Application of Big Data in Public Security Governance: Dilemma, Risk and Optimization Path

Xin Xie[1], Xiaofeng Luo[2,*]

[1]e-mail: cuitll@qq.com

[2*]Corresponding author: e-mail: 646013637@qq.com

[1]Department of police management Sichuan Police College Luzhou, China

[2]Department of computer science and technology Sichuan Police College Luzhou, China

Abstract—In public security governance, big data is playing an increasingly important role, which also puts forward higher requirements for the comprehensive utilization ability of data and data mining and analysis ability of public security organs. At present, there are some problems in the application of big data in public security governance, such as the lack of effective integration of data, weak data processing ability and low quality of data collection, as well as the risk that citizens' privacy is easily violated, algorithm discrimination, data leakage and illegal use. We need to optimize the application of big data in public security governance by integrating and sharing data resources, improving technology application level, improving data collection quality, strengthening data security protection and promoting the integrated development of big data, artificial intelligence and police blockchain in public security governance.

Keywords- big data; Public security governance; Optimization path

1 INTRODUCTION

We have entered the era of big data. Today, as a valuable asset, data resources play an important role in many aspects of our lives. In many fields, including public security governance, the value of big data has been gradually reflected and the scope of application is becoming wider and wider. In the context of big data, complying with the requirements of police informatization reform and accelerating the application of big data in public security governance can not only innovate the social governance model, but also greatly improve the intelligence analysis and judgment ability of public security organs, which is conducive to maintaining national security and social stability.

The rapid development of Internet technology puts forward higher requirements for the comprehensive utilization ability of data and data mining and analysis ability of public security organs. Actively using big data, artificial intelligence and cloud computing to improve the information construction level of public security organs is the key link to improve the ability of

ICIDC 2022, June 17-19, Qingdao, People's Republic of China

DOI 10.4108/eai.17-6-2022.2322735

public security governance. At present, some big data products with early warning nature have been used in public security investigation and traffic management, but there is still a big gap from the real intelligent application. To fully understand and master the theory, thinking and technology related to big data and build a systematic intelligent public security governance system is the direction of our work for a long time in the future.

2 The dilemma of big data in the application of Public Security Governance

2.1 Lack of effective data integration

The application of big data is a highly integrated system engineering, which involves many aspects such as data, algorithm, Internet, Internet of things and artificial intelligence. For a long time, all subjects of public security governance, especially the grass-roots public security departments, do not have the awareness of resource sharing in the construction of information system. The characteristics of system construction and information utilization are obvious, resulting in many valuable information can not be fully utilized, and the phenomenon of "information island" is more common.

The ability of information collaboration among various departments of public security organs is insufficient, and a large number of business data are lack of integration. It is difficult to form an effective correlation between these elements of "personnel time place materials events". The utilization and sharing of data are relatively low. With the development of monitoring technology and the widespread use of monitoring equipment, public security organs can obtain a large amount of video monitoring information at a low cost. However, due to the existence of information barriers among various departments, the application of using trajectory to mine relevant social relations in practical work is rare. This situation makes the role of the important investigation means combined with the social connections of the suspect track not to the maximum extent. It is difficult to determine the scope of investigation quickly and accurately, and weaken the ability of public security organs to solve cases.

2.2 Weak data processing ability

The effective processing of data is as important as the acquisition of underlying data. In the face of massive data, the public security organ needs a very strong data analysis ability to process the data timely, scientifically and efficiently. This ability is a kind of comprehensive ability. On the one hand, it involves the specific application of basic theories such as Criminology and criminal psychology; On the other hand, it is necessary to build a practical analysis model with the help of modern information technology. At present, there are many problems in the actual combat, such as the prediction model of recidivism of key personnel in the category of financial invasion, the analysis and mining model of high-risk personnel and groups, the analysis and mining model of abnormal addresses of key personnel, the analysis and mining model of high-risk vehicle fraud high-risk personnel and groups, etc. for example, in the analysis of the law of crime, The analysis focuses on the characteristics of suspect and the time and place of crime [1]. However, the analysis of the suspect's characteristics basically adopts the non real time perception data of the traditional criminology research, such as the psychological and emotional state, the income situation and the pressure situation. In fact, the data we get are more fragmented, which can not meet the requirements of model prediction. In the analysis of the time law of crime, the public security department mainly focuses on the conventional time points, less on a longer time period, and the analysis of specific time points (such as festivals) is not in place.

2.3 Low quality of data acquisition

Data quality is the lifeline of big data. Data quality consists of two factors: one is the quality of the data itself; The second is the quality of data process. The quality of the data itself requires that the data must truly and accurately reflect the actual situation, the data related to the event is complete, and the constraints of the data shall not be self contradictory. The quality of data process mainly emphasizes that its use should be standardized. For example, the data must be stored in the specified medium to ensure that it will not be disturbed by external factors.

The quality of data related to public security governance is mainly determined by the collection level of basic data of public security organs. Limited by the collection conditions and ability of grass-roots police, many basic data, especially dynamic data, are distorted. For example, some community police mainly relied on the consciousness of residents and did not carefully check the relevant data when filling in the data of standard address, actual resident population, real houses, actual business units, industrial sites and employees. Once these basic data are wrong, it will seriously affect the effect of data analysis.

3 Risks of big data in the application of Public Security Governance

3.1 Risk of infringement of citizens' privacy

The use of big data not only facilitates our life, but also greatly improves the efficiency of public security governance. Modern data technology uses various ways to collect different types of data in order to identify people more accurately. From the perspective of privacy protection, the data information of public group users collected by public security governance can not be regarded as an infringement of citizens' privacy. However, through the processing of these data, we can accurately infer personal information, such as citizens' biometric information, financial product information, genetic information, even life trajectory and behavior preference, so there is a risk of infringing citizens' privacy.

The application of data belongs to the initial stage in China. During this period, there is no consensus on the protection of the rights and interests of various subjects and the right attribute of data object in the application of data processing, and there is also a lack of specific basis at the legal level. In addition, the development of information technology in the era of big data has broken through the boundaries of time and space. The "4V" characteristics of big data: volume, variety, velocity and value have greatly increased the difficulty of privacy protection. Of course, it also further magnified the negative impact caused by privacy disclosure.

3.2 Algorithm discrimination risk

The data itself is objective and should be regarded as neutral. However, in the era of big data, there is a huge risk, that is, data collectors choose data based on their subjective preferences. Then, such data itself contains some bias, which makes some specific objects unfairly treated.

The simplification and classification of the algorithm will objectively ignore the existence of object heterogeneity. Usually, the designer of the algorithm will simplify the features of the object through some common features, then divide it into specific categories, and give targeted program instructions to different groups. When people are regarded as algorithm objects, some common features are used to classify people, which obviously ignores the complexity of individuals. Algorithm discrimination not only leads to the deviation of data analysis results, but also causes great harm to the personal rights and interests of specific groups. With the development of artificial intelligence, information asymmetry such as algorithm "black box" will make discrimination more hidden and difficult to be detected by people. For example, when predicting the future crime rate, the US police mainly analyze it based on historical arrest data. In fact, in the daily process of law enforcement, the American police will pay more attention to people of color and low-income groups. These groups will be mainly considered in data analysis, which will strengthen the racial bias of the police, resulting in algorithmic discrimination.

3.3 Risk of data leakage and illegal use

The public security big data platform collects a large amount of data. If these data are leaked or used illegally, it will bring huge risks. Data itself contains value. Because of this, it is very easy to become the target of criminals. At the same time, it is also illegally used by insiders. The risks of data leakage and illegal use are mainly caused by the following factors: first, big data business is more and more widely used in public security departments; Second, the source and structure of basic data are becoming more and more complex; Third, the data itself involves many departments, especially many non public security departments; Fourth, the popularity of mobile data terminals; Fifth, many grass-roots departments lack classified management of data; Sixth, unstructured data (such as video, pictures, etc.) increases the difficulty of screening classified information [2].

In terms of illegal use of data, in recent years, the public security organs have strengthened the education and supervision of police and police auxiliary personnel, but the monitoring system for compliance use of data is difficult to cover all data resources and their application systems. Of course, the confidentiality awareness of some police officers is not strong, resulting in the frequent occurrence of illegal use of data.

4 Optimization path of big data in the application of Public Security Governance

4.1 Integrate data resources and realize data sharing of Public Security Governance

Public security big data governance is a new governance form based on the comprehensive development and utilization of relevant data resources. The full utilization of data resources is an embodiment of the modernization of governance ability. The primary task of integrating data resources and realizing data sharing of public security governance is to eliminate the phenomenon of "data island" in both internal and external aspects of public security organs, resort out business processes, break through barriers to data exchange, promote business cooperation through integrating data resources, and form business linkage between public security organs and relevant external departments.

From the perspective of information technology, the integration of data resources requires the construction of a whole process technical support system that can cover the integration and sharing of public security data resources through big data construction, and the use of technical means to ensure data collection, data collection, data association, data integration, data exchange, data storage, data management, data processing, data encryption, data transmission, data docking A series of processes such as data security guarantee and system platform support. The traditional technical support system mainly includes front-end database collection mode, database docking mode, application interface mode, agent mode, XML mode, etc[3]. Although these technologies can meet the current requirements of data integration and sharing, there are some problems, such as low processing efficiency, complex implementation process and unstable results. With the continuous development of information technology, cloud computing, blockchain and other technologies are more and more widely used in government departments, which technically provides a more optimized technology option for public security governance data integration. In addition, in order to break the information barrier and truly implement the concept of information sharing, as a condition for information exchange, some enterprises can be allowed to obtain the non confidential information of the public security department.

4.2 Improve the application level of technology and enhance the ability of data processing

Science and technology can greatly improve the level of productivity. Public security organs should enhance the awareness of active learning, improve the level of technology application, and accelerate the upgrading of big data processing technology. For example, in the face of massive unstructured data such as pictures and videos, if we can't make full use of them, it may have a negative impact on the effectiveness of public security governance. Through the improvement of big data processing ability, unstructured data can be transformed into structured data to generate intelligence information, so as to promote the multi-dimensional integrated application of information. Especially with the current large-scale use of video surveillance, transforming video surveillance information into structured data can make full use of the authenticity and full-time advantages of surveillance data.

Improving the technical level of the application platform is also an effective means to enhance the data processing ability. The construction of the platform should be based on the service practice, optimize the data processing process, and ensure the integrity and timeliness of the data. Try to establish a comprehensive data processing system jointly constructed and used by different regions and different police types according to unified standards and unified planning, strengthen data intensive construction, and realize that non secret related data business applications are carried by a unified platform, so that information resources can be fully utilized and economies of scale can be formed.

4.3 Improve data acquisition quality

There are many sources of public security governance data. In addition to the data from the public security organs, the data from telecom operators and Internet companies are also important components. To improve the quality of data collection, we need to formulate scientific and rigorous measures for the methods, process specifications and standard requirements of data collection in the three links of data collection, inspection and input, so as to ensure the standardization and institutionalization of data collection [4].By strictly checking and proofreading the collected data, improve the quality of the used data and ensure the accuracy and authenticity of the data.

Specifically, we should pay attention to the following points: first, the front-end data collectors should do a good job in data proofreading. For example, the community police should enhance their sense of responsibility. They should not upload the data directly to the system only according to the information obtained from the telephone survey. They should make a household survey or check with the community workers before deciding whether to enter the data. Second, the person in charge of verifying the data that does not conform to the logic can also verify the data that does not conform to the logic, and the person in charge of summarizing the data that does not conform to the logic can also verify the data that is invalid. Third, the technicians in charge of data analysis and processing should strictly follow the requirements of technical specifications to check whether the format of preliminary data summary personnel is standardized and whether the standard table script runs normally.

The quality of data collection is directly related to the use value of data. Many Internet enterprises have accumulated travel trajectories, consumption preferences, POI and other data of great value to public security governance. Public security organs should promote business docking with enterprises, especially accelerate the concentration of data in the field of public security and services, and improve the quality of data collection.

4.4 Strengthen data security protection

With the continuous development of information technology, all kinds of information platforms are more open than before. At the same time, the security threats are also significantly increased. The data is stored in the database, mainly transmitted through the network and displayed at the terminal. Therefore, to strengthen data security protection, we should start from the aspects of database, network layer and terminal layer. Relatively speaking, data transmission through the public security intranet is safer than data transmission through the Internet. If the conditions for intranet transmission are not met, attention should also be paid to encrypting the confidential data information when using the extranet, so as to ensure that the original data will not be leaked and used for other purposes [5]. In addition, we can learn from the use paradigm of "data available and invisible" to further ensure data security protection.

The data used in public security governance needs classified and hierarchical security protection according to the confidentiality level, and a technical system for data security risk prevention and control is established. In accordance with national regulations, promote the formulation of big data analysis and transaction prohibition list, strengthen the supervision of the three stages before, during and after the use of data, and establish a data consumption control mechanism. Within the public security organ, it is necessary to improve the staff's awareness of data security protection, continue to improve the mechanism of Hierarchical Authorization to access big data, and ensure that digital certificates and keys are only used by users themselves. The access to big data shall strictly abide by the confidentiality rules, and it is prohibited to access big data irrelevant to work or use big data beyond authority. In order to ensure that big data is not used illegally, the management department should strictly perform its regulatory responsibilities, record users' use of big data in detail, record access operation logs, conduct irregular supervision and audit, and seriously deal with malicious access.

4.5 Promote the integrated development of big data, artificial intelligence and police blockchain in public security governance

The application of artificial intelligence and blockchain has greatly improved the technical content of public security governance. The learning and reasoning ability of artificial intelligence can bring revolutionary changes to the verification of big data, and also provide strong technical support for the further improvement of public security governance ability and level. Artificial intelligence has promoted the change of public security governance mode in at least the following three aspects: first, artificial intelligence can combine with the police mobile terminal which has been widely used by the police to verify the identity by using face recognition and fingerprint recognition, so as to greatly improve the work efficiency of the police; Second, the use of artificial intelligence technology can solve the picture, audio and video unstructured data that has long limited the police's ability to analyze big data; Third, big data technology based on artificial intelligence plays a great role in urban community grass-roots governance. Using police mobile terminals, community police can more conveniently engage in information collection, data sharing and key personnel management and control of public security governance, reducing the workload of grass-roots workers.

In the construction of public security governance system, the public security department should make full use of artificial intelligence technology, pay attention to its value in data processing and scene simulation, and provide support for the analysis and processing of massive data in public security governance. Public security departments can use blockchain technology more effectively. Other public security management departments have cooperated with social organizations to expand the scope of data acquisition. Through the integrated development of big data, artificial intelligence and police blockchain in public security governance, network nodes in different regions and different types of police can be obtained and written respectively, and management permissions can be set. Using the tamper proof characteristics of blockchain technology, the "dirty data" can be excluded from the system to improve data quality. It can be predicted that the integrated application of big data, artificial intelligence and police blockchain will be more and more deeply and widely used in public security governance.

5 EPILOGUE

Promoting the application of big data in public security governance is conducive to further implementing the requirements of "reforming and strengthening the police" and "public security big data strategy", and is of great help to improve the intelligent level of public security governance and the work efficiency of public security organs. For a long time, building a "smart public security" model and promoting the in-depth reform and development of public security technology are important tasks faced by public security organs at all levels. We should recognize the importance of big data to public security governance and the urgency of practical requirements from a strategic perspective. The construction of "smart public security" model based on the development of modern information technology should pay more attention to the role of big data in public security governance, promote the information construction of public security technology through the integrated development of big data, artificial intelligence, police blockchain and other technologies, improve the combat effectiveness of public security organs, and enable public security organs to better perform the functions of combating crime, maintaining social order and serving the masses.

Based on the study of the problems and risks existing in the application of existing big data in the field of public security governance, this paper puts forward a model to optimize the application of big data in public security governance (Figure 1) with the goal of improving the quality of big data application, improving data quality, strengthening data security protection and promoting the integrated development of big data, artificial intelligence and blockchain. This model has nothing to do with specific technology and has no close relationship with specific products, components and services. This model not only attaches importance to the value and application of data itself, but also introduces privacy protection and integrated development with other technologies, which is more conducive to the improvement of the efficiency of big data in public security governance. Next, it is planned to conduct research from the aspects of mining and improving the accuracy of public security big data supply, exploring and building a data distributed search architecture, etc.

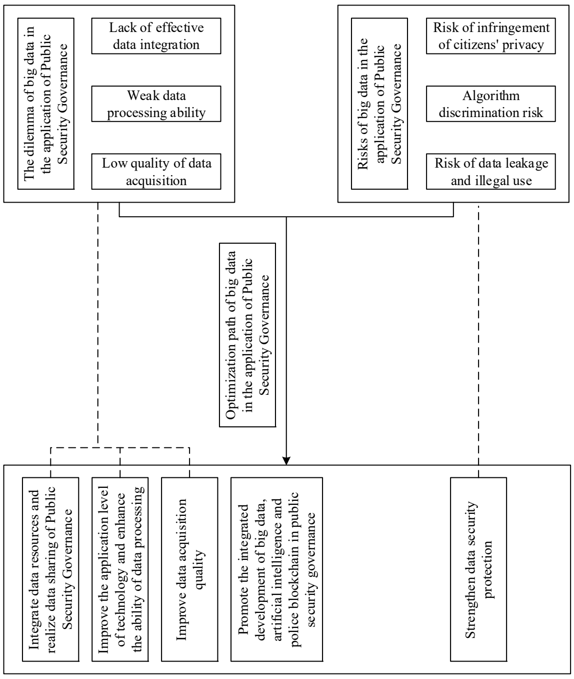
The dilemma of big data in the application of Public Security Governance
Lack of effective data integration
Weak data processing ability
Low quality of data acquisition
Risks of big data in the application of Public Security Governance
Risk of infringement of citizens' privacy
Algorithm discrimination risk
Risk of data leakage and illegal use
Optimization path of big data in the application of Public Security Governance
Integrate data resources and realize data sharing of Public Security Governance
Improve the application level of technology and enhance the ability of data processing
Improve data acquisition quality
Promote the integrated development of big data, artificial intelligence and police blockchain in public security governance
Strengthen data security protection

Figure 1 Analysis framework of big data application in the field of Public Security Governance

REFERENCES

[1] Sarah Brayne. “Big Data Surveillance: the Case of Policing,” American Sociological Review,2017,Vol.82(5), pp. 977 - 1008.

[2] Janet Chan and Lyria Bennett Moses, “Is Big Data Challenging Criminology?” Theoretical Criminology,2016,Vol. 20(1), pp. 21 - 39.

[3] Andrew Guthrie Ferguson, “Big Data and Predictive Reasonable Suspicion,” University of Pennsylvania Law Review,2015,Vol. 163, pp. 327 – 410.

[4] Pedro Domingos. “A Few Useful Things to Know About Machine Learning,”Communications of the ACM,2012,Vol.55, pp .78-87.

[5] Alkesh Bharati and Dr Sarvanguru RA.K. “Crime Prediction and Analysis Using Machine Learning,” International Research Journal of Engineering and Technology,2018,Vol.5, pp .1037-1042.