Macrothink Institute™

Journal of Social Science Studies
ISSN 2329-9150
2021, Vol. 8, No. 2

On the Protection of Personal Data Information in Big Data Investigation Activities

Xinzhao Pang (Corresponding author)

University of Maryland, College Park

Received: December 10, 2021 Accepted: December 23, 2021 Published: December 30, 2021

doi: 10.5296/jsss.v8i2. URL: https://doi.org/10.5296/jsss.v8i2.

Abstract

In the context of the vigorous development of big data and network communication technologies, the universality of personal data information processing, the openness of concept definitions, and the potential risks in practice have led to theoretical and practical changes in the definition of personal data information. With the widespread use of big data technology in criminal investigations, the theoretical and practical activities of big data investigation have gradually formed. Big data investigation activities are often accompanied by infringements on citizens' personal data and other legitimate rights and interests. At present, the traditional model of personal data information protection cannot restrict the code of conduct in big data investigation activities. For this reason, it is necessary to introduce a comprehensive governance model, which mainly includes relative control of individuals, balance of multiple interests and dynamic risk adjustment. Etc., and focus on the transformation of the legal protection model of personal information.

Keywords: big data investigation, personal data information, personal data information protection model

As a new scientific and technological method, big data is widely used in today's social life. In judicial practice, especially in the investigation stage of criminal litigation work, big data technology has provided assistance for case detection in the public security and procuratorial process, making investigation activities more efficient and easier to coordinate. However, it is undeniable that, as a new type of investigation mode, big data investigation activities are still immature and imperfect. The most prominent and serious problem is the violation of personal data information security and citizens' individual rights. How to treat this new investigation model dialectically, to sublate, and to explore a practical protection path for the protection of personal data in big data reconnaissance activities is also imminent.

1. Big Data Investigation Activities

(1) The concept of big data investigation

Defined from a macro perspective, big data refers to complex data that is large in quantity, diverse in variety, rapidly growing, and sparse in value under the premise of integrating a variety of today's advanced technologies. In short, it is a "large and complex" data set. As an information asset, it is necessary to use new processing thinking and interpretation techniques to realize the value of big data.

Investigation, to be specific, is a process stage of criminal proceedings. Public security organs and procuratorial organs usually investigate the truth of the case, which usually includes special investigations. When necessary, some compulsory measures can be taken. The investigation interval is generally opened by the case. The decision is made to decide whether to transfer for prosecution. The rapid development of computer and network communication technology and the digital informatization of citizen activity recording and control provide technical guarantee and support for big data investigation activities. Big data investigation is an advanced stage of informatization investigation. Compared with traditional investigation, big data investigation activities are generally mainly applied to the special investigation work of cases, that is, through the processing of big data information, the conclusion is summarized and the case Relevant clues or carry out big data processing activities based on known clues, in order to find more clues and determine the information and behavioral life patterns of the criminal suspect, so as to determine whether the criminal suspect is suspicious. At the same time, big data investigations also require investigators to change their previous thinking of handling cases, that is, they should have the thought of discovering the causal relationship between the cause and the caused by the evidence and the facts, and build a panoramic investigation without missing any data details. thinking.

(2) The necessity of big data investigation

In today's economic and social development, the number of cases of traditional crimes continues to decline. In addition to fraud, the number of violent crimes such as robbery, robbery and theft (ie "two robberies and one theft") has been well controlled; The number of traditional crimes continues to rise. This means that with the progress and development of economy and technology and low tolerance policies for violent traditional crimes, criminals are also exploring new and technological crime models.

Among the new crimes, the most prominent is cyber crime. Due to the characteristics of anonymity and concealment of the Internet, cybercrime presents a characteristic of high crime rate and low crime detection rate. Moreover, cybercrime presents a trend of ecological development with a fine division of labor, which has increased the number of crimes resolved. Difficulty. Therefore, this has also forced public security and other departments to change their thinking and mode of handling cases. In this process, improving the level of technical investigations and using big data in investigations can provide new ideas and new methods for the detection of these complex and difficult cases. Big data investigation also came into being.

2. The Impact of Big Data Investigations on Citizens' Personal Data

(1) Definition of personal data information

The extension of personal information is more extensive, including personal data information. Personal data information is a collective term for digitized personal information. Specifically, it is data left by individuals on the Internet or other digital media. These data can directly or indirectly refer to specific individuals. By aggregating these digitized information by certain means, the behavior patterns of specific individuals can be identified or predicted. At the current stage, personal data information is also diverse in variety and content, and the scope of legally protected personal data information can be effectively defined through some descriptive methods for personal information in a broad sense.

In judicial practice, the identification theory is a common theory in the process of defining personal data information. This theory also shows the fundamental reason why personal information needs legal protection, and is currently widely accepted in legislation. In this theory, a specific person can be directly or indirectly identified through the big data information related to the individual, which is the so-called "recognition". An important standard used to define personal data information is the "identifiable" of the information. In addition, when judging whether personal data information is identifiable, all reasonable methods that the information controller and any third party can take under the current social background should be considered comprehensively. The information that can be used for identification is either direct, intuitive, or indirect, and needs to be combined with specific conditions to make judgments.

In summary, the scope of personal data information can be defined from the following three perspectives at present: (1) Through measures such as assessing the use of personal data information and strengthening the identification of judicial cases, strive to clarify and overcome concepts. The defect of self-ambiguity. (2) More and more research supports the establishment of risk management concepts in the implementation of legislation and personal data information protection, as well as the establishment of incentive-compatible personal data information governance models. (3) Should focus on the life cycle of information and data, that is, the environment and stage of personal data information. “Relative anonymization involves the risk of re-identification of personal data information. A piece of information may selectively apply differentiated compliance obligations and legal responsibilities at different stages due to different risk assessment results.”[1]

(2) Threats of Big Data Investigation to the Security of Citizens’ Personal Data Information

The view of trace science in the field of big data investigation shows two-sided characteristics. In the digital age, the data sources of big data investigation are very extensive, and even include information related to personal privacy such as surfing the Internet and communicating with acquaintances. For ordinary citizens, it is tantamount to "running naked" under the investigation measures of investigators. Combined with the current Skynet system,

[1] Fan Wei. (2016). Reconstruction of the path of personal information protection in the era of big data. Global Legal Review (05), 92-115. doi:CNKI:SUN:WGFY.0.2016-05-007.

investigative agencies can accurately and efficiently identify specific citizens, which is a greater threat to citizens' personal data. Prevent machine learning from threats to humans in the three aspects of information security, ethics and privacy. The current dilemma is mainly manifested in: First, the defects of the current big data investigation algorithm lead to the initiative of the big clue investigation, and this and the process lack reasonable standards and principles to restrict; second, the investigators often conduct big data investigations. The presumption of guilt refers to finding evidence of a crime based on the assumption of a citizen's guilt; third, the massive personal data information held by the investigative agency, including other personal-related information, is at risk of leakage. Once it is used by criminals, the consequences will be unimaginable.

In addition, the compulsory measures included in the investigation will actually be effective in the process of information collection. The big data investigation is reflected in the compulsory measures in the source data collection. When considering the personal data and information of citizens involved in the big data investigation, Source data collection measures should be paid due attention to the infringement of personal data information and the intervention of citizens' personality rights in data applications. Citizen privacy and personal data information are not only subject to actual intervention by big data investigations, but also citizens' personal information is exposed to leakage or abuse at any time. This will pose a great threat to the legitimate rights and interests of citizens. Therefore, big data investigations are included. The scope of compulsory investigation is a wise move.

3. Protection Methods and Modes of Personal Data Information in Big Data Investigation Activities

(1) Defects of the traditional protection model of personal data information

Judging from my country's current practical experience in the protection of personal data and information, my country's "traditional protection model" dialectically absorbs the content of early foreign legislation and the spirit embodied in the principles of some international conventions. In general, it is Selective inheritance of foreign traditional protection models. In judicial practice, infringement remedies are often used to provide ex post compensation and compensation. In general, cases of infringement of personal data and information are classified as privacy dispute cases. Analyzed from the perspective of administrative supervision, most of them use administrative interviews or rectification methods to protect personal data information, but there is a lack of linkage mechanisms between multiple legal departments and substantive supervision and supervision methods.

At present, the traditional protection model can no longer adapt to the rapid development of high technology such as computers and big data and the rapid changes in society. Subjects' overall control of personal data and information is facing major challenges in the current context, which has caused serious conflicts with the development of the digital economy. "The traditional protection model with informed consent" as the core can neither provide substantial protection for citizens' personal information, but also become an obstacle to the development of data value in practice.In the traditional protection model, the notification and permission, information fuzzification and information anonymization methods also have some problems. For example, it is difficult to clearly inform the purpose of information use,

and the development of information technology makes it difficult to achieve anonymization of information. The feasibility and rationality of the traditional protection model in the new era have been questioned by academic circles.

Therefore, the traditional protection model is difficult to implement in practice, and it is impossible to completely prevent the abuse of personal data information. The era background of the digital economy and society's actual demand for data circulation make it necessary to change the protection mode of personal data information.

(2) The transformation of the legal protection model of personal data in big data investigation

The construction of a new model of legal protection of personal data information should be based on national conditions and local resources, and based on the characteristics of the national criminal justice system. Specifically: First, we should proceed from reality and clarify the scope of protection of personal data information based on practical experience in big data investigation practices. Secondly, the construction of the new model should start from one-way protection to multiple balances, proceed from the social attributes of personal data information, adhere to the combination of static protection and dynamic protection, and standardize the management of the risk of personal data information utilization in big data investigations. Furthermore, at the level of prevention, it should focus on the identification and resolution of risks before and during the event, rather than just taking infringement remedies or administrative penalties after engaging in it. Finally, the new protection model pays more attention to the combination of law and technology, and actively adopts legislation and judicial interpretation to refine the scope of personal data information risk assessment, and strive to establish a relationship of trust and mutual assistance between the subject of data information and the investigative agency."Therefore, the personal information protection mode in the context of big data should be based on scenario classification"[2] and "refined risk assessment",[3] and different departments and levels should be combined and coordinated to play a role.

Based on the idea of model transformation, the personal data information protection model in the new era should also focus on the rational use and circulation of data information, so that investigative agencies use personal data information to solve the case, while effectively protecting the safety of personal data information and its subjects, and making use of them. Big data technology can better create value for society. "In the state of relatively balanced interests, information providers and users should be in a state of cooperation and win-win situation." [4] "Personal information needs dynamic risk regulation and comprehensive

[2] Wen Yanyan & Peng Yan. (2018). Research on the protection mechanism of personal information. Journal of Information (07), 127-131.

[3]. Zhang Tao. (2019). EU personal data anonymization governance: law, technology and risk. Library Forum (12), 90-101.

[4] Zhu Yue. (2020). A review of the research on the legal protection of personal information in the context of big data. Library Forum (07), 36-45

protection."[5] This requires that while strictly complying with the existing personal information protection laws, establish risk management concepts in future personal data protection legislation and existing implementations, and establish an incentive-compatible personal data information governance model. The protection of personal data information involves many fields, including national security, intelligence collection, information processing and other fields. Therefore, in the legislative practice of the Personal Information Protection Law, it is necessary to integrate relevant knowledge of informatics and informatics."Scholars in the field of information science focus on the performance of users' personal privacy threats and the impact assessment of personal information leakage, and strengthen the protection of personal information from the perspective of government and enterprise risk assessment." [6]"The work of intelligence and counterintelligence aims to implement the overall national security concept and maintain the overall security of the society including personal security. Therefore, the personal information of the public should be respected most fundamentally."[7] Article 19 of the National Intelligence Law stipulates that national intelligence agencies and their staff shall not disclose personal information. Therefore, from the level of intelligence security and national security to a broader perspective, we must gradually incorporate the protection of personal data in big data investigation activities into the framework of information security protection, and regulate the procedures of big data investigation through laws. While continuously training and ethical education for investigators, we should pay attention to the construction of personal data information protection systems in different contexts, and restrict big data investigation agencies from engaging in illegal activities of illegal collection and processing of personal data from multiple angles and aspects. In addition, the law and ethics are also taken into consideration, and legal norms and ethics are established in online social scenes, business development scenes, network search scenes, etc., so that big data investigation agencies have laws to follow.

At present, research on the construction of the new protection model is mostly focused on the infringement of privacy by big data investigation activities and the confirmation of the personality rights of personal data, focusing on the control of the collection, processing and use of information by big data investigation agencies. Most scholars regard this as the protection of the personality rights of citizens and institutions. However, with the continuous occurrence of data competition and data disputes, the infringement of the property rights contained in the data by big data investigation activities has become the focus of research.

[5] Zhang Xinbao. (2018). Discussion on the main contradictions in the legislation of my country's personal information protection law. Journal of Social Sciences of Jilin University (05), 45-56+204-205. doi:10.15939/j.jujsse.2018.05.fx2.

[6] Su Ling & Lou Cequn. (2019). Analysis of Big Data Research in the Field of Information Science and Communication in my country. Information Science (05), 31-37. doi:10.13833/j.issn.1007-7634.2019.05.006.

[7] Wang Ying & Wang Tao. (2019). The View of Intelligence in my country's Network and Information Security Policies and Laws. Information Work (01), 15-22. doi:CNKI:SUN:QBZL.0.2019-01-005.

This is because the requirements of natural persons for their personal data and information are not limited to the interests of personal personality rights, but gradually extend to the interests of personal property. Therefore, some scholars have begun to explore the path of personal data information protection in big data investigation activities from the perspective of property rights, and advocate the path of embodying property rights in legislation. However, whether it is for personality rights or property rights, it emphasizes the control of the collection and processing of data and information in big data investigation activities. In the process of implementing protective measures, it is still only the protection of a single interest, which lacks systemicity and operability. It is unable to cope with the complex case situation in current judicial practice and the multiple interests and balance demands contained in personal data information. Moreover, because the current personal data protection rules are relatively simple, most of the research results are purely based on the information protection legislation experience of other countries and international organizations to propose solutions and legislative suggestions. Such operations cannot adapt to the actual development of the country and the new requirements of criminal justice practices in the new era. Therefore, in the construction of a new protection model, it is necessary to fully learn from the actual judicial situation and establish a comprehensive protection model based on the concept of rights protection to better balance the interests of all parties and realize data information in big data investigations and comprehensive protection of rights and interests.

In order to better build a new protection model, the first task is to establish a code of conduct to prevent and control personal data information risks so as to achieve the right to control personal data information in big data investigation activities. In the legislative process, our country should base itself on reality, absorb beneficial international experience, and adhere to the concepts of diversified duty subjects, complete legal regulations, and diversified protection roads in legislation, so as to promote procedural justice in big data investigation activities. The focus of research on the protection of personal data information should be on specific plans for the distribution of responsibilities, dynamic balance of interests, and risk supervision, and implement the responsibility system so that the main body of big data investigations can bear the adverse consequences of infringing on personal data information. In addition, the construction of a new model cannot ignore the convergence of personal data protection rules in civil law, administrative law, and criminal law, nor can it avoid disputes over the distribution of responsibilities in big data investigations. In addition, the protection of personal data information is itself an interdisciplinary academic issue. The realization of comprehensive management of personal data information risk is based on a more scientific risk assessment. The formation of anonymity technical standards requires research on the generation, acquisition, transmission and information identification methods of data information; the determination of risk scenarios requires theoretical research on the development trend of the digital economy and the evolution of data transaction business models; the construction of a data security environment requires the entire system Optimizing the development path of technology and discussing personal living habits. The personal data information protection compliance standards of investigative agencies need to improve the internal control system and improve management efficiency, so as to protect personal data and information in terms of entities and procedures. Relying on legal disciplines alone cannot

complete a multi-dimensional assessment of the risk of personal information use, and cannot quantify the weight of risk elements. Therefore, when discussing the reform and innovation of the legal protection model of personal data information, the research results of information science, economics, sociology, management and other disciplines should also be absorbed.

4. Concluding Remarks

In the big data investigation activities, the traditional protection model can no longer provide comprehensive protection of personal data information. It is urgent to construct a new model or protection mode in the process of transforming the legal protection mode of personal data information. What we should see is that the comprehensive management of personal data information risk is based on a more scientific risk assessment and a clear understanding of the current problems of big data investigation. The construction process of the new protection model is a dynamic evaluation process that needs to be continuously transformed according to the actual situation. We need to build a local resource and actual situation based on the reasonable definition of the concept of big data investigation and personal data information. Model. The construction of this model is an interdisciplinary and systematic project. It needs to be controlled in all aspects of legislation, justice, and law enforcement. It also needs to learn from the research objects and research of many disciplines such as criminology, law, and sociology. method. From the current point of view, there is a long way to go to build a comprehensive and reasonable new protection model. The re-examination of the personal data information protection system is a new perspective to study personal data information and even the legal protection model of personal information.

References

Fan, W. (2016). Reconstruction of the path of personal information protection in the era of big data. *Global Legal Review, 5*, 92-115.

Su, L., & Lou, C. (2019). Analysis of Big Data Research in the Field of Information Science and Communication in my country. *Information Science, 05*, 31-37.

Wang, Y., & Wang, T. (2019). The View of Intelligence in my country's Network and Information Security Policies and Laws. *Information Work, 01*, 15-22.

Wen, Y. Y., & Peng, Y. (2018). Research on the protection mechanism of personal information. *Journal of Information, 07*, 127-131.

Zhang, T. (2019). EU personal data anonymization governance: law, technology and risk. *Library Forum, 12*, 90-101.

Zhang, X. B. (2018). Discussion on the main contradictions in the legislation of my country's personal information protection law. *Journal of Social Sciences of Jilin University, 05*, 45-56+204-205.

Zhu, Y. (2020). Overview of the research on the legal protection of personal information in the context of big data. *Library Forum, 07*, 36-45.