Security Big Data Scenario. Journal of Public Security (Journal of Zhejiang Police College), 2020(03):113-117.
[13] Li Songtao, Xie Zongxiao. Analysis on Data Classification and Related Standards. China Quality and Standards Review, 2019(04):14-16.
[14] Zhu Xiaoyu, Zheng Ting. Research on Data Governance in Public Security Big Data Scenario. Journal of Public Security (Journal of Zhejiang Police College), 2020(03):113-117.

[15] Li Xin, Hu Shiyan. Research on the Construction of Public Security Big Data Talents. Journal of People's Public Security University of China (Science and Technology), 2019, 25(03):18-21.